

Tahina RAMANANANDRO

Ph. D., Computer Science

Senior Research Software Development Engineer
Research in Software Engineering (RiSE)
Microsoft Research
Redmond, Building 99, Office 2961

+1 (425) 421 7263

Tahina Ramananandro
Microsoft Corporation
taramana 99/2961
1 Microsoft Way
Redmond, WA 98052, USA

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

In Short

Versatile and skilled computer scientist and mathematician. Strengths in logic, languages, algorithms, architectures, and operating systems.

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. 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 system kernels.

- 2016 – present **Microsoft Research, Redmond (Washington), USA**
The F^* dependently typed functional language. The Lean proof assistant. The Everest project: formal verification of a reference implementation of TLS and other network protocols.
- 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	Ph. D.	Computer Science	Université Paris. Diderot (Paris 7)	Paris (France)
09/2007	Master's Degree	Computer Science	École normale supérieure	Paris (France)
09/2005	Bachelor's Degree	Mathematics	Université Paris. Diderot (Paris 7)	Paris (France)

References

Nikhil SWAMY, Senior Researcher,	Microsoft Research	nswamy@microsoft.com
Richard LETHIN, President,	Reservoir Labs, Inc.	lethin@reservoir.com
Zhong SHAO, Professor,	Yale University	zhong.shao@yale.edu
Xavier LEROY, Senior Research Scientist,	INRIA	xavier.leroy@inria.fr

Summary of held positions

Employment

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

Internships

09/2008	– 01/2012	Ph. D. Research Intern INRIA Paris-Rocquencourt	Rocquencourt (France)
03/2007	– 09/2007	Masters Research Intern INRIA Paris-Rocquencourt	Rocquencourt (France)
03/2006	– 08/2006	Research Intern Massachusetts Institute of Technology	Cambridge, Massachusetts (USA)
06/2005	– 08/2005	Research Intern INRIA Sophia Antipolis	Valbonne (France)

Research

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

Senior Research Software Development Engineer (September 2016 – present)

- Implementation of the F^* functional language with refinement types, and development and formal verification of its standard library.
- Implementation of the Lean proof assistant, and development and formal verification of its standard library.
- The Everest project: specification, development and formal verification of a reference implementation of TLS and other network protocols.
Related Publications: [C10] [C9] [C8]

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

Senior Engineer (October 2014 – September 2016)

- Key personnel for the DARPA-funded PERFECT (Power Efficiency Revolution for Embedded Computing Technologies) project, SPOTTER team (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 backprojection image processing algorithms.
Related publications: [C6] [T4]
- 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] [T2]
- Specification, implementation, verification and verified compilation of the CertiKOS layered operating system kernel and hypervisor, using the Coq proof assistant:
 - LayerLib: compositional verification for layered systems.
 - CompCertX: verified separate compilation for layered systems.

Related publications: [C4] [C5] [T3]

- 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
 Research Intern and 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.
 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*.
 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] [T1]
- 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

- [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 (39th ACM SIGPLAN Conference on Programming Languages Design and Implementation)
 Accepted for publication, to appear
- [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 (7th 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-LAUAUD, Catalin HRITCU, Karthikeyan BHARGAVAN, Cédric FOURNET and Nikhil SWAMY
*Verified Low-Level Programming Embedded in F**
 ICFP 2017 (22nd ACM SIGPLAN International Conference on Functional Programming)
- [C8] Karthikeyan BHARGAVAN, Barry BOND, Antoine DELIGNAT-LAUAUD, 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 (2nd 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 (20th 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 (5th 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 (4th 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 (42nd 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 (35th 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 (39th 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 (38th 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 10th, 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.

Talks

List of public dissemination talks additionally to those given for peer-reviewed conference papers or thesis defenses.

- [T4] *Formal Verification of Floating-Point Computations in C Programs: Verified Error Bounds for Signal Processing*
HCSS 2016 (CPS-VO Conference on High-Confidence Software and Systems)
- [T3] *CompCertX: Verified Separate Compilation for Compositional Verification of Operating-System Kernels*
INRIA Gallium team seminar, August 2014
- [T2] *End-to-End Verification of Stack-Space Bounds for C Programs*
INRIA Gallium team seminar, April 2014
- [T1] *Alloy / Mondex Case Study: Refinement Checks with Model-Finding*
3rd VSR-NET meeting, May 2006

Community service

ACM/SIGPLAN ICFP 2017 (artifact evaluation committee member), ACM/SIGADA HILT 2016 (PC member), ACM/SIGPLAN HOPE 2015 (PC member), SSV 2012 (EPTCS 102) (reviewer)

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; LaTeX.

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, admitted, 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 high-competitive exams to enter *Grandes Écoles*).
 2002 Scientific *Baccalauréat* (national high school diploma)

Computer skills

- Programming languages: OCaml, F#, C, C++, Java (including Java bytecode), x86 (IA-32) assembly, Basic variants¹.
- Scripting languages: bash, Perl (including CGI scripting), PHP, JavaScript.
- Database processing languages: SQL.
- Text processing languages: LaTeX, HTML/XHTML, CSS.
- Administration: Docker, Ubuntu Linux, Apache HTTP server, Drupal CMS.
- Scientific tools: Maple.
- Formal methods: F*, Coq, Alloy.

Languages

- Fluent French (mother tongue). 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, Chinese.

Leisure

- Mycology (studying fungi).
- Playing and inventing games.
- Urban planning and public transportation networks.

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