Vincent Cheval

Centre Inria de Paris,
2 Rue Simone IFF,
75012 Paris
FRANCE
✉ *vincent.cheval@inria.fr*
homepage: https://members.loria.fr/vcheval/

Curriculum Vitae

2020-Present **Researcher**, *Centre Inria de Paris*, Paris, FR.

2015-2020 **Researcher**, *Laboratoire lorrain de recherche en informatique et ses applications, INRIA*, Nancy, FR.

2015 **Lecturer**, *School of Computing, University of Kent*, Canterbury,UK.

2014 **Postdoctoral fellow**, *Laboratoire lorrain de recherche en informatique et ses applications*, Nancy, FR.

2013–2014 **Postdoctoral fellow**, *University of Birmingham*, Birmingham, UK.

2009–2012 **PhD student**, *Laboratoire Spécification et Vérification (LSV), ENS Cachan & CNRS*, Cachan, FR.

"Automatic verification of cryptographic protocols: privacy-type properties"

Co-advisors Hubert Comon-Lundh and Stéphanie Delaune
PhD defence: December 3th , 2012

2006-2009 **Normalien**, *École Normale Supérieure de Cachan*, Cachan.

- **2009:** Master in computer science, *Master Parisien de Recherche en Informatique*, with distinction
- **2007:** Licence in computer science, with high distinction

2003-2006 **Student in preparatory school**, *Lycée Henri Wallon*, Valenciennes.

Research

Topics Automatic verification of cryptographic protocols

- applications: certificate management, RFID protocols, electronic voting, secure emails, cloud computing, etc.
- equivalence properties: anonymity, privacy, unlinkability, strong secrecy, accountability, etc.

Tools Participation to the development of six tools.

- **DeepSecUI (2019-now):** Developer of DeepSec UI (Javascript,Vue.js), a user interface for DeepSec allowing an intuitive display of cryptographic protocols, attacks and allow users to simulate equivalence properties. Url of the tool: `https://github.com/DeepSec-prover/deepsec_ui`
- **DeepSec (2017-now):** Main developer of DeepSec (Ocaml language, around 30000 lines), a state of the art tool for deciding trace equivalence between bounded protocols with cryptographic primitives modeled with a subterm convergent rewrite system. Url of the tool: `https://deepsec-prover.github.io`

- **ProVerif (2012-now):** Participation to the development of an extension of ProVerif (Ocaml language) allowing ProVerif to prove more observational equivalences. Currently main developper of the ongoing evolution of ProVerif. Url of the tool: `http://prosecco.gforge.inria.fr/personal/bblanche/proverif/`
- **GSVerif (2017):** Sole developer of GSVerif (Ocaml language, around 7000 lines), a front-end for the tool ProVerif allowing to efficiently verify stateful protocols. Url of the tool: `https://sites.google.com/site/globalstatesverif/`
- **APTE (2010-2014):** Sole developer of APTE (Ocaml language, around 13000 lines), the first tool that can decide the trace equivalence between protocols possibly non-deterministic, containing possible else branches, and for a bounded number of sessions. Url of the tool: `http://projects.lsv.ens-cachan.fr/APTE/`
- **Adecs (2009-1010):** Sole developer of Adecs (Ocaml language, around 6000 lines), a tool that can decide the symbolic equivalence between two constraint systems. Url of the tool: `http://www.cs.bham.ac.uk/~chevavfp/tools/adecs/`

Publications

International journals with review committee

[J1] Kushal Babel, Vincent Cheval, and Steve Kremer. "On the semantics of communications when verifying equivalence properties". In: *Journal of Computer Security* 28.1 (2020), pages 71–127.

[J2] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. "A procedure for deciding symbolic equivalence between sets of constraint systems". In: *Information and Computation* 255 (2017), pages 94–125.

[J3] Rohit Chadha, Vincent Cheval, Ştefan Ciobâcă, and Steve Kremer. "Automated verification of equivalence properties of cryptographic protocols". In: *ACM Transactions on Computational Logic* 17.4 (2016). **Listed in ACM Computing Reviews' 21st Annual Best of Computing list of notable books and articles for 2016**, pages 1–32.

[J4] Jiangshan Yu, Vincent Cheval, and Mark Ryan. "DTKI: A New Formalized PKI with Verifiable Trusted Parties". In: *The Computer Journal* 59.11 (2016), pages 1695–1713.

[J5] Vincent Cheval, Véronique Cortier, and Stéphanie Delaune. "Deciding equivalence-based properties using constraint solving". In: *Theoretical Computer Science* 492 (June 2013), pages 1–39.

International conferences with review committee

[C1] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. "The hitchhiker's guide to decidability and complexity of equivalence properties in security protocols". In: *Logic, Language, and Security. Essays Dedicated to Andre Scedrov on the Occasion of His 65th Birthday*. Edited by V. Nigam, C. Talcott, J. Guttman, T. Ban Kirigan, S. Kuznetsov, M. Okada, and B. Thau Loo. Volume 12300. Lecture Notes in Computer Science. Springer, 2020.

[C2] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. "Exploiting Symmetries When Proving Equivalence Properties for Security Protocols". In: *Proceedings of the 2019 IEEE ACM SIGSAC Conference on Computer and Communications Security (CCS 2019)*. ACM Press, November 2019, pages 905–922.

[C3] Vincent Cheval, Véronique Cortier, and Mathieu Turuani. "A little more conversation, a little less action, a lot more satisfaction: Global states in ProVerif". In: *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'18)*. Edited by Steve Chong and Stéphanie Delaune. Oxford, UK: IEEE Computer Society Press, July 2018.

[C4] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. "DEEPSEC: Deciding Equivalence Properties in Security Protocols - Theory and Practice". In: *Proceedings of the 39th IEEE Symposium on Security and Privacy (S&P'18)*. **Distinguished paper award**. San Francisco, CA, USA: IEEE Computer Society Press, May 2018.

[C5] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. "The DEEPSEC prover". In: *Proceedings of the 30th International Conference on Computer Aided Verification (CAV'18)*. To appear. Oxford, UK: Springer, July 2018.

[C6] Kushal Babel, Vincent Cheval, and Steve Kremer. "On communication models when verifying equivalence properties". In: *Proceedings of the 6nd International Conference on Principles of Security and Trust (POST'17)*. Volume 10204. Lecture Notes in Computer Science. Springer Berlin Heidelberg, April 2017, pages 141–163.

[C7] Vincent Cheval, Véronique Cortier, and Bogdan Warinschi. "Secure composition of PKIs with public key protocols". In: *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'17)*. IEEE Computer Society Press, August 2017.

[C8] Myrto Arapinis, Vincent Cheval, and Stéphanie Delaune. "Composing security protocols: from confidentiality to privacy". In: *Proceedings of the 4th International Conference on Principles of Security and Trust (POST'15)*. Volume 9036. Lecture Notes in Computer Science. Springer Berlin Heidelberg, April 2015, pages 324–343.

[C9] Vincent Cheval and Véronique Cortier. "Timing attacks: symbolic framework and proof techniques". In: *Proceedings of the 4th International Conference on Principles of Security and Trust (POST'15)*. Volume 9036. Lecture Notes in Computer Science. Springer Berlin Heidelberg, April 2015, pages 280–299.

[C10] Vincent Cheval, Eric Le Morvan, and Véronique Cortier. "Secure Refinements of Communication Channels". In: *Proceedings of the 35th IARCS Annual Conference of Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2015)*. Volume 45. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl, 2015, pages 575–589.

[C11] Vincent Cheval. "APTE: an Algorithm for Proving Trace Equivalence". In: *Proceedings of the 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'14)*. Volume 8413. Lecture Notes in Computer Science. Springer Berlin Heidelberg, April 2014, pages 587–592.

[C12] Vincent Cheval, Stéphanie Delaune, and Mark Ryan. "Tests for establishing security properties". In: *Revised Selected Papers of the 9th International Symposium on Trustworthy Global Computing (TGC'14)*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, September 2014, pages 82–96.

[C13] Vincent Cheval and Bruno Blanchet. "Proving More Observational Equivalences with ProVerif". In: *Proceedings of the 2nd International Conference on Principles of Security and Trust (POST'13)*. Volume 7796. Lecture Notes in Computer Science. Springer Berlin Heidelberg, March 2013, pages 226–246.

[C14] Vincent Cheval, Véronique Cortier, and Antoine Plet. "Lengths may break privacy – or how to check for equivalences with length". In: *Proceedings of the 25th International Conference on Computer Aided Verification (CAV'13)*. Volume 8044. Lecture Notes in Computer Science. Springer Berlin Heidelberg, July 2013, pages 708–723.

[C15] Myrto Arapinis, Vincent Cheval, and Stéphanie Delaune. "Verifying privacy-type properties in a modular way". In: *Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF'12)*. IEEE Computer Society Press, June 2012, pages 95–109.

[C16] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. "Trace Equivalence Decision: Negative Tests and Non-determinism". In: *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)*. ACM Press, October 2011, pages 321–330.

[C17] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. "Automating security analysis: symbolic equivalence of constraint systems". In: *Proceedings of the 5th International Joint Conference on Automated Reasoning (IJCAR'10)*. Volume 6173. Lecture Notes in Artificial Intelligence. Springer-Verlag, July 2010, pages 412–426.

Other publications

[A1] Vincent Cheval. "Automatic verification of cryptographic protocols: privacy-type properties". PhD Thesis. Laboratoire Spécification et Vérification, ENS Cachan, France, December 2012.

[A2] Vincent Cheval. "Algorithme de décision de l'équivalence symbolique de systèmes de contraintes". Rapport de Master. Master Parisien de Recherche en Informatique, Paris, France, September 2009.

[A3] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. "A decision procedure for proving observational equivalence". In: *Preliminary Proceedings of the 7th International Workshop on Security Issues in Coordination Models, Languages and Systems (SecCo'09)*. October 2009.

Management and participation in research projects

Ongoing projects:

2018-2022 ANR TECAP, **PI** — *Protocol Analysis - Combining Existing Tools.*

2015-2020 ERC Consolidator Grant SPOOC, member — *Automated Security Proofs Of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols.*

2014-2019 ANR Sequoia, member — *Security properties, process equivalences and automated verification.*

Some past projects:

2016 JCJC PEPS VESPA, **co-head** — *Verifying Equivalence Security in Protocols: Tools and Algorithms*

2012-2016 ANR JCJC VIP, member — *Verification of Indistinguishability Properties.*

2010-2014 ANR ProSe, member — *Security Protocols : formal model, computational model, and implementations.*

2008-2011 ANR AVOTE, member — *Analyse formelle de protocoles de vote électronique.*

Collaborations & visits

2014 One-year post-doctoral stay at Laboratoire lorrain de recherche en informatique et ses applications (France), in the team CASSIS headed by Michaël Rusinowitch.

2013 One-year post-doctoral stay at University of Birmingham (UK), in the team of Mark Ryan.

2011-2013 Several stay in LORIA (Nancy, France) in the team CASSIS to collaborate with Véronique Cortier.

2011-2012 Stay of three months from September to December 2011 at École Normale Supérieure de Paris under the supervision of Bruno Blanchet and several visits at INRIA Paris-Rocquencourt in 2012 to collaborate with Bruno Blanchet.

2009 Stay of three months from april to june in the laboratory AIST of Tokyo, Japon, during the internship of my master degree.

Teaching

Lectures at Telecom Nancy.

2019 Protocoles de sécurité et Vérification (8H)
2019 Introduction to theoretical computer science (48H)
2016 Introduction to theoretical computer science (64H)
2015 Introduction to theoretical computer science (32H)

Lectures at École Normale Supérieure de Cachan.

2010-2012 *Cours de programmation pour la préparation à l'agrégation*. (64H)
2010 *Programmation en JAVA* (16H)
2010 *TP programmation* - Dpt. électronique électrotechnique automatique (16H)
2011-2012 *Projet programmation* - Licence 3 Dpt. informatique (32H)

Supervision of student

PhD students

2017-2020 Itsaka Rakotonirina with co-advisor Steve Kremer
2015-16 Eric Le Morvan with co-advisor Véronique Cortier
2013-14 Jiangshan Yu with co-advisor Mark Ryan

Master and bachelor students

2020 Émile Larroque with co-advisor Steve Kremer
2020 Timothé Bonhoure with co-advisor Lucca Hirschi
2020 Hemant Kumar Chodipilli with co-advisor Steve Kremer
2019 Valentin Lecombe with co-advisor Véronique Cortier
2019 Ky NGuyen with co-advisor Véronique Cortier
2019 Aman Kansal with co-advisor Steve Kremer
2018 Aman Bansal with co-advisor Steve Kremer
2017 Sreekar Garlapati with co-advisor Steve Kremer
2016 Itsaka Rakotonirina with co-advisor Steve Kremer
2016 Kushal Babel with co-advisor Steve Kremer

Dissemination

2013 **Discovery of a new attack on the protocols of the electronic passport**.
- Article in *Journal du CNRS*, September-October 2013, number 274, page 9, http://www.cnrs.fr/ins2i/spip.php?article521
- Boxed text in *Pour la Science*, special number on "Big-bang numérique", November 2013, number 433, page 77

Workshops and conferences

Program committees

- The 33rd IEEE Computer Security Foundations Symposium, Boston, US, June 22th, 2020
- The 4th Workshop on Program Equivalence and Relational Reasoning, Los Angeles, US, July 19th, 2020

- The 25th Australasian Conference on Information Security and Privacy, Perth, Australia, July 15th, 2020
- The 33rd ACM/SIGAPP Symposium On Applied Computing, Pau, France, April 9th, 2018
- 5th Workshop on Formal Methods for Security, Tunis, Tunisia, June 23rd, 2014
- 3rd CryptoForma workshop, Royal Holloway University of London, September 12th, 2013

Conference organization

- Member of the organization committee of the 24th IEEE Computer Security Foundations Symposium (CSF'11) (90 attendees) , June 2011

Administrative tasks

2013 Organiser of the Security Seminar in the School of Computer Science, University of Birmingham

2012 Development of the database and web API for the human ressources in the Laboratoire Spécification et Vérification.

Programming skills

Basic python

Intermediate PHP, html, java, FStar

Advanced Ocaml, C, C++, LaTeX

Languages

French Mothertongue

English Advanced *Conversationally fluent*