Vincent Cheval

Laboratoire lorrain de recherche en informatique et ses applications, INRIA
Campus scientifique BP 239,
54506 Vandoeuvre-lès-Nancy Cedex
FRANCE
☎ *+33 (0)354958651*
✉ *vincent.cheval@loria.fr*
homepage: https://members.loria.fr/vcheval/

Curriculum Vitae

2015-Present **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 three tools.

- **APTE:** 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/`
- **ProVerif:** Participation to the development of an extension of ProVerif (Ocam language) allowing ProVerif to prove more observational equivalences. Url of the tool: `http://prosecco.gforge.inria.fr/personal/bblanche/proverif/`

- **Adecs:** 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

[J1] Rohit Chadha, Vincent Cheval, Ștefan Ciobâcă, and Steve Kremer. "Automated verification of equivalence properties of cryptographic protocols". In: *ACM Transactions on Computational Logic* (2016). To appear.

[J2] Jiangshan Yu, Vincent Cheval, and Mark Ryan. "DTKI: A New Formalized PKI with Verifiable Trusted Parties". In: *The Computer Journal* (2016).

[J3] Vincent Cheval, Véronique Cortier, and Stéphanie Delaune. "Deciding equivalence-based properties using constraint solving". In: *Theoretical Computer Science* 492 (June 2013), pages 1–39.

[C1] 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)*. Lecture Notes in Computer Science. To appear. Springer Berlin Heidelberg, 2015.

[C2] 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)*. Lecture Notes in Computer Science. To appear. Springer Berlin Heidelberg, 2015.

[C3] 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.

[C4] 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, 2014, pages 587–592.

[C5] 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, 2014, pages 82–96.

[C6] 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, 2013, pages 226–246.

[C7] 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, 2013, pages 708–723.

[C8] 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, 2012, pages 95–109.

[C9] 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, 2011, pages 321–330.

[C10] 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, 2010, pages 412–426.

[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)*. 2009.

[R1] Vincent Cheval, Stéphanie Delaune, and Hubert Comon-Lundh. "A procedure for deciding symbolic equivalence between sets of constraint systems". In: *Information and Computation* (2016). Submitted.

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.

2016 Introduction to theoretical computer science (32H)

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

2015-16 Eric Le Morvan with co-advisor Véronique Cortier

2013-14 Jiangshan Yu with co-advisor Mark Ryan

Master and bachelor students

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

Talks and seminars

Several talks for working groups at LSV, University of Birmingham and Kent University

Year 2016

June 30th Conference CSF, Lisbon, Portugal - How the internal communication of the applied-pi calculus is messing with equivalence properties

Year 2015

April 17th Conference POST 2015, London, UK - Timing attacks: symbolic framework and proof techniques

February 26th Seminar University of Edinburgh, Edinburgh, UK - Timing attacks: symbolic framework and proof techniques

Year 2014

September 6th Conference TGC 2014, Roma, Italy - Tests for establishing security properties

April 11th Conference TACAS 2014, Grenoble, France - APTE: an Algorithm for Proving Trace Equivalence

April 5th Workshop HotSpot 2014, Grenoble, France - Timing attacks: symbolic framework and proof techniques

April 2nd Seminar LORIA, Nancy, France – DTKI, a new formalised PKI with no trusted parties

Year 2013

March 19th Conference POST 2013, Rome, Paris - Proving more observational equivalences with ProVerif

February 22th Seminar INRIA Paris-Rocquencourt, Paris, France - Automatic tools to prove privacy-type properties

February 5th Second Workshop on Formal Methods And Tools for Security (FMATS2), Cambridge, UK - 5 min talk : Tools for proving equivalence.

Year 2012

October 30th ANR project meeting ProSe, Paris, France - Verifying privacy-type properties in a modular way.

July 26th Seminar School of Computer Science, University of Birmingham, Birmingham, UK - Proving more observational equivalences with ProVerif.

June 25th — Conference CSF 2012, Harvard University, Cambridge MA, USA - Verifying privacy-type properties in a modular way.

Year 2011

November 11th — Seminar LORIA, Nancy, France - Decision procedure for trace equivalence.

October 18th — Conference CCS 2011, Chicago, IL, USA - Decision procedure for trace equivalence.

October 13th — Seminar LIENS, Paris, France - Decision procedure for trace equivalence.

September 5th — Workshop SecCo 2011, Aachen, Germany - Decision procedure for trace equivalence.

June 27th — Conference CSF 2011, Vaux de Cernay, France - 5 min talk : Decision procedure for trace equivalence.

Year 2010

December 10th — General meeting of project ANR AVOTE, Cachan, France - A decision procedure for proving trace equivalence (Work in progress)

July 19th — Conference IJCAR, Edimbourg, Scotland - A decision procedure for proving symbolic equivalence.

June 18th — Workshop SeCret 2010, Valence, Spain - A decision procedure for proving symbolic equivalence.

Workshops and conferences

Program committees

- 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

Article reviews

- Papers for the following workshops and conferences: CCS 2011, FOSSACS 2013, CSF 2013, CCS 2013, POST 2014,CCS 2014, CSF 2014, ESORICS 2014, FMS 2014, ICALP 2014, HotSpot 2014,STM 2014, POST 2015, AsiaCCS 2015
- Papers for the following journals: Journal of Automated Reasoning, Journal of Symbolic Computation, Journal of Computer Security

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*