Aymeric Fromherz

Curriculum Vitae

aymeric.fromherz@inria.fr

Education

2017-2021 **PhD**, *Electrical and Computer Engineering*, Carnegie Mellon University
A Proof-Oriented Approach to Low-Level, High-Assurance Programming
coadvised by Bryan Parno and Corina Pasareanu

2014–2015, 2016–2017 **Master (M.Sc.)**, *Computer Science*, Paris, Summa cum laude
MPRI (Master Parisien de Recherche en Informatique)

2014–2015 **Licence (B.Sc.)**, *Mathematics*, École Normale Supérieure, Paris

2013–2014 **Licence (B.Sc.)**, *Computer Science*, École Normale Supérieure, Paris, Summa cum laude

2011–2013 **Preparatory classes**, *MPSI/MP* (Maths-Physics)*, Lycée du Parc, Lyon

2011 **Baccaulauréat (French high school diploma)**, *Scientific*, Cité Scolaire Internationale, Lyon, Summa cum laude

Professional appointments

2022-now **Inria Starting Faculty Position**, *Prosecco Team*, Inria, France

2021-2022 **Postdoctoral Researcher**, *Prosecco Team*, Inria, France

Summer 2020 **Research Intern**, *Supervised by Nikhil Swamy*, Microsoft Research, Redmond, WA, USA

Summer 2019 **Research Intern**, *Supervised by Nikhil Swamy*, Microsoft Research, Redmond, WA, USA

Sept 2015–June 2016 **Development and Formal Proof of a MicroKernel**, ProvenRun, Paris, France, Engineer position

Honors and Awards

2022 **ACM SIGSAC Dissertation Award**

2022 **A.G. Milnes Award**, *Carnegie Mellon University*, Awarded to a graduating ECE Ph.D. student for the Ph.D. thesis work judged to be of the highest quality and which has had, or is likely to have, significant impact in his or her field.

2019 **Cylab Presidential Fellow**

2017 **Fondation Monahan Fellow**

2017 **Google Summer of Code**, Java Pathfinder, Mentor

2016 **Google Summer of Code**, Java Pathfinder, Student

2013 **Admission at the École Normale Supérieure, Paris**, National exam for computer science majors, ranked 13th

2011 **Abitur**, (German high school diploma)

Publications

Charon: An Analysis Framework for Rust, Son Ho, Guillaume Boisseau, Lucas Franceschino, Yoann Prak, Aymeric Fromherz, Jonathan Protzenko, *International Conference on Computer-Aided Verification (CAV), 2025*

CUTECat: Concolic Execution for Computational Law, Pierre Goutagny, Aymeric Fromherz, Raphaël Monat, *European Symposium on Programming (ESOP), 2025*, **Distinguished Artifact Award**

StarMalloc: Verifying a Modern, Hardened Memory Allocator, Antonin Reitz, Aymeric Fromherz, Jonathan Protzenko, *International Conference on Object-Oriented Programming, Systems,*

Languages and Applications (OOPSLA), 2024

Sound Borrow-Checking for Rust via Symbolic Semantics, Son Ho, Aymeric Fromherz, Jonathan Protzenko, *International Conference on Functional Programming (ICFP), 2024*

Formalizing Date Arithmetic and Statically Detecting Ambiguities for the Law, Raphael Monat, Aymeric Fromherz, Denis Merigoux, *European Symposium on Programming (ESOP), 2024*, **Best Tool Paper Award**

Modularity, Code Specialization, and Zero-Cost Abstractions for Program Verification, Son Ho, Aymeric Fromherz, Jonathan Protzenko, *International Conference on Functional Programming (ICFP), 2023*

FastVer2: A Provably Correct Monitor for Concurrent, Key-Value Stores, Arvind Arasu, Tahina Ramananandro, Aseem Rastogi, Nikhil Swamy, Aymeric Fromherz, Kesha Hietala, Bryan Parno, Ravi Ramamurthy, *International Conference on Certified Programs and Proofs (CPP), 2023*

Self-Repairing Neural Networks: Provable Safety for Deep Networks via Dynamic Repair, Klas Leino, Aymeric Fromherz, Ravi Mangal, Matt Fredrikson, Bryan Parno, Corina Pasareanu, *Workshop on Formal Methods for ML-Enabled Autonomous Systems (FoMLAS), 2022*

Turning Catala into a Proof Platform for the Law, Alain Delaët, Denis Merigoux, Aymeric Fromherz, *Programming Languages and the Law (ProLaLa), 2022*

Steel: Proof-oriented Programming in a Dependently Typed Concurrent Separation Logic, Aymeric Fromherz, Aseem Rastogi, Nikhil Swamy, Sydney Gibson, Guido Martínez, Denis Merigoux, Tahina Ramananandro, *International Conference on Functional Programming (ICFP), 2021*

Fast Geometric Projections for Local Robustness Certification, Aymeric Fromherz, Klas Leino, Matt Fredrikson, Bryan Parno, Corina Pasareanu, *International Conference on Learning Representations (ICLR), Spotlight Paper, 2021*

HACLxN: Verified Generic SIMD Crypto (for All Your Favourite Platforms), Marina Polubelova, Karthikeyan Bhargavan, Jonathan Protzenko, Benjamin Beurdouche, Aymeric Fromherz, Natalia Kulatova, Santiago Zanella-Béguelin, *ACM Conference on Computer and Communications Security (CCS), 2020*

SteelCore: An Extensible Concurrent Separation Logic for Effectful Dependently Typed Programs, Nikhil Swamy, Aseem Rastogi, Aymeric Fromherz, Denis Merigoux, Danel Ahman, Guido Martinez, *International Conference on Functional Programming (ICFP), 2020*

Steel: Scaling up Memory Reasoning for F*, Aymeric Fromherz, Denis Merigoux, *Automated Deduction for Separation Logics (ADSL), 2020*

EverCrypt: A Fast, Verified, Cross-Platform Cryptographic Provider, Jonathan Protzenko, Bryan Parno, Aymeric Fromherz, Chris Hawblitzel, Marina Polubelova, Karthikeyan Bhargavan, Benjamin Beurdouche, Joonwon Choi, Antoine Delignat-Lavaud, Cédric Fournet, Tahina Ramananandro, Aseem Rastogi, Nikhil Swamy, Christoph Wintersteiger, and Santiago Zanella-Beguelin, *IEEE Symposium on Security and Privacy (Oakland), 2020*

Symbolic Pathfinder for SV-COMP - (Competition Contribution), Yannic Noller, Corina S. Pasareanu, Aymeric Fromherz, Xuan-Bach D. Le, Willem Visser, *International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2019*

A Verified, Efficient Embedding of a Verifiable Assembly Language, Aymeric Fromherz, Nick Giannarakis, Chris Hawblitzel, Bryan Parno, Aseem Rastogi, and Nikhil Swamy, *Symposium on Principles of Programming Languages (POPL), 2019*

Static Value Analysis of Python Programs by Abstract Interpretation, Aymeric Fromherz, Abdelraouf Ouadjaout, Antoine Miné, *NASA Formal Methods Symposium (NFM), 2018*

Symbolic Arrays in Symbolic Pathfinder, Aymeric Fromherz, Kasper S. Luckow, Corina S. Pasareanu, *Java PathFinder Workshop, 2016*

Preprints

Project Everest: Perspectives from Developing Industrial-grade High-Assurance Software, Danel Ahman, Karthikeyan Bhargavan, Chris Brzuska, Barry Bond, Jay Bosamiya, Antoine Delignat-Lavaud, Aymeric Fromherz, Cédric Fournet, Sydney Gibson, Chris Hawblitzel, Cătălin Hriţcu, Markulf Kohlweiss, Guido Martinez, Haobin Ni, Bryan Parno, Jonathan Protzenko, Tahina Ramananandro, Aseem Rastogi, Exequiel Rivas, Nikhil Swamy, Santiago Zanella-Béguelin

Technical Reports

Layered Indexed Effects. Foundations and Applications of Effectful Dependently Typed Programming, Aseem Rastogi, Guido Martínez, Aymeric Fromherz, Tahina Ramananandro, Nikhil Swamy

Teaching Experience

Fall-Winter 2024 **Proofs of Security Protocols**, 2-30, *Master Parisien de Recherche en Informatique (MPRI)*, Lecturer

Fall-Winter 2024 **Proofs of Security Protocols**, 2-30, *Master Parisien de Recherche en Informatique (MPRI)*, Lecturer

Fall-Winter 2023 **Proofs of Security Protocols**, 2-30, *Master Parisien de Recherche en Informatique (MPRI)*, Lecturer

Spring 2019 **Secure Software Systems**, 18-732, *Carnegie Mellon University*, Head Teaching Assistant

Spring 2018 **Secure Software Systems**, 18-732, *Carnegie Mellon University*, Head Teaching Assistant

Professional Service

Program Committee member. CPP 26, PriSC 26, CSF 26, ITP 25, USENIX Security' 25, CSF 25, POPL 24, USENIX Security' 24, JFLA' 23, USENIX Security' 23, USENIX Security' 22

Artifact Evaluation Committee member. ICFP' 22, ICFP' 21, POPL'21, ICFP'20, ISSTA'20

External Reviewer. ESOP'21, POPL'20, CPP'20, ESOP'20, FSE'19