

# Tahina RAMANANANDRO

Ph. D., Computer Science

Principal Research Software Development Engineer  
Research in Software Engineering (RiSE)  
Microsoft Research  
Redmond, Building 99, Office 3121

+1 (425) 421 7263

Tahina Ramananandro  
Microsoft Corporation  
taramana 99/3121  
1 Microsoft Way  
Redmond, WA 98052, USA

taramana@microsoft.com, tahina@ramananandro.org  
<http://tahina.ramananandro.org>

## In Short

Versatile computer scientist skilled in both research and engineering. Strengths in logic, languages, algorithms, architectures, protocols, and operating systems.

15+ years of extensive expertise on formal verification, using the Coq proof assistant and the F\* programming language: semantics of programming languages and their memory models (C, C++, and domain-specific languages), program verification, verified compilation, verified parsers and serializers for binary data formats, verified protocol implementations. Focus on end-to-end verification from high-level specifications down to the actual code, compositional verification of modular systems, and applications of formal verification to industrial-grade software and operating systems.

2016 – present **Microsoft Research, Redmond (Washington), USA**

EverParse: automatic generation of fully verified parsers and serializers for binary data formats.

The  $F^*$  dependently typed functional programming language and proof assistant.

The Everest project: formal verification of a reference implementation of TLS, QUIC and other network protocols.

FastVer: formally verified runtime security monitors for zero-trust cloud service providers

2014 – 2016 **Reservoir Labs, Inc., New York (New York), USA**

Formal verification of C programs with floating-point computations for energy-efficient implementations of radar algorithms, using Coq

Efficient tensor decompositions for the ENSIGN Tensor Toolbox

Advanced testing of the R-Stream automatic parallelizing compiler using Csmith

2012 – 2014 **Yale University, New Haven (Connecticut), USA**

Post-doc: specification, implementation, verification and verified compilation of the CertiKOS operating-system kernel and hypervisor, using Coq and the CompCert verified compiler

2007 – 2012 **INRIA, Paris-Rocquencourt, France**

Ph. D: mechanized formal semantics and verified compilation for C++ objects

Master's: formally verified implementation of a garbage collector for a verified compiler with Coq

2006 **MIT, Cambridge (Massachusetts), USA**

Mondex, an electronic purse for digital cash: specification, refinement and proof using the Alloy model-finding method

2005 **INRIA, Sophia-Antipolis, France**

Formal verification of probabilistic algorithms with Coq

## Higher Education Degrees

|         |                          |                         |                                     |                |
|---------|--------------------------|-------------------------|-------------------------------------|----------------|
| 01/2012 | <b>Ph. D.</b>            | <b>Computer Science</b> | Université Paris. Diderot (Paris 7) | Paris (France) |
| 09/2007 | <b>Master's Degree</b>   | <b>Computer Science</b> | École normale supérieure            | Paris (France) |
| 09/2005 | <b>Bachelor's Degree</b> | <b>Mathematics</b>      | Université Paris. Diderot (Paris 7) | Paris (France) |

## References

Nikhil SWAMY, Senior Principal Researcher, Microsoft Research [nswamy@microsoft.com](mailto:nswamy@microsoft.com)

Zhong SHAO, Professor, Yale University [zhong.shao@yale.edu](mailto:zhong.shao@yale.edu)

Xavier LEROY, Professor, Collège de France [xavier.leroy@college-de-france.fr](mailto:xavier.leroy@college-de-france.fr)

## Summary of held positions

### Employment

|         |   |         |  |                              |
|---------|---|---------|--|------------------------------|
| 03/2021 | – | present | <b>Principal Research Software Development Engineer</b>                                      |                              |
| 09/2016 | – | 02/2021 | <b>Senior Research Software Development Engineer</b>   |                              |
|         |   |         | Microsoft Corp.  | Redmond, Washington (USA)    |
| 10/2014 | – | 09/2016 | <b>Senior Engineer</b>   |                              |
|         |   |         | Reservoir Labs Inc.  | New York, New York (USA)     |
| 01/2013 | – | 09/2014 | <b>Associate Research Scientist</b>  |                              |
| 01/2012 | – | 12/2012 | <b>Post-Doctoral Associate</b>   |                              |
|         |   |         | Yale University  | New Haven, Connecticut (USA) |
| 09/2011 | – | 12/2011 | <b>Research Associate</b>  |                              |
|         |   |         | École normale supérieure   | Paris (France)               |
| 09/2008 | – | 08/2011 | <b>Ph. D. student and Teaching Assistant</b>   |                              |
|         |   |         | Université Paris. Diderot (Paris 7)  | Paris (France)               |
|         |   |         | <i>Ph. D. Research performed at INRIA Paris-Rocquencourt</i>                                 | Rocquencourt (France)        |
| 09/2004 | – | 08/2008 | <b>Student with civil servant status</b>   |                              |
|         |   |         | École normale supérieure   | Paris (France)               |
| 03/2008 | – | 05/2008 | <b>Teaching Assistant</b> (concurrent employment)  |                              |
|         |   |         | IFIPS (Paris-Sud Institute for Training Engineers),<br>Université Paris Sud Orsay (Paris 11) | Orsay (France)               |

### Internships

|         |   |         |                                       |                                |
|---------|---|---------|---------------------------------------|--------------------------------|
| 03/2007 | – | 09/2007 | <b>Masters Research Intern</b>        |                                |
|         |   |         | INRIA Paris-Rocquencourt              | Rocquencourt (France)          |
| 03/2006 | – | 08/2006 | <b>Research Intern</b>                |                                |
|         |   |         | Massachusetts Institute of Technology | Cambridge, Massachusetts (USA) |
| 06/2005 | – | 08/2005 | <b>Research Intern</b>                |                                |
|         |   |         | INRIA Sophia Antipolis                | Valbonne (France)              |

## Research

2016 – present **Microsoft Research, Redmond, Washington (USA)**

Principal Research Software Development Engineer (March 2021 – present)

Senior Research Software Development Engineer (September 2016 – February 2021)

- Main author of EverParse, a formally verified library and automatic generator for fully verified parsing and serialization of binary data formats.  
Related Publications: [C19] [C18] [N1] [C13]
- Implementation of the  $F^*$  functional programming language with refinement types, and development and formal verification of its standard library.  
Related Publications: [C17] [C12] [C10] [C9]
- The Everest project: specification, development and formal verification of a reference implementation of TLS, QUIC and other network protocols.  
Related Publications: [C15] [C14] [C8]
- FastVer: Formal verification of runtime security monitors for zero-trust cloud service providers  
Related Publications: [C20] [C16]

2014 – 2016 **Reservoir Labs Inc., New York, New York (USA)**

Senior Engineer (October 2014 – September 2016)

- Key personnel for the Reservoir Labs team part of the DARPA-funded PERFECT (Power Efficiency Revolution for Embedded Computing Technologies) project (October 2014 – November 2015): software and algorithms to reduce power consumption in embedded computing systems:
  - End-to-end formal verification of floating-point computations in C programs using the Coq proof assistant, and application to energy-efficient implementations of Synthetic Aperture Radar back-projection image processing algorithms.  
Related publications: [C6]
  - The ENSIGN Tensor Toolbox: performance testing, and implementation of efficient algorithms for Tucker tensor decomposition.  
Related Publication: [C7]
  - The R-Stream automatic parallelizing compiler: correctness testing with Csmith.
- Collaboration with Prof. Zhong Shao, Yale University: specification, implementation, verification and verified compilation of the CertiKOS layered operating system kernel and hypervisor, using the Coq proof assistant.  
Related publication: [C11]

2012 – 2014 **Yale University, New Haven, Connecticut (USA)**

*Verified Separate Compilation and Compositional Verification of Operating System Kernels*

Associate Research Scientist (January 2013 – September 2014)

Post-doctoral Associate (January – December 2012)

Research directed by Zhong SHAO, FLINT, Department of Computer Science

- Key personnel for the DARPA-funded HACMS (High-Assurance Cyber-Military Systems) project, CARS team (August 2012 – September 2014): development of fully verified robotics software and operating system for unmanned ground and air vehicles.
  - Quantitative CompCert: source-level verification of resource consumption guarantees and verified preservation during compilation.  
Related publications: [C3]
  - Specification, implementation, verification and verified compilation of the CertiKOS layered operating system kernel and hypervisor, using the Coq proof assistant.  
Related publications: [C4] [C5]

- 2008 – 2012 **INRIA (French National Institute for Research in Computer Science and Control) Paris-Rocquencourt (France)**  
*Mechanized Formal Semantics and Verified Compilation for C++ Objects*  
 Ph. D. student (September 2008 – January 2012)  
 Ph. D. directed by Xavier LEROY, *Gallium*.  
 Specification and implementation of a verified compiler front-end to CompCert for a subset of C++ with multiple inheritance, using the Coq proof assistant: verified object layout and verified compilation of function dispatch, construction and destruction.  
 Ph. D. awarded by Université Paris. Diderot (Paris 7), Paris (France).  
 Related Publications: [C2] [C1] [Θ3]
- 2007 **INRIA Paris-Rocquencourt**  
*Formal verification of a garbage collector implementation for a verified compiler with Coq*  
 Research Intern and Masters student (March – September)  
 Master’s Thesis directed by Xavier LEROY, *Gallium*.  
 Master’s Degree awarded by École normale supérieure, Paris (France).  
 Related Publication: [Θ2]
- 2006 **MIT (Massachusetts Institute of Technology), Cambridge, Massachusetts (USA)**  
*Mondex, an electronic purse: specification, verification and proof with Alloy*  
 Research intern (March – August)  
 Directed by Daniel JACKSON, *Software Design Group*, CSAIL (Computer Science and Artificial Intelligence Laboratory).  
 Part of VSR-NET project (*Verified Software Repository*), *Grand Challenge 6 : Dependable Systems Evolution*, directed by Jim WOODCOCK, University of York (United Kingdom).  
 Related Publications: [J1]
- 2005 **INRIA Sophia-Antipolis (France)**  
*Formal verification of probabilistic algorithms with Coq*  
 Research intern (June – August)  
 Directed by Philippe AUDEBAUD and Laurent THÉRY, *Marelle*.  
 Related Publication: [Θ1]

## Publications

### International peer-reviewed conferences and workshops

- [C20] Arvind ARASU, Tahina RAMANANANDRO, Aseem RASTOGI, Nikhil SWAMY, Aymeric FROMHERZ, Kesha HIETALA, Bryan PARNO, Ravi RAMAMURTHY  
*FastVer2: A Provably Correct Monitor for Concurrent, Key-Value Stores*  
 CPP 2023 (12<sup>th</sup> ACM SIGPLAN International Conference on Certified Programs and Proofs)  
 Accepted for publication, to appear
- [C19] Haobin NI, Antoine DELIGNAT-LAVAUD, Cédric FOURNET, Tahina RAMANANANDRO, Nikhil SWAMY  
*ASN1\*: Provably Correct Non-Malleable Parsing for ASN.1 DER*  
 CPP 2023 (12<sup>th</sup> ACM SIGPLAN International Conference on Certified Programs and Proofs)  
 Accepted for publication, to appear
- [C18] Nikhil SWAMY, Tahina RAMANANANDRO, Aseem RASTOGI, Irina SPIRIDONOVA, Haobin NI, Dmitry MALLOY, Juan VAZQUEZ, Michael TANG, Omar CARDONA, Arti GUPTA  
*Hardening Attack Surfaces with Formally Proven Binary Format Parsers*  
 PLDI 2022 (43<sup>rd</sup> ACM SIGPLAN Conference on Programming Language Design and Implementation)
- [C17] Aymeric FROMHERZ, Aseem RASTOGI, Nikhil SWAMY, Sydney GIBSON, Denis MERIGOUX, Tahina RAMANANANDRO  
*Steel: Proof-oriented Programming in a Dependently Typed Concurrent Separation Logic*  
 ICFP 2021 (26<sup>th</sup> ACM SIGPLAN International Conference on Functional Programming)
- [C16] Arvind ARASU, Johannes GEHRKE, Esha GHOSH, Donald KOSSMANN, Jonathan PROTZENKO, Ravi RAMAMURTHY, Tahina RAMANANANDRO, Aseem RASTOGI, Srinath SETTY, Nikhil SWAMY, Alexander VAN RENEN, Min XU  
*FastVer: Making Data Integrity a Commodity*  
 ACM SIGMOD 2021

- [C15] Antoine DELIGNAT-LAVAUD, Cédric FOURNET, Bryan PARNO, Jonathan PROTZENKO, Tahina RAMANANANDRO, Jay BOSAMIYA, Joseph LALLEMAND, Itsaka RAKOTONIRINA, Yi ZHOU  
*A Security Model and Fully Verified Implementation for the IETF QUIC Record Layer*  
S&P “Oakland” 2021 (42<sup>nd</sup> IEEE Symposium on Security and Privacy)
- [C14] 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, Santiago ZANELLA-BÉGUELIN  
*EverCrypt: A Fast, Verified, Cross-Platform Cryptographic Provider*  
S&P “Oakland” 2020 (41<sup>st</sup> IEEE Symposium on Security and Privacy)
- [C13] Tahina RAMANANANDRO, Antoine DELIGNAT-LAVAUD, Cédric FOURNET, Nikhil SWAMY, Tej CHAJED, Nadim KOBEISSI and Jonathan PROTZENKO  
*EverParse: Verified Secure Zero-Copy Parsers For Authenticated Message Formats*  
USENIX Security 2019 (28<sup>th</sup> Symposium)
- [C12] Guido MARTÍNEZ, Danel AHMAN, Victor DUMITRESCU, Nick GIANNARAKIS, Chris HAWBLITZEL, Catalin HRITCU, Monal NARASIMHAMURTHY, Zoe PARASKEVOPOULOU, Clément PIT-CLAUDEL, Jonathan PROTZENKO, Tahina RAMANANANDRO, Aseem RASTOGI, Nikhil SWAMY  
*Meta-F\*: Proof Automation with SMT, Tactics and Metaprograms*  
ESOP 2019 (28<sup>th</sup> ETAPS European Symposium on Programming)
- [C11] Ronghui GU, Zhong SHAO, Jieung KIM, Xiongnan (Newman) WU, Jérémie KOENIG, Vilhelm SJÖBERG, Hao CHEN, David COSTANZO and Tahina RAMANANANDRO  
*Certified Concurrent Abstraction Layers*  
PLDI 2018 (39<sup>th</sup> ACM SIGPLAN Conference on Programming Languages Design and Implementation)
- [C10] Niklas GRIMM, Kenji MAILLARD, Cédric FOURNET, Catalin HRITCU, Matteo MAFFEI, Jonathan PROTZENKO, Tahina RAMANANANDRO, Aseem RASTOGI, Nikhil SWAMY and Santiago ZANELLA-BÉGUELIN  
*A Monadic Approach to Relational Verification: Applied to Information Security, Program Equivalence, and Optimizations*  
CPP 2018 (7<sup>th</sup> ACM SIGPLAN International Conference on Certified Programs and Proofs)
- [C9] Jonathan PROTZENKO, Jean-Karim ZINZINDOHOUE, Aseem RASTOGI, Tahina RAMANANANDRO, Peng WANG, Santiago ZANELLA-BÉGUELIN, Antoine DELIGNAT-LAVAUD, Catalin HRITCU, Karthikeyan BHARGAVAN, Cédric FOURNET and Nikhil SWAMY  
*Verified Low-Level Programming Embedded in F\**  
ICFP 2017 (22<sup>nd</sup> ACM SIGPLAN International Conference on Functional Programming)
- [C8] Karthikeyan BHARGAVAN, Barry BOND, Antoine DELIGNAT-LAVAUD, Cédric FOURNET, Chris HAWBLITZEL, Catalin HRITCU, Samin ISHTIAQ, Markulf KOHLWEISS, Rustan LEINO, Jay LORCH, Kenji MAILLARD, Jianyang PANG, Bryan PARNO, Jonathan PROTZENKO, Tahina RAMANANANDRO, Ashay RANE, Aseem RASTOGI, Nikhil SWAMY, Laure THOMPSON, Peng WANG, Santiago ZANELLA-BÉGUELIN and Jean-Karim ZINZINDOHOUE  
*Everest: Towards a Verified, Drop-in Replacement of HTTPS*  
SNAPL 2017 (2<sup>nd</sup> Summit on Advances in Programming Languages)
- [C7] Muthu BASKARAN, M. Harper LANGSTON, Tahina RAMANANANDRO, David BRUNS-SMITH, Tom HENRETTY, James EZICK and Richard LETHIN  
*Accelerated Low-Rank Updates to Tensor Decompositions*  
HPEC 2016 (20<sup>th</sup> IEEE Conference on High Performance Extreme Computing)
- [C6] Tahina RAMANANANDRO, Paul MOUNTCASTLE, Benoît MEISTER and Richard LETHIN  
*A Unified Coq Framework for Verifying C Programs with Floating-Point Computations*  
CPP 2016 (5<sup>th</sup> ACM SIGPLAN Conference on Certified Programs and Proofs)
- [C5] Tahina RAMANANANDRO, Zhong SHAO, Shu-Chun WENG, Jérémie KOENIG and Yuchen FU  
*A Compositional Semantics for Verified Separate Compilation and Linking*  
CPP 2015 (4<sup>th</sup> ACM SIGPLAN Conference on Certified Programs and Proofs)
- [C4] Ronghui GU, Jérémie KOENIG, Tahina RAMANANANDRO, Zhong SHAO, Xiongnan WU, Shu-Chun WENG, Haozhong ZHANG and Yu GUO  
*Deep Specifications and Certified Abstraction Layers*  
POPL 2015 (42<sup>nd</sup> ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages)

- [C3] Quentin CARBONNEAUX, Jan HOFFMANN, Tahina RAMANANANDRO and Zhong SHAO  
*End-to-End Verification of Stack-Space Bounds for C Programs*  
PLDI 2014 (35<sup>th</sup> ACM SIGPLAN Conference on Programming Languages Design and Implementation)
- [C2] Tahina RAMANANANDRO, Gabriel DOS REIS and Xavier LEROY  
*A Mechanized Semantics for C++ Object Construction and Destruction, with Applications to Resource Management*  
POPL 2012 (39<sup>th</sup> ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages)
- [C1] Tahina RAMANANANDRO, Gabriel DOS REIS and Xavier LEROY  
*Formal verification of object layout for C++ multiple inheritance*  
POPL 2011 (38<sup>th</sup> ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages)

## International peer-reviewed journals

- [J1] Tahina RAMANANANDRO  
*Mondex, an electronic purse : specification, and refinement checks with the Alloy model-finding method*  
Formal Aspects of Computing, 20.1, Springer, January 2008.

## Theses

- [Θ3] *Mechanized Formal Semantics and Verified Compilation for C++ Objects*  
Ph. D. thesis, Université Paris. Diderot (Paris 7)  
Successfully defended on January 10<sup>th</sup>, 2012 at École normale supérieure.
- [Θ2] *Vérification formelle d'une implémentation d'un gestionnaire de mémoire pour un compilateur certifié*  
Master's thesis, École normale supérieure, Paris (France)  
Successfully defended in September 2007 at École normale supérieure.
- [Θ1] *Vérification formelle d'algorithmes probabilistes*  
Bachelor's Degree thesis, Université Paris. Diderot (Paris 7)  
Successfully defended in September 2005 at École normale supérieure.

## News and Blog Articles

- [N1] Tahina RAMANANANDRO, Aseem RASTOGI, Nikhil SWAMY  
*EverParse: Hardening critical attack surfaces with formally proven message parsers*  
Microsoft Research Blog, May 3<sup>rd</sup>, 2021



## Community service

### Conferences

Program committee member: ACM/SIGPLAN ICFP 2023  
 Program committee member: ACM/SIGPLAN PLDI 2021  
 Program committee member: ACM/SIGPLAN CPP 2021  
 External review committee member: ACM/SIGPLAN PLDI 2020  
 Artifact evaluation committee member: ACM/SIGPLAN ICFP 2017

### Workshops

Program committee member: IEEE S&P LangSec 2023, IEEE HPCS CADO 2018, ACM/SIGADA HILT 2016, ACM/SIGPLAN HOPE 2015.  
 Reviewer: SSV 2012 (EPTCS 102)

## Teaching

2012 **Yale University**  
*CS421: Compilers and Interpreters* course by Zhong SHAO  
 2 lectures on Certified Compilers

2008 – 2011 **Université Paris. Diderot (Paris 7)**  
 Teaching assistant for undergraduate students.

2011 *Virtual machines* course by Gabriel KERNEIS  
 2011 *Syntactic analysis and Compilation* course by Yann RÉGIS-GIANAS  
 2010 *Functional programming with Objective CAML* course by Ralf TREINEN  
 2010 *The C programming language* course by Jean-Marie RIFFLET  
 2009 *Object-oriented programming with Java* course by Hugues FAUCONNIER  
 2009 *Java data types and objects* course by Hugues FAUCONNIER

2008 **Lycée Louis-le-Grand, Paris**  
 Teaching assistant for undergraduate *Classes préparatoires* students (*colles*)  
*CAML programming* course by Anne-Laure BIOLLEY

2008 **IFIPS (Paris-Sud Institute for Training Engineers),  
 Université Paris 11 – Paris-Sud Orsay**  
 Teaching assistant for undergraduate students.  
*Compilation* course by François YVON

2005 – 2011 **École normale supérieure**  
 Training and support volunteer (*Tuteur informatique*)  
*Linux-powered workstations; L<sup>A</sup>T<sub>E</sub>X.*

## Education

- 2008 – 2012     **Université Paris. Diderot (Paris 7)**  
Ph. D., Computer Science.
- 2004 – 2008     **ENS (École normale supérieure), Paris**  
2005 – 2007     *MPRI (Parisian Master of Research in Computer Science).*  
Master's Degree, Computer Science.
- 2004 – 2005     *MMFAI (Magistère of Fundamental and Applied Mathematics and Computer Science), first year.*  
2004            Entrance exam: INFO, succeeded, rank 3.
- 2004 – 2005     **Université Paris. Diderot (Paris 7)**  
Bachelor's Degree, Mathematics.
- 1999 – 2004     **Lycée Kléber, Strasbourg**  
2002 – 2004     *Classes préparatoires* (intensive courses preparing to highly competitive exams to enter *Grandes Écoles* schools of higher education).
- 2002            Scientific *Baccalauréat* (national high school diploma)

## Computer skills

- Programming languages: **OCaml**, **C**, **F#**, **C++**, **Java** (including Java bytecode), **x86 (IA-32) assembly**, Basic variants<sup>1</sup>.
- Formal methods: **F\***, **Coq**, Alloy.
- CI/CD and Admin: **git**, **GitHub Actions**, **Docker**, **Ubuntu Linux**, Azure DevOps, Apache HTTP server, Drupal
- Scripting languages: **bash**, Perl (including CGI scripting), **PHP**, **JavaScript**.
- Text processing languages: **L<sup>A</sup>T<sub>E</sub>X**, **HTML/XHTML**, **CSS**.
- Database processing languages: **SQL**.
- Scientific tools: Maple.

## Languages

- Native French. Winner of French National Dictation Championship *Les Dicos d'Or* by Bernard PIVOT, School Juniors, at *Olympia*, Paris, January 2001.
- Fluent English and German.
- Learning Malagasy, Mandarin Chinese.

---

<sup>1</sup>including TI-Basic, QBasic, Visual Basic, VBA/Excel, OpenOffice.org Basic