Cătălin Hriţcu

Curriculum Vitae

Contact

Max Planck Institute for Security and Privacy (MPI-SP)
Universitätsstraße 140, 44799 Bochum, Germany

catalin.hritcu@mpi-sp.org https://catalin-hritcu.github.io

Education

02/2018–01/2019 **Habilitation** in Computer Science from ENS Paris and PSL Research University

06/2007–01/2012 **Ph.D.** in Computer Science from Saarland University, **Summa cum Laude**

10/2005–05/2007 **M.Sc.** in Computer Science from Saarland University, Germany, **Honors degree**

09/2001–06/2005 **Licentiate** (4 years undergrad degree) in Computer Science from "Alexandru Ioan Cuza" University, Iaşi, Romania, **Honors degree**

Positions

05/2020–now **Tenured Faculty** (W2 Research Group Leader with Tenure) at the **Max Planck Institute for Security and Privacy (MPI-SP)** in Bochum, Germany.

10/2013–04/2020 **Tenured Researcher** (chargé de recherche) at **Inria Paris** in the Prosecco team

09–10/2016 **Visiting Researcher** at **Microsoft Research Redmond**

05/2011–09/2013 **Postdoctoral Research Associate** at **University of Pennsylvania**; DARPA CRASH/SAFE project; Supervisor: Benjamin C. Pierce

09–11/2009 **Research Intern** at **Microsoft Research Cambridge (UK)**

Grants

2020–now **Co-PI of CASA Excellence Cluster** at Ruhr University Bochum (RUB)

01/2017–12/2021 **PI of SECOMP ERC Starting Grant** from the European Research Council on *Efficient Formally Secure Compilers to a Tagged Architecture*

03/2019–05/2020 **Co-PI of Tezos Foundation Grant** on *The Formal Semantics and Evolution of the F⋆ Verification System*

12/2017–05/2020 **Co-PI of DARPA SSITH/HOPE grant** on *Advanced New Hardware Optimized for Policy Enforcement, A New HOPE*

10/2013–04/2020 **Co-PI on Microsoft Everest Expedition** funded by MSR-Inria Joint Centre on *Provably Secure Communication Software*

07/2016 **PI of QuickChick Young Researcher grant (JCJC)** from the French National Research Agency (ANR) on *Property-based Testing for Coq* (14.2% acceptance rate, declined in favor of ERC Starting Grant)

Awards

05/2021 **Distinguished Paper Award** at CSF 2021 for "SSProve: A Foundational Framework for Modular Cryptographic Proofs in Coq"

04/2020 **Nominated for EATCS Award** for the best ETAPS paper in theoretical computer science for "Trace-Relating Compiler Correctness and Secure Compilation"

05/2019	**Distinguished Paper Award** at CSF 2019 for "Journey Beyond Full Abstraction"
03/2016	**Inria Award for PhD Supervising and for Research** (PEDR)
02/2008	**Günter Hotz Medal** for outstanding CS graduates, Alumni organization of Saarland University

Fellowships

03/2007–04/2011	**Ph.D. fellowship** from Microsoft Research Cambridge (UK) and the the International Max Planck Research School for Computer Science (IMPRS-CS)

Current Research Group

10/2021–now	Cezar-Constantin Andrici (PhD student, MPI-SP)
02/2018–now	Jérémy Thibault (PhD student, MPI-SP)
02/2023–now	Maxi Wuttke (PhD student, MPI-SP)
01/2018–now	Roberto Blanco (Postdoctoral Researcher, MPI-SP)
03/2023–now	Dongjae Lee (Research Intern, MPI-SP)
04/2017–now	Guido Martínez (Co-Supervised PhD Student, NU Rosario)

Previous Group Members

12/2017–04/2022	Carmine Abate (**Graduated PhD student**, MPI-SP)
01/2018–09/2022	Théo Winterhalter (Postdoctoral Researcher, MPI-SP)
07/2022–09/2022	Aïna Linn Georges (Research Intern, MPI-SP)
09/2019–10/2021	Adrien Durier (Postdoctoral Researcher, Inria Paris, then MPI-SP)
03/2019–04/2020	Exequiel Rivas (Starting Researcher Position, Inria Paris)
09/2016–11/2019	Kenji Maillard (**Graduated PhD student**, ENS Paris)
05/2019–04/2020	Antoine Van Muylder (Research Intern, Inria Paris)
07/2018–04/2020	Théo Laurent (Research Intern / Engineer, Inria Paris)
07/2018–12/2019	Éric Tanter (Visiting Professor, University of Chile)
07/2019–04/2020	Ramkumar Ramachandra (Research Engineer, Inria Paris)
04/2018–10/2019	Florian Groult (Research Intern / Engineer)
09/2018–01/2019	Elizabeth Labrada (Research Intern, University of Chile)
01/2017–11/2018	Victor Dumitrescu (Research Engineer, MSR-Inria)
04/2017–09/2018	Danel Ahman (Postdoctoral Researcher)
08/2011–10/2017	Arthur Azevedo de Amorim (**Graduated PhD student**, University of Pennsylvania, co-supervised with Benjamin C. Pierce)
09/2017–07/2018	Amal Ahmed (Visiting Professor, Northeastern University)
09/2017–07/2018	Aaron Weiss (Visiting PhD Researcher, Northeastern University)
01–12/2017	Marco Stronati (Postdoctoral Researcher)
01–12/2017	Guglielmo Fachini (Research Engineer)

10–12/2017	William J. Bowman (Research Intern, Northeastern University)
07–10/2017	Clément Pit-Claudel (Research Intern, MIT)
01–07/2017	Tomer Libal (Research Engineer, MSR-Inria)
05–07/2017	Ana Nora Evans (Visiting PhD Researcher, University of Virginia)
03/2015–09/2016	Yannis Juglaret (Student, Université Paris Diderot – Paris 7)
2008–2016	Supervised 12 MSc internships/theses, 10 of which have already resulted in research papers published at good conferences. 10 of the students continued with a PhD (2× Princeton, 1× UPenn, 1× Inria Paris, 1× École Polytechnique, 1× Université Paris-Sud, 1× IST Vienna, 1× IMDEA, 1× MPI-INF Saarbrücken, 1× NU Rosario).

Publications

Conferences

[1] Akram El-Korashy, Roberto Blanco, Jérémy Thibault, Adrien Durier, Deepak Garg, and Cătălin Hriţcu. SecurePtrs: Proving secure compilation with data-flow back-translation and turn-taking simulation. In *35th IEEE Computer Security Foundations Symposium, (CSF)*, August 2022. (Acceptance rate: 32/165=19.4).

[2] Carmine Abate, Philipp G. Haselwarter, Exequiel Rivas, Antoine Van Muylder, Théo Winterhalter, Cătălin Hriţcu, Kenji Maillard, and Bas Spitters. SSProve: A foundational framework for modular cryptographic proofs in Coq. In *34th IEEE Computer Security Foundations Symposium (CSF)*, pages 608–622. IEEE, 2021. (Acceptance rate: 43/172=0.25).

[3] Maximilian Algehed, Jean-Philippe Bernardy, and Cătălin Hriţcu. Dynamic IFC theorems for free! In *34th IEEE Computer Security Foundations Symposium, (CSF)*, pages 1–14. IEEE, 2021. (Acceptance rate: 43/172=0.25).

[4] Carmine Abate, Roberto Blanco, Ştefan Ciobâcă, Deepak Garg, Cătălin Hriţcu, Marco Patrignani, Éric Tanter, and Jérémy Thibault. Trace-relating compiler correctness and secure compilation. In *29th European Symposium on Programming (ESOP)*, pages 1–28. Springer, April 2020. (Acceptance rate: 27/87=0.31).

[5] Kenji Maillard, Cătălin Hriţcu, Exequiel Rivas, and Antoine Van Muylder. The next 700 relational program logics. *PACMPL*, 4(POPL):4:1–4:33, 2020.

[6] Kenji Maillard, Danel Ahman, Robert Atkey, Guido Martínez, Cătălin Hriţcu, Exequiel Rivas, and Éric Tanter. Dijkstra monads for all. *PACMPL*, 3(ICFP):104:1–104:29, 2019.

[7] Carmine Abate, Roberto Blanco, Deepak Garg, Cătălin Hriţcu, Marco Patrignani, and Jérémy Thibault. Journey beyond full abstraction: Exploring robust property preservation for secure compilation. In *32nd IEEE Computer Security Foundations Symposium (CSF)*, pages 256–271. IEEE, June 2019. (Acceptance rate: 30/89=0.34).

[8] Guido Martínez, Danel Ahman, Victor Dumitrescu, Nick Giannarakis, Chris Hawblitzel, Cătălin Hriţcu, Monal Narasimhamurthy, Zoe Paraskevopoulou, Clément Pit-Claudel, Jonathan Protzenko, Tahina Ramananandro, Aseem Rastogi, and Nikhil Swamy. Meta-F*: Proof automation with SMT, tactics, and metaprograms. In *28th European Symposium on Programming (ESOP)*, pages 30–59. Springer, April 2019. (Acceptance rate: 28/86=0.33).

[9] Carmine Abate, Arthur Azevedo de Amorim, Roberto Blanco, Ana Nora Evans, Guglielmo Fachini, Cătălin Hriţcu, Théo Laurent, Benjamin C. Pierce, Marco Stronati, and Andrew Tolmach. When good components go bad: Formally secure compilation despite dynamic compromise. In *25th ACM Conference on Computer*

and Communications Security (CCS), pages 1351–1368. ACM, October 2018. (Acceptance rate: 134/809=0.17).

[10] Arthur Azevedo de Amorim, Cătălin Hriţcu, and Benjamin C. Pierce. The meaning of memory safety. In *7th International Conference on Principles of Security and Trust (POST)*, pages 79–105, April 2018. (Acceptance rate: 14/45=0.31).

[11] Danel Ahman, Cédric Fournet, Cătălin Hriţcu, Kenji Maillard, Aseem Rastogi, and Nikhil Swamy. Recalling a witness: Foundations and applications of monotonic state. *PACMPL*, 2(POPL):65:1–65:30, January 2018.

[12] Niklas Grimm, Kenji Maillard, Cédric Fournet, Cătălin Hriţcu, Matteo Maffei, Jonathan Protzenko, Tahina Ramananandro, Aseem Rastogi, Nikhil Swamy, and Santiago Zanella-Béguelin. A monadic framework for relational verification: Applied to information security, program equivalence, and optimizations. In *7th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP)*, pages 130–145. ACM, January 2018. (Acceptance rate: 22/51=0.43).

[13] Jonathan Protzenko, Jean-Karim Zinzindohoué, Aseem Rastogi, Tahina Ramananandro, Peng Wang, Santiago Zanella-Béguelin, Antoine Delignat-Lavaud, Cătălin Hriţcu, Karthikeyan Bhargavan, Cédric Fournet, and Nikhil Swamy. Verified low-level programming embedded in F*. *PACMPL*, 1(ICFP):17:1–17:29, September 2017.

[14] Karthikeyan Bhargavan, Barry Bond, Antoine Delignat-Lavaud, Cédric Fournet, Chris Hawblitzel, Cătălin Hriţcu, 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, Perry Wang, Santiago Zanella-Béguelin, and Jean-Karim Zinzindohoué. Everest: Towards a verified, drop-in replacement of HTTPS. In *2nd Summit on Advances in Programming Languages (SNAPL)*, May 2017. (Acceptance rate: 18/28=0.64).

[15] Danel Ahman, Cătălin Hriţcu, Kenji Maillard, Guido Martínez, Gordon Plotkin, Jonathan Protzenko, Aseem Rastogi, and Nikhil Swamy. Dijkstra monads for free. In *44th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL)*, pages 515–529. ACM, January 2017. (Acceptance rate: 64/279=0.23).

[16] Leonidas Lampropoulos, Diane Gallois-Wong, Cătălin Hriţcu, John Hughes, Benjamin C. Pierce, and Li-yao Xia. Beginner's Luck: A language for random generators. In *44th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL)*, pages 114–129. ACM, January 2017. (Acceptance rate: 64/279=0.23).

[17] Yannis Juglaret, Cătălin Hriţcu, Arthur Azevedo de Amorim, Boris Eng, and Benjamin C. Pierce. Beyond good and evil: Formalizing the security guarantees of compartmentalizing compilation. In *29th IEEE Symposium on Computer Security Foundations (CSF)*, pages 45–60. IEEE, July 2016. (Acceptance rate: 31/87=0.36).

[18] Nikhil Swamy, Cătălin Hriţcu, Chantal Keller, Aseem Rastogi, Antoine Delignat-Lavaud, Simon Forest, Karthikeyan Bhargavan, Cédric Fournet, Pierre-Yves Strub, Markulf Kohlweiss, Jean-Karim Zinzindohoue, and Santiago Zanella-Béguelin. Dependent types and multi-monadic effects in F*. In *43rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 256–270. ACM, January 2016. (Acceptance rate: 59/253=0.23).

[19] Zoe Paraskevopoulou, Cătălin Hriţcu, Maxime Dénès, Leonidas Lampropoulos, and Benjamin C. Pierce. Foundational property-based testing. In *6th International Conference on Interactive Theorem Proving (ITP)*, volume 9236 of *Lecture Notes in Computer Science*, pages 325–343. Springer, 2015. (Acceptance rate: 30/54=0.55).

[20] Arthur Azevedo de Amorim, Maxime Dénès, Nick Giannarakis, Cătălin Hriţcu, Benjamin C. Pierce, Antal Spector-Zabusky, and Andrew Tolmach. Micro-Policies: Formally verified, tag-based security monitors. In *36th IEEE Symposium on Security and Privacy (Oakland S&P)*, pages 813–830. IEEE Computer Society, May 2015. (Acceptance rate: 55/420=0.13).

[21] Udit Dhawan, Cătălin Hriţcu, Rafi Rubin, Nikos Vasilakis, Silviu Chiricescu, Jonathan M. Smith, Thomas F. Knight, Jr., Benjamin C. Pierce, and André DeHon. Architectural support for software-defined metadata processing. In *20th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, pages 487–502. ACM, March 2015. (Acceptance rate: 48/287=0.17).

[22] Arthur Azevedo de Amorim, Nathan Collins, André DeHon, Delphine Demange, Cătălin Hriţcu, David Pichardie, Benjamin C. Pierce, Randy Pollack, and Andrew Tolmach. A verified information-flow architecture. In *41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 165–178. ACM, January 2014. (Acceptance rate: 51/220=0.23).

[23] Cătălin Hriţcu, John Hughes, Benjamin C. Pierce, Antal Spector-Zabusky, Dimitrios Vytiniotis, Arthur Azevedo de Amorim, and Leonidas Lampropoulos. Testing noninterference, quickly. In *18th ACM SIGPLAN International Conference on Functional Programming (ICFP)*, pages 455–468. ACM, September 2013. (Acceptance rate: 40/133=0.30).

[24] Cătălin Hriţcu, Michael Greenberg, Ben Karel, Benjamin C. Pierce, and Greg Morrisett. All your IFCException are belong to us. In *34th IEEE Symposium on Security and Privacy (Oakland S&P)*, pages 3–17. IEEE, May 2013. (Acceptance rate: 38/315=0.12).

[25] Michael Backes, Alex Busenius, and Cătălin Hriţcu. On the development and formalization of an extensible code generator for real life security protocols. In *4th NASA Formal Methods Symposium (NFM)*, pages 371–387. Springer, April 2012. (Acceptance rate: 36/93=0.39).

[26] Michael Backes, Cătălin Hriţcu, and Thorsten Tarrach. Automatically verifying typing constraints for a data processing language. In *First International Conference on Certified Programs and Proofs (CPP 2011)*, pages 296–313. Springer, December 2011. (Acceptance rate: 24/49=0.49).

[27] Michael Backes, Cătălin Hriţcu, and Matteo Maffei. Union and intersection types for secure protocol implementations. In *Theory of Security and Applications (TOSCA 2011; part of ETAPS and the precursor of POST)*, pages 1–28. Springer, March 2011. Invited paper.

[28] Gavin M. Bierman, Andrew D. Gordon, Cătălin Hriţcu, and David Langworthy. Semantic subtyping with an SMT solver. In *15th ACM SIGPLAN International Conference on Functional programming (ICFP 2010)*, pages 105–116. ACM Press, September 2010. (Acceptance rate: 30/99=0.30).

[29] Michael Backes, Martin P. Grochulla, Cătălin Hriţcu, and Matteo Maffei. Achieving security despite compromise using zero-knowledge. In *22th IEEE Symposium on Computer Security Foundations (CSF 2009)*, pages 308–323. IEEE, July 2009. (Acceptance rate: 22/93=0.24).

[30] Michael Backes, Cătălin Hriţcu, and Matteo Maffei. Type-checking zero-knowledge. In *15th ACM Conference on Computer and Communications Security (CCS 2008)*, pages 357–370. ACM Press, October 2008. (Acceptance rate: 51/281=0.18).

[31] Michael Backes, Cătălin Hriţcu, and Matteo Maffei. Automated verification of remote electronic voting protocols in the applied pi-calculus. In *21th IEEE Symposium on Computer Security Foundations (CSF 2008)*, pages 195–209. IEEE, June 2008. (Acceptance rate: 21/115=0.18).

Journals

[32] Philipp G. Haselwarter, Exequiel Rivas, Antoine Van Muylder, Théo Winterhalter, Carmine Abate, Nikolaj Sidorenco, Cătălin Hriţcu, Kenji Maillard, and Bas Spitters. SSProve: A foundational framework for modular cryptographic proofs in Coq. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, January 2023. To appear.

[33] Carmine Abate, Roberto Blanco, Ştefan Ciobâcă, Adrien Durier, Deepak Garg, Catalin Hritcu, Marco Patrignani, Éric Tanter, and Jérémy Thibault. An extended account of trace-relating compiler correctness and secure compilation. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 43(4):14:1–14:48, 2021.

[34] Arthur Azevedo de Amorim, Nathan Collins, André DeHon, Delphine Demange, Cătălin Hriţcu, David Pichardie, Benjamin C. Pierce, Randy Pollack, and Andrew Tolmach. A verified information-flow architecture. *Journal of Computer Security (JCS); Special Issue on Verified Information Flow Security*, 24(6):689–734, December 2016.

[35] Cătălin Hriţcu, Leonidas Lampropoulos, Antal Spector-Zabusky, Arthur Azevedo de Amorim, Maxime Dénès, John Hughes, Benjamin C. Pierce, and Dimitrios Vytiniotis. Testing noninterference, quickly. *Journal of Functional Programming (JFP); Special issue for ICFP 2013*, 26:e4 (62 pages), April 2016.

[36] Michael Backes, Cătălin Hriţcu, and Matteo Maffei. Union, intersection, and refinement types and reasoning about type disjointness for secure protocol implementations. *Journal of Computer Security (JCS); Special Issue on Foundational Aspects of Security*, 22(2):301–353, February 2014.

[37] Gavin M. Bierman, Andrew D. Gordon, Cătălin Hriţcu, and David Langworthy. Semantic subtyping with an SMT solver. *Journal of Functional Programming (JFP)*, 22(1):31–105, March 2012.

[38] Cătălin Hriţcu and Jan Schwinghammer. A step-indexed semantics of imperative objects. *Logical Methods in Computer Science (LMCS)*, 5(4:2):1–48, December 2009.

Books

[39] Benjamin C. Pierce, Arthur Azevedo de Amorim, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, and Brent Yorgey. *Software Foundations: Logical Foundations*. Electronic textbook, August 2018.

[40] Benjamin C. Pierce, Arthur Azevedo de Amorim, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, Andrew Tolmach, and Brent Yorgey. *Software Foundations: Programming Language Foundations*. Electronic textbook, August 2018.

Chapter

[41] Leonidas Lampropoulos, Diane Gallois-Wong, Cătălin Hriţcu, John Hughes, Benjamin C. Pierce, and Li-yao Xia. *Luck: A Probabilistic Language for Testing*, chapter 13, pages 449–488. Cambridge University Press, November 2020.

Editor

[42] David Chisnall, Deepak Garg, Catalin Hritcu, and Mathias Payer. Secure Compilation (Dagstuhl Seminar 21481). *Dagstuhl Reports*, 11(10):173–204, 2021.

[43] Cătălin Hriţcu and Andrei Popescu, editors. *Proceedings of the 10th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2021, Virtual Event, Denmark, January 17-19, 2021*. ACM, 2021.

[44] Jasmin Blanchette and Cătălin Hriţcu, editors. *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, New Orleans, LA, USA, January 20-21, 2020*. ACM, 2020.

[45] Amal Ahmed, Deepak Garg, Cătălin Hriţcu, and Frank Piessens. Secure Compilation (Dagstuhl Seminar 18201). *Dagstuhl Reports*, 8(5):1–30, 2018.

Theses

[46] Cătălin Hriţcu. *The Quest for Formally Secure Compartmentalizing Compilation*. Habilitation thesis, ENS Paris; PSL Research University, January 2019.

[47] Cătălin Hriţcu. *Union, Intersection, and Refinement Types and Reasoning About Type Disjointness for Security Protocol Analysis*. PhD thesis, Saarland University, January 2012.

[48] Cătălin Hriţcu. A step-indexed semantic model of types for the functional object calculus. Master's thesis, Saarland University, May 2007.

Informal

[49] Cezar-Constantin Andrici, Cătălin Hriţcu, Guido Martínez, Exequiel Rivas, and Théo Winterhalter. Securely compiling verified F* programs with IO. Draft. Submitted to ICFP'23, March 2023.

[50] Philipp G. Haselwarter, Benjamin Salling Hvass, Lasse Letager Hansen, Théo Winterhalter, Cătălin Hriţcu, and Bas Spitters. The last yard: Foundational end-to-end verification of high-speed cryptography. Draft. Submitted to CSF'23, February 2023.

[51] Jérémy Thibault, Arthur Azevedo de Amorim, Roberto Blanco, Aïna Linn Georges, Cătălin Hriţcu, and Andrew Tolmach. SECOMP2CHERI: Securely compiling compartments from CompCert C to a capability machine. Extended Abstract at Workshop on Principles of Secure Compilation (PriSC), January 2023.

[52] Théo Winterhalter, Cezar-Constantin Andrici, Cătălin Hriţcu, Kenji Maillard, Guido Martínez, and Exequiel Rivas. Partial Dijkstra monads for all. Extended abstract of presentation at the 28th International Conference on Types for Proofs and Programs (TYPES), June 2022.

[53] Cezar-Constantin Andrici, Théo Winterhalter, Cătălin Hriţcu, and Exequiel Rivas. Verifying non-terminating programs with IO in F*. Presentation at the 10th ACM SIGPLAN Workshop on Higher-Order Programming with Effects (HOPE), September 2022.

[54] Jérémy Thibault and Cătălin Hriţcu. Nanopass back-translation of multiple traces for secure compilation proofs. PriSC, January 2021.

[55] Alejandro Aguirre, Cătălin Hriţcu, Chantal Keller, and Nikhil Swamy. From F* to SMT (extended abstract). Talk at 1st International Workshop on Hammers for Type Theories (HaTT), July 2016.

[56] Udit Dhawan, Albert Kwon, Edin Kadric, Cătălin Hriţcu, Benjamin C. Pierce, Jonathan M. Smith, Gregory Malecha, Greg Morrisett, Thomas F. Knight, Jr., Andrew Sutherland, Tom Hawkins, Amanda Zyxnfryx, David Wittenberg, Peter Trei, Sumit Ray, Greg Sullivan, and André DeHon. Hardware support for safety interlocks and introspection. In *SASO Workshop on Adaptive Host and Network Security*, September 2012.

Research Prototypes / Software Tools

2015 – now **SECOMP**: Formally secure prototype compiler chains to a tagged architecture

2014 – now **F***: Program verification system for ML and C programs

2013 – now **Micro-Policies**: Formally verified, tag-based security monitors

2013 – 2016 **QuickChick**: Foundational property-based testing plugin for Coq

2014 – 2016 **Luck**: Domain-specific language for property-based generators for random testing

2011 – 2012 **Breeze**: Language with dynamic information-flow control and label-based access control

2011 – 2013 **CRASH/SAFE**: clean-slate co-design of a secure architecture, including novel hardware, OS, and programming language

2010 – 2011 **DVerify**: Verification tool for the data processing language that served as the main starting point for the query language of Microsoft Power Query for Excel

2009 – 2010 **Dminor**: Type-checker based on semantic subtyping for this data processing language

2009 – 2011 **F5**: Type-checker for concurrent language with refinement, union, and intersection types

2008 – 2011 **Expi2Java**: Turns verifiable protocol models into interoperable Java implementations

2008 – 2011 **zk-typechecker**: First type-checker for protocols that use zero-knowledge proofs

Community Service

PC chair:

- 10th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2021)
- 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)
- 2nd Workshop on Principles of Secure Compilation (PriSC 2018)

Steering committees:

- **SC Chair** for ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP) since 2021
- **SC Chair** for Workshop on Principles of Secure Compilation (PriSC) since 2019

PC member for conferences:

- 51st ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2024)
- 42nd IEEE Symposium on Security and Privacy (Oakland S&P 2021)
- 34rd IEEE Computer Security Foundations Symposium (CSF 2021)
- 33rd IEEE Computer Security Foundations Symposium (CSF 2020)
- 19th International Conference on Runtime Verification (RV 2019)
- 4th IEEE Cybersecurity Development Conference (SecDev 2019)
- 25th ACM Conference on Computer and Communications Security (CCS 2018)
- 3rd IEEE European Symposium on Security and Privacy (EuroS&P 2018)
- 26th European Symposium on Programming (ESOP 2018)
- 44th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2017)
- 6th International Conference on Principles of Security and Trust (POST 2017)
- 29th IEEE Computer Security Foundations Symposium (CSF 2016)
- 7th International Conference on Interactive Theorem Proving (ITP 2016)

- 4th ACM-SIGPLAN Conference on Certified Programs and Proofs (CPP 2016)

PC member for workshops:

- 1st Workshop on Type-Directed Programming (TyDe 2016)
- 1st International Workshop on Hammers for Type Theories (HaTT 2016)
- Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography (FCS-FCC 2014)
- 10th Workshop on Foundations of Computer Security (FCS 2013)

Reviewer for grants: ERC in 2022, DFG in 2020

Reviewer for journals:
JACM (×1), JCS (×4), TOPLAS (×4), JFP (×2), JAR (×1), HOSC (×1), JLAMP (×1)

Organization

- Test-of-Time Awards Chair for IEEE Computer Security Foundations Symposium (CSF) in 2023 and 2024
- **Conference Chair** for 10th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2021)
- **General Chair** for 2nd IEEE European Symposium on Security and Privacy (EuroS&P 2017) (26-28 April 2017, Paris; 250 registered participants)
- Main organizer of 2 Dagstuhl Seminars on Secure Compilation (May 2018 and December 2021)
- Artifact Evaluation Co-Chair for Principles of Programming Languages (POPL 2018 and POPL 2019)
- Co-Organizer of ESOP Program Committee Workshop at Inria Paris (December 2017, approx 40 participants)
- Organizer of Everest workshop at Inria Paris (October 2017, approx 40 participants)
- Main organizer of the Joint EasyCrypt-F⋆-CryptoVerif School 2014 in Paris (80+ participants)

PhD thesis reviewer

- Matteo Busi, Secure Compilation All the Way Down, University of Pisa, Italy, 2021.
- Liam O'Connor, Type systems for system types, University of New South Wales, Kensington, Australia, 2019.

PhD defense committee

- Alejandro Aguirre, Relational logics for higher-order effectful programs, Universidad Politécnica de Madrid, Spain, 2021.
- Arthur Azevedo de Amorim, A Methodology for Micro-Policies, University of Pennsylvania, USA, 2017.

PhD follow-up committee (fr. comité suivi doctoral)

- Meven Bertrand, Effects in Type Theory, Gallinette Team, Inria, Nantes.
- Balthazar Bauer, Transferable Electronic Currencies, ENS Paris.
- Michele Orrù, Multi-Party Computation and Zero-Knowledge Proofs, ENS Paris.
- Cyprien Mangin, Higher-Dimensional Dependent Pattern Matching, PiR2 team, Inria Paris.
- Thomas Williams, A Principled Approach to Ornamentation in ML, Gallium team, Inria Paris.

Teaching

- Upcoming: *Proofs are Programs* course at Ruhr University Bochum, 6 March–13 July, 2023
- *Writing and Verifying Functional Programs in Coq* course at Summer School on Cryptography, Blockchain, and Program Verification, Mathinfoly 2019, 24-31 August 2019 at INSA, Lyon, France (3 full days)
- *Program Verification in F** course at Université de la Grande Région Summer School on Verification Technology, Systems & Applications (VTSA 2019), 1-5 July 2019, Luxembourg (6h)
- *Formally Secure Compartmentalizing Compilation* course at International School on Foundations of Security Analysis and Design (FOSAD), 27-28 August, 2018, Bertinoro, Italy (6h)
- *Program Verification in F** course at EPIT 2018 Software Verification Spring School, 7-11 May 2018, Aussois, France (4.5h)
- *Verifying Cryptographic Implementations with F** course at Computer-aided security proofs summer school. Aarhus, Denmark, October, 2017 (4h)
- *Verifying Cryptographic Implementations with F** course at Models and Tools for Cryptographic Proofs summer school, Nancy, France, July 2017 (4h30min)
- *Program Verification with F** part of *Cryptographic protocols: formal and computational proofs* course at **Parisian Master of Research in Computer Science (MPRI)**, lecturer for 1/4 of the course, Winter 2016/2017 (12h)
- *Verifying Cryptographic Protocol Implementations with F** course at *Computer Aided Analysis of Cryptographic Protocols* summer school, Bucharest, September 2016 (2h)
- *F* Tutorials* at POPL 2015 (3h), ICFP 2015 (3h30min), and the Joint EasyCrypt-F*-CryptoVerif School 2014 (3h).
- *F* Course: Type Systems for Security Verification*, Advanced Block Lecture, Saarland University, together with Matteo Maffei, March 2015 (**main lecturer**, 6 lectures and 6 tutorial sessions, 24h)
- *Advanced Martial Arts in Coq*, CIS 670, University of Pennsylvania, Benjamin C. Pierce, Fall 2012 (guest lecturer for 2 lectures / 3h).
- *Software Foundations*, CIS 500, University of Pennsylvania, Benjamin C. Pierce, Spring 2012 (teaching assistant – 31h of office hours; guest lecturer for 6 lectures / 9h; **book co-author**).
- *Advanced Topics in Programming Languages*, CIS 670, UPenn, Benjamin C. Pierce, Fall 2011 (guest lecturer for 2 lectures / 3h).
- *Security*, Core Lecture, Saarland University, Michael Backes, Winter 2010–2011 (guest lecturer for 1 lecture / 1h45min).
- *Practical Aspects of Security*, Advanced Lecture, Saarland University, Michael Backes, 2009 (teaching assistant – 14h of office hours; guest lecturer for 3 lectures / 6h25min; **best course award**).
- *Observational Equivalence for Security Protocols*, Saarland University, Michael Backes, Winter 2008–2009 (seminar organizer and student adviser).
- *The Analysis of Electronic Voting Protocols* and *The Secure Implementation of Cryptographic Protocols*, Saarland University, Michael Backes, Winter 2007–2008 (seminar organizer and student adviser).
- *Introduction to Computational Logic* Core Lecture, Saarland University, Gert Smolka, Summer 2007 (teaching assistant – 33h of recitation sections / tutorials and office hours).
- *Language-based Security* Advanced Lecture, Saarland University, Matteo Maffei, Winter 2006–2007 (teaching assistant – 38h of recitation sections / tutorials and office hours).

Languages

English (proficient, C2), German (intermediate, B1.2–B2), French (intermediate, B1.2–B2), Italian (elementary, A1–A2), Romanian (native)

Hobbies

Biking, Running (10-15 km), Soccer, Cooking, Reading, Basketball, Hiking

April 3, 2023