Vincent Cheval

Inria Paris
2 Rue Simone IFF 75012 Paris
France
8 Sep 1985
+33 (0)180494350
vincent.cheval@inria.fr
https://chevalvi.gitlabpages.inria.fr/chevalvi/
VincentCheval
DBLP

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

Awards

2018 **Distinguished paper award at S&P 2018**, with S. Kremer, and I. Rakotonirina.

2016 **Paper listed in ACM Computing Rewiews 21st Annual Best of Computing list of notable books and articles for 2016**, with R. Chadha, S. Ciobaca, and S. Kremer.

Research Interests

My research area is the formal analysis and design of **cryptographic protocols**, with an emphasis on **automated verification** in the so-called symbolic model and the development of state-of-the-art **verification tools**. The theories behind my research and tools have root in automated reasoning, rewriting, (probabilistic) model-checking, first-order logic and concurrency theory. During my PhD,

I mainly focused on **privacy-type** security properties such as nonymity, privacy, unlinkability, strong secrecy that can be expressed by the means of behavioral equivalences. More recently, through my work on **ProVerif**, I have tackled a broader set of security proeprties, including for example accountability, injective-correspondence, end-to-end verifiability, liveness. My research aims at verifying relevant security protocols, e.g. TLS, cryptocurrency blockchain based protocols, electronic voting protocols, RFID protocols, certificate management protocols, telecommunication protocols, cloud computing...

Participation to the development of six tools.

- **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: `https://bblanche.gitlabpages.inria.fr/proverif/`
- **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`
- **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/`

Complete list of publications

Submitted

[S1] V. Cheval and I. Rakotonirina. Going beyond diff equivalence in proverif: Proving observational and may-testing equivalences and their pre-order, 2022.

[S2] V. Cheval, J. Moreira, and M. D. Ryan. Automatic verification of transparency protocols, May 2022.

[S3] V. Cheval, S. Kremer, and I. Rakotonirina. Deepsec: Deciding equivalence properties for security protocols - improved theory and practice. 2022.

[S4] N. Borisov, V. Cheval, T. Eaton, T. Lepoint, , and C. Wood. An analysis of rate-limited privacy pass, May 2022.

International conferences with review committee

[C1] V. Cheval, C. Cremers, A. Dax, L. Hirschi, C. Jacomme, and S. Kremer. Hash gone bad: Automated discovery of protocol attacks that exploit hash function weaknesses. In

32nd USENIX Security Symposium (USENIX Security'23), Anaheim, CA, USA, Aug. 2023. USENIX Association. To appear.

[C2] V. Cheval, C. Jacomme, S. Kremer, and R. Künnemann. SAPIC+: protocol verifiers of the world, unite! In *31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022*, pages 3935–3952. USENIX Association, 2022.

[C3] V. Cheval, R. Crubillé, and S. Kremer. Symbolic protocol verification with dice: process equivalences in the presence of probabilities. In *35th IEEE Computer Security Foundations Symposium, CSF 2022, Haifa, Israel, August 7-10, 2022*, pages 319–334. IEEE, 2022.

[C4] B. Blanchet, V. Cheval, and V. Cortier. Proverif with lemmas, induction, fast subsumption, and much more. In *43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, May 22-26, 2022*, pages 69–86. IEEE, 2022.

[C5] K. Bhargavan, V. Cheval, and C. A. Wood. A symbolic analysis of privacy for TLS 1.3 with encrypted client hello. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*, pages 365–379. ACM, 2022.

[C6] V. Cheval, S. Kremer, and I. Rakotonirina. The hitchhiker's guide to decidability and complexity of equivalence properties in security protocols. In V. Nigam, C. Talcott, J. Guttman, T. Ban Kirigan, S. Kuznetsov, M. Okada, and B. Thau Loo, editors, *Logic, Language, and Security. Essays Dedicated to Andre Scedrov on the Occasion of His 65th Birthday*, volume 12300 of *Lecture Notes in Computer Science*. Springer, 2020.

[C7] V. Cheval, S. Kremer, and I. 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)*, pages 905–922. ACM Press, Nov. 2019.

[C8] V. Cheval, S. Kremer, and I. Rakotonirina. The DEEPSEC prover. In *Computer Aided Verification - 30th International Conference, CAV 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 14-17, 2018, Proceedings, Part II*, volume 10982 of *Lecture Notes in Computer Science*, pages 28–36. Springer, 2018.

[C9] V. Cheval, S. Kremer, and I. 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)*, San Francisco, CA, USA, May 2018. IEEE Computer Society Press. **Distinguished paper award**.

[C10] V. Cheval, V. Cortier, and M. Turuani. A little more conversation, a little less action, a lot more satisfaction: Global states in proverif. In S. Chong and S. Delaune, editors, *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'18)*, Oxford, UK, July 2018. IEEE Computer Society Press.

[C11] V. Cheval, V. Cortier, and B. 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, Aug. 2017.

[C12] K. Babel, V. Cheval, and S. 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 of *Lecture Notes in Computer Science*, pages 141–163. Springer Berlin Heidelberg, Apr. 2017.

[C13] V. Cheval, E. Le Morvan, and V. 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 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 575–589. Schloss Dagstuhl, 2015.

[C14] V. Cheval and V. 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 of *Lecture Notes in Computer Science*, pages 280–299. Springer Berlin Heidelberg, Apr. 2015.

[C15] M. Arapinis, V. Cheval, and S. 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 of *Lecture Notes in Computer Science*, pages 324–343. Springer Berlin Heidelberg, Apr. 2015.

[C16] V. Cheval, S. Delaune, and M. 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, pages 82–96. Springer Berlin Heidelberg, Sept. 2014.

[C17] V. 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 of *Lecture Notes in Computer Science*, pages 587–592. Springer Berlin Heidelberg, Apr. 2014.

[C18] V. Cheval, V. Cortier, and A. 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 of *Lecture Notes in Computer Science*, pages 708–723. Springer Berlin Heidelberg, July 2013.

[C19] V. Cheval and B. Blanchet. Proving more observational equivalences with proverif. In *Proceedings of the 2nd International Conference on Principles of Security and Trust (POST'13)*, volume 7796 of *Lecture Notes in Computer Science*, pages 226–246. Springer Berlin Heidelberg, Mar. 2013.

[C20] M. Arapinis, V. Cheval, and S. Delaune. Verifying privacy-type properties in a modular way. In *Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF'12)*, pages 95–109. IEEE Computer Society Press, June 2012.

[C21] V. Cheval, H. Comon-Lundh, and S. Delaune. Trace equivalence decision: Negative tests and non-determinism. In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)*, pages 321–330. ACM Press, Oct. 2011.

[C22] V. Cheval, H. Comon-Lundh, and S. Delaune. Automating security analysis: symbolic equivalence of constraint systems. In *Proceedings of the 5th International Joint Conference*

on Automated Reasoning (IJCAR'10), volume 6173 of *Lecture Notes in Artificial Intelligence*, pages 412–426. Springer-Verlag, July 2010.

[C23] V. Cheval, H. Comon-Lundh, and S. 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)*, Oct. 2009.

International journals with review committee

[J1] K. Babel, V. Cheval, and S. Kremer. On the semantics of communications when verifying equivalence properties. *Journal of Computer Security*, 28(1):71–127, 2020.

[J2] V. Cheval, H. Comon-Lundh, and S. Delaune. A procedure for deciding symbolic equivalence between sets of constraint systems. *Information and Computation*, 255:94–125, 2017.

[J3] J. Yu, V. Cheval, and M. Ryan. Dtki: A new formalized pki with verifiable trusted parties. *The Computer Journal*, 59(11):1695–1713, 2016.

[J4] R. Chadha, V. Cheval, Ş. Ciobâcă, and S. Kremer. Automated verification of equivalence properties of cryptographic protocols. *ACM Transactions on Computational Logic*, 17(4):1–32, 2016. **Listed in ACM Computing Reviews' 21st Annual Best of Computing list of notable books and articles for 2016**.

[J5] V. Cheval, V. Cortier, and S. Delaune. Deciding equivalence-based properties using constraint solving. *Theoretical Computer Science*, 492:1–39, June 2013.

Others

[O1] V. Cheval. *Automatic verification of cryptographic protocols: privacy-type properties*. Phd thesis, Laboratoire Spécification et Vérification, ENS Cachan, France, Dec. 2012.

[O2] V. Cheval. Algorithme de décision de l'équivalence symbolique de systèmes de contraintes. Rapport de Master, Master Parisien de Recherche en Informatique, Paris, France, Sept. 2009.

Management and participation in research projects

Ongoing projects:

2022-2028 SVP Project - PEPR Cybersecurity, member – *Verification of Security Protocols*

2020-2024 ANR ASAP, member — *Research and teaching chair in AI*

Some past projects:

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

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

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.*

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.*

Teaching

Lectures

2020-21 **Proofs of security protocols**, *Master course*, Univeristé de Paris, (12h each year)

2020-21 **Programming project**, *L2 course*, Univeristé de Paris, (12h each year)

2020-21 **Algorithmics**, *L2 course*, Univeristé de Paris, (36h each year)

2019 **Security protocols and Verification**, *Master course*, Telecom Nancy, (8h)

2019 **Introduction to theoretical computer science**, *L3 course*, Telecom Nancy, (48h)

2015-16 **Introduction to theoretical computer science**, *L3 course*, Telecom Nancy, (48h each year)

2015 **Practical session on HTML language**, *BSc course*, University of Kent, (32H)

2015 **Introduction to Cryptographic protocols**, *BSc course*, University of Kent, (6H)

2010-12 **Programming lectures for *agrégration* preparation**, *Master course*, ENS Cachan, (64H)

2011-12 **Programming project**, *L3 course*, ENS Cachan, (32H)

2010 **Java Programming**, *L3 course*, ENS Cachan, (16H)

Summer Schools

2021 VeriCrypt: An Introduction to Tools for Verified Cryptography, Online

2018 CARI-ICTAC Research School, Stellenbosch, South Africa

2018 Modelling and Verification of Parallel Processes (MOVEP), Paris, France

2017 Summer School on Models and Tools for Cryptographic Proofs, Nancy, France

Supervision of students

PhD students

2017-2020 Itsaka Rakotonirina with co-advisor Steve Kremer

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

Master and bachelor students

2022 Ellenor Taghayor and Benjamin Catinaud

2020 Émile Larroque and Hemant Kumar Chodipilli with co-advisor Steve Kremer

2020 Timothé Bonhoure with co-advisor Lucca Hirschi

2019 Valentin Lecombe and 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 and Kushal Babel with co-advisor Steve Kremer

Committees

Program committees

2021 The 2021 ACM SIGSAC Conference on Computer and Communications Security, November 15th

2020 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

2018 The 33rd ACM/SIGAPP Symposium On Applied Computing, Pau, France, April 9th

2014 5th Workshop on Formal Methods for Security, Tunis, Tunisia, June 23rd

2013 3rd CryptoForma workshop, Royal Holloway University of London, September 12th

Conference organization

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

Hiring commitees

2022 Member of the hiring committee Assistant Professor Position in ENS Cachan

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

Other responsabilities

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.