Cătălin Hriţcu

Curriculum Vitae

Contact

Inria Prosecco, 2 rue Simone Iff, 75012 Paris, France

catalin.hritcu@gmail.com   http://prosecco.gforge.inria.fr/personal/hritcu/

Education

06/2007–01/2012	**Ph.D.** in Computer Science from Saarland University, **Summa cum Laude**, Advisors: Michael Backes (official supervisor), Matteo Maffei, and Andrew D. Gordon
10/2005–05/2007	**M.Sc.** in Computer Science from Saarland University, Saarbrücken, Germany, **Honors degree**, Thesis advisors: Gert Smolka and Jan Schwinghammer
09/2001–06/2005	**Licentiate** (4 years undergrad degree) in Computer Science from "Alexandru Ioan Cuza" University, Iaşi, Romania, **Honors degree**

Positions

10/2013–now	**Researcher** (chargé de recherche; tenured) at **Inria Paris** in the Prosecco team
09–10/2016	**Visiting Researcher** at **Microsoft Research Redmond**
05/2011–09/2013	**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

01/2017–now	**PI of SECOMP ERC Starting Grant** from the European Research Council on *Efficient Formally Secure Compilers to a Tagged Architecture*
12/2017–now	**Co-PI of DARPA SSITH/HOPE grant** on *Advanced New Hardware Optimized for Policy Enforcement, A New HOPE"*
2016–now	**Co-PI on Project Everest** funded by Microsoft Research via MPI-Inria Joint Centre on *Verified Secure Implementations of the HTTPS Ecosystem*
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 grant)

Awards

03/2016	**Inria Award for PhD Supervising and for Research** (PEDR)

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

09/2016–now	Kenji Maillard (PhD student, ENS Paris)
04/2017–now	Guido Martínez (Co-Supervised PhD Student, NU Rosario)

04/2017–now	Danel Ahman (Postdoctoral Researcher)
01/2018–now	Roberto Blanco (Postdoctoral Researcher)
01/2017–now	Victor Dumitrescu (Research Engineer)
12/2017–now	Carmine Abate (Research Intern, University of Trento)
02/2018–now	Jérémy Thibault (Research Intern, ENS Rennes)
09/2017–now	Amal Ahmed (Visiting Professor, Northeastern University)
09/2017–now	Aaron Weiss (Visiting PhD Researcher, Northeastern University)

Previous Group Members

08/2011–10/2017	Arthur Azevedo de Amorim (Graduated PhD student, University of Pennsylvania, co-supervised with Benjamin C. Pierce)
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)
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).

New Group Members Starting Soon

07/2018–02/2019	Éric Tanter (Visiting Professor, University of Chile)
04–10/2018	Florian Groult (Research Intern, Orléans University)
09/2018–01/2019	Elizabeth Labrada (Research Intern, University of Chile)

Publications

Conferences   [1] Arthur Azevedo de Amorim, Cătălin Hriţcu, and Benjamin C. Pierce. The meaning of memory safety. Accepted at 7th International Conference on Principles of Security and Trust (POST), April 2018.

[2] 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.

[3] 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).

[4] 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.

[5] 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).

[6] 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).

[7] 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).

[8] 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 Computer Society Press, July 2016. (Acceptance rate: 31/87=0.36).

[9] 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).

[10] 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).

[11] 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).

[12] 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).

[13] 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).

[14] 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).

[15] 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 Computer Society Press, May 2013. (Acceptance rate: 38/315=0.12).

[16] 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).

[17] 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).

[18] 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.

[19] 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).

[20] 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 Computer Society Press, July 2009. (Acceptance rate: 22/93=0.24).

[21] 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).

[22] 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 Computer Society Press, June 2008. (Acceptance rate: 21/115=0.18).

Journals

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

Book   [28] Benjamin C. Pierce, Arthur Azevedo de Amorim, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, and Brent Yorgey. *Software Foundations*. Electronic textbook, May 2017.

PhD Thesis   [29] Cătălin Hriţcu. *Union, Intersection, and Refinement Types and Reasoning About Type Disjointness for Security Protocol Analysis*. PhD thesis, Saarland University, January 2012.

Informal   [30] 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, and Nikhil Swamy. Meta-f*: Metaprogramming and tactics in an effectful program verifier. arXiv, March 2018.

[31] Guglielmo Fachini, Cătălin Hriţcu, Marco Stronati, Arthur Azevedo de Amorim, Ana Nora Evans, Carmine Abate, Roberto Blanco, Théo Laurent, Benjamin C. Pierce, and Andrew Tolmach. When good components go bad: Formally secure compilation despite dynamic compromise. arXiv:1802.00588, February 2018.

[32] Deepak Garg, Cătălin Hriţcu, Marco Patrignani, Marco Stronati, and David Swasey. Robust hyperproperty preservation for secure compilation (extended abstract). arXiv:1710.07309, October 2017.

[33] 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.

[34] Yannis Juglaret, Cătălin Hriţcu, Arthur Azevedo de Amorim, Benjamin C. Pierce, Antal Spector-Zabusky, and Andrew Tolmach. Towards a fully abstract compiler using Micro-Policies: Secure compilation for mutually distrustful components. Technical Report, arXiv:1510.00697, October 2015.

[35] 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 compilers 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

Organization

- **General Chair** of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P 2017) (26-28 April 2017, Paris, France; 250 registered participants)

- Main organizer of Dagstuhl Seminar 18201 on Secure Compilation (May 13-18, 2018)

- Artifact Evaluation Co-Chair for Principles of Programming Languages (POPL 2018 and 2019)

- Main organizer of the Workshop on Principles of Secure Compilation (PriSC) at POPL (# of registered participants: 31 in 2017 and 40 in 2018)

- 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)

PC member for conferences:

- 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:

- **Program Chair** for 2nd Workshop on Principles of Secure Compilation (PriSC 2018)

- 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 journals:
JACM ($\times$1), JCS ($\times$4), TOPLAS ($\times$3), JFP ($\times$2), HOSC ($\times$1), JLAMP ($\times$1)

Recent Talks

- *Formally Secure Compilation of Unsafe Low-level Components*

02/2018   IRIF, Paris 7

02/2018   SoSySec seminar on Software and Systems Security at IRISA, Rennes

01/2018   Workshop on Principles of Secure Compilation (PriSC'18) at POPL'19

12/2017   Al. I. Cuza University of Iasi

12/2017   ESOP PC Workshop at Inria Paris

01/2018 *Program Chair's Welcome Message* at Workshop on Principles of Secure Compilation (PriSC'18)

10/2017 *What's new in F*?* at Everest Workshop at Inria Paris

- *Verified Effectful Programming in F**

06/2017   **Invited Keynote Talk** at Trends in Functional Programming (TFP)

06/2017   Inria Prosecco Seminar

06/2017 *Presentation of Inria Prosecco team* at French-American Doctoral Exchange Program 2017: Cybersecurity

04/2017 *General Chair's Welcome Message* for European Symposium on Security and Privacy, EuroS&P 2017

- *Efficient Formally Secure Compilers to a Tagged Architecture*

04/2017   Université Clermont Auvergne

03/2017   LRI VALS seminar at University Paris-Sud

12/2016   CEA List seminar

11/2016   Microsoft Research Redmond security seminar

09/2016   Inria Gallium seminar

08/2016   Secure compilation meeting at Inria Paris

05/2016   ERC Starting Grant interview

03/2016   Inria Prosecco Seminar

02/2016   MPI-SWS Colloquium, Saarbrücken

01/2017 *What is secure compilation?* Short talk at Secure Compilation Meeting at POPL'17

- *Dependent Types and Multi-Monadic Effects in F**

03/2016   Dagstuhl Seminar 16131 on Language Based Verification Tools for Functional Programs

09/2015   ML Workshop at ICFP

- *Secure Software Systems by Formal Verification, Testing, Secure Compilation, and Dynamic Monitoring*

12/2015   **Invited Vision Talk** at Scientific Committee meeting of Nokia's Bell Labs – Inria common lab

- *Micro-Policies: Formally Verified, Tag-Based Security Monitors*

08/2015   Microsoft Research Redmond

07/2015   **Invited Keynote Talk** at Workshop on Programming Languages and Analysis for Security (PLAS)

06/2015   Inria Rennes – DGA Seminar on Formal Methods and Security

05/2015   HP Labs - Inria seminar in Paris

03/2015   Inria Prosecco team evaluation

07/2014   Joint Workshop on Foundations of Computer Security & Formal and Computational Cryptography

03/2014   Grande Region Security and Reliability Day in Saarbrücken

- *Foundational Property-Based Testing*

08/2015   PLSE seminar ar University of Washington

01/2015   CoqPL Workshop at POPL'15 in Mumbai, India

10/2014   GT LTP of GDR GPL at Paris Sud

- *QuickChick: Property-based testing for Coq*

03/2014   Coq Working Group at PPS, Paris 7

11/2013   Inria Prosecco seminar

Recent Teaching

- *Formally Secure Compilation* course at International School on Foundations of Security Analysis and Design (FOSAD), 27 August - 1 September, 2018, Bertinoro, Italy (4-6h)

- *Program Verification in F** course at EPIT 2018 Software Verification Spring School, planned for 7-11 May 2018, Aussois, France (6-8h)

- *Verifying Cryptographic Implementations with F** 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 $F^\star$* in the Cryptographic Protocols course at Parisian Master of Research in Computer Science (MPRI), Winter 2016/2017 (lecturer for 4 lectures, 3h each)

- *$F^\star$ Introduction* at Cryptographic Protocols summer school, Bucharest, September 2016

- *$F^\star$ Tutorials* at POPL 2015, ICFP 2015, and the Joint EasyCrypt-$F^\star$-CryptoVerif School 2014.

- *$F^\star$ 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).

- *Advanced Martial Arts in Coq*, University of Pennsylvania, Fall 2012 (guest lecturer for 2 lectures).

- *Software Foundations*, University of Pennsylvania, Benjamin C. Pierce, Spring 2012 (teaching assistant and guest lecturer for 6 lectures; **book co-author**).

- *Advanced Topics in Programming Languages*, UPenn, Fall 2011 (guest lecturer for 2 lectures).

- *Practical Aspects of Security*, Advanced Lecture, Saarland University, Michael Backes, 2009 (teaching assistant and guest lecturer for 3 lectures; **best course award**).

Languages

English (proficient, C2), German (upper intermediate, B2),
French (intermediate, B1), Italian (elementary, A2), Romanian (native)

References

Benjamin C. Pierce, Professor at University of Pennsylvania
3330 Walnut Street, Philadelphia, PA 19104, USA; Phone: +1 215 898 6222;
E-mail: bcpierce@cis.upenn.edu

Michael Backes, Professor at Saarland University, Max Planck Fellow at MPI-SWS, Chairman & Scientific Director at CISPA - Helmholtz Center, and Vice-coordinator of MMCI. Postfach 15 11 50, D-66041 Saarbrücken, Germany;
Phone: +49 681 302 3249; E-mail: backes@cispa.saarland

Andrew D. Gordon, Principal Researcher at Microsoft Research Cambridge and Manager of the PPT Group; Professor at University of Edinburgh
21 Station Road, Cambridge CB1 2FB, UK; Phone: +44 1223 479780;
E-mail: adg@microsoft.com

Karthikeyan Bhargavan, Senior Researcher (DR) and leader of the Prosecco team at Inria Paris; 2 rue Simone Iff, Paris 75012, France;
Phone: +33 1 39 63 59 45; E-mail: karthikeyan.bhargavan@inria.fr

Matteo Maffei, Professor at Technische Universität Wien
Favoritenstrasse 9-11, Stiege 2, 1. Stock, A-1040, Wien, Austria;
Phone: +43 (1) 58801 184860; E-mail: matteo.maffei@tuwien.ac.at

Greg Morrisett, Dean of Computing and Information Sciences at Cornell University; 105 Bill and Melinda Gates Hall, Hoy Road, Ithaca, NY 04153, USA;
Phone: +1 607 255-9188; E-mail: greg.morrisett@cornell.edu

March 17, 2018