Véronique Cortier

LORIA, Cassis project
Campus Scientifique, BP 239
54506 Vandœuvre-lès-Nancy, France
tel : +(33) 3 83 59 30 55

2 children
e-mail : *veronique.cortier@loria.fr*
web page : *https ://members.loria.fr/VCortier/*

Professional experience and Education

Since Oct. 2010 Research director (directrice de rechercher) of the French National Scientific Research Center (CNRS), at the LORIA laboratory, Nancy, France.

Since Nov. 2009 Habilitation to conduct researches. This French diploma gives the official authorization to supervise PhD students on its own. The defense was held on November 18th, 2009.

Oct. 2003 Research Scientist (chargée de recherche) of the French National Scientific Research Center (CNRS), at the LORIA laboratory, Nancy, France.

Sept. 2000 - March 2003 PhD in Computer Science, École Normale Supérieure de Cachan. Supervisor : Pr. Hubert Comon Defense : 20th March 2003
Title : Automatic Verification of Cryptographic Protocols. (**Two Awards**)

Sept. 1997 - Sept. 2001 Master in Mathematics and Computer Science at the École Normale Supérieure de Cachan. "Agrégation" in Mathematics (in 2000).

Awards

Best paper award at Esorics'20 for the paper Automatic generation of sources lemmas in Tamarin : towards automatic proofs of security protocols with Stéphanie Delaune and Jannik Dreier.

Distinguished paper award at CSF'20 for the paper Fifty Shades of Ballot Privacy : Privacy against a Malicious Board with Joseph Lallemand.

EASST best paper award at ETAPS 2016 with Antoine Dallon and Stéphanie Delaune for the paper *Bounding the number of agents, for equivalence too* presented at POST 2016.

Inria-French Académie des sciences Young Researcher Award 2015

Scientific PhD thesis Award 2004 from *Le Monde* (one of the main French newspapers).

PhD thesis Award 2003 from SPECIF (French association of University professors in Computer Science).

Professional activities

Publications 20+ international journals, 2 edited books and, 70+ international conferences.

Editor in chief of *Journal of Computer Security* (JCS) since 2019, and member of the editorial board from 2012 to 2019.

Member of the editorial board of *ACM Transactions on Privacy and Security (TOPS, previously TISSEC)* since 2015.

Member of the editorial board of *Foundations and Trends (FnT) in Security and Privacy* since 2014.

Member of the editorial board of *Information and Computation* (I&C) from 2012 to 2018.

Member of the Steering committee of CSF (*Computer Security Conference*) (2011-2019)

Member of the Steering committee of POST (*Conference on Principles of Security and Trust*) (2014-2018)

Chair of EVoteID'18 and EVoteID'19

Chair of CSF'12 and CSF'13

Vice-chair of the international working group IFIP Wg-1.7 Foundations of Security Analysis since 2009.

Program committees member of several conferences each year, in the **security community**, *e.g.* S&P'19-20-22, CCS'10-12-13-14-16-17-18-20, CSF'06-08-09-12-13-19-21-22, ESORICS'10-11-12-14, EuroCrypt'21, EVoteID'16-17-18-19-20-21-22, POST'12-13-15-17-18-19, as well as the **formal methods community**, *e.g.* LICS'10-13-15-17, CONCUR'15-16-20, ICALP'14, FOSSACS'14, FSTTCS'10, MFCS'16.

Head of the « security axis » of Loria of the Loria lab, and **member of the scientific council** of the Loria lab from 2012 to 2018.

Head of the Verification working group (GT-Verif) of the GdR-IM (2012-2017). This working group gathers about 200 members.

Executive member of SigLog ACM Special Interest Group on Logic and Computation since 2014, Vice-Chair since 2019.

Member of the Scientific Council of INS2I CNRS institute (2014-2018).

Member of the Scientific Council of ANSSI (2019-).

Member of the Scientific Council of IAEM, Lorraine University (2011-2016).

Member of the Scientific Council of ESIEE, Marne la Vallée (2016-2018).

Member of evaluation committees INRIA evaluation committee, several hiring committees (in France and Germany)

Reviews Reviewer for national grants (e.g. for the French ANR agency and Swiss, FWO in Belgium, Luxembourg, Italy, Croatia).
Reviews of more than 30 papers each year in journals (TCS, JACM, JLAP, TOCL, JCS, MSCS, ACTA INFORMATICA, SAR, ...), conferences (STACS, ICALP, FOSSACS, ESOP, CADE, CSL, FSTTCS, CSFW, ACM CCS, SP Oakland, CONCUR, AMAST, RTA, FM, ...) and workshops.

Teaching *Theory of Security* (Advanced lecture in Master) since 2005.

Supervision of research

PhDs

Quentin Yang (Oct. 2020 -)

Joseph Lallemand (Sept. 2016 - Nov. 2019), now CNRS researcher at Irisa (Rennes)

Antoine Dallon (Nov. 2015 - Nov. 2018), now research engineer at DGA-MI

Alicia Filipiak (March 2015 - March 2018), now research engineer at Orange

Éric Le Morvan (Oct. 2013 - discontinued), now Math teacher in highscool

Rémy Chrétien (Oct. 2012 - Jan. 2016), now scientific expert at the Ministery of Defense

Cyrille Wiedling (Sept. 2011 - Nov. 2014), now research engineer at DGA-MI

Guillaume Scerri (Sept. 2011 - Jan. 2015), now assistant professor at the university of Versailles

Stefan Ciobaca (Sept. 2008 - Nov 2011), now lecturer at Iasu University, Roumania

Mathilde Arnaud (Sept. 2008 - Oct 2011), now engineer at CEA, France

Heinrich Hördegen (Oct. 2005 - Nov. 2007), now at the Di-IT company, Germany

Eugen Zalinescu (Oct. 2004 - Dec. 2007), now research assistant at TUM, Munich

7 Post-docs

13 Masters

Some Participation in Research Projects

Chaire IA (member) (2020-2025)

ANR project Tecap. (member) (2018-2021)

ANR project Sequoia. (member) (2015-2018)

ERC Starting Grant project ProSecure. (principal investigator) *Provably secure systems : foundations, design, and modularity* (1 400 kE, Feb. 2011 - Jan. 2016)

ANR AVOTÉ project (principal investigator) on analyzing e-voting protocols. Grant : 500kE for four years and for four partners (19 members involved). (Jan. 2008 - Dec. 2011)

In the past, I was also co-investigator of the PHC Alliance project on refinement of security properties (6kE for the French side) principal investigator of a French national project (the ACI Jeunes Chercheurs JC9005, 6 members, 80kE, 2004-2007), principal investigator for the French side of a Franco-Tunisian project (about 6kE, 2007-2008). I was also local investigator (for my Lab) of the ARA SSIA FormaCrypt project (about 35kE for my Lab, 2006-2008). Most of these projects included both academic and industrial partners.

Some contracts with industrial partners

In the context of contracts between my team and industrial or State partners, I have worked with the Foreign Affaire ministry (MEAE), Swiss Post, Nomadic Labs, Idemia, Docaposte, Genova canton, Scytl, Voxaly, Orange.

Selected Invited talks

Keynote speaker of EVoteID 2022 Bregenz, Austria, October 2022.

Invited talk at the Isaac Newton Institute workshop on Verified software : from theory to practice (virtual), May 2021.

Invited talk at IndoCrypt 2020 Bangalore (virtual), India, December 2020.

Plenary talk of CSL 2020 Barcelona, Spain, January 2020.

Keynote speaker of PLAS 2019 London, UK, November 2019.

Keynote speaker of Esorics 2019 Luxembourg, September 2019.

Lecturer at the winter school of VMCAI 2019, Lisbon, Portugal, January 2019.

Keynote speaker of DisCoTec 2018 Madrid, Spain, June 2018.

Invited tutorial at ETAPS 2017, Uppsala, Sweden, April 2017.

Invited talk at Highlights 2017, London, UK, September 2017.

Invited talk at FPS 2017, Nancy, France, October 2017.

Invited talk at CIAA 2017, Marne-la-Vallée, France, June 2017.

Invited talk at Models and Tools for Security Analysis and Proofs Workshop , affiliated with Eurocrypt 2017, Paris, France, April 2017.

Keynote Speech of LIG 2016, Grenoble, France, October 2016.

Colloquium LIRRM 2016, Montpellier, France, September 2016.

GdR-IM National days 2016, Invited talk at the 2016 Colloquium of the French Society in Computer Science, Strasbourg, France, January 2016.

SIF 2016, Invited talk at the 2016 National days of the GdR-IM, Villetaneuse, France, January 2016.

Collège de France 2015 Seminar at "Collège de France", Chaire of Gérard Berry, Paris, March 2015.

Marktoberdorf 2015 Lectures at Summer School Marktoberdorf 2015, Marktoberdorf, Germany, August 2015.

EJCP 2015 Lectures at EJCP 2015, Nancy, France, June 2015.

TGC 2014 Invited speaker at TGC 2014 (Trustworthy Global Computing), Roma, September, 2014.

FLOC 2014 Plenary speaker at FLOC 2014 (Federated Logic Conference), Vienna, July 20th, 2014.

Summer School Lectures at the Fourth Summer School on Formal Techniques, Menlo College, Atherton, CA, May 2014.

Invited speaker at the Science and Society conferences, Nancy, January 17th, 2013. (slides - in French)

Invited talk at the Jacques Morgenstern Colloquium, Sophia-Antipolis, France, June 7th, 2012.

Collège de France 2011 Seminar at "Collège de France", Chaire of Martin Abadi, Paris, May 18th, 2011.

STACS 2011 Invited lecture at STACS 2011, Symposium on Theoretical Aspects of Computer Science, Dortmund, Germany, March 12th, 2011.

TOSCA 2011 Invited speaker at TOSCA 2011, Theory of Security and Applications, affiliated with ETAPS 2011, March 31st and April 1st, 2011.

FOSAD 2010, International School on Foundations of Security Analysis and Design, Bertinoro (Italy), September 5-12, 2010.

VMCAI'09, Conference on Verification, Model Checking, and Abstract Interpretation, January 18-20, 2009, Savannah, GA, USA (co-located with POPL 2009).

RTA'08, International Conference on Rewriting Techniques and Applications, July 15-17, 2008. Hagenberg, Austria.

TFIT'08, Fourth Taiwanese-French Conference on Information Technology (TFIT'08), Taipei, Taiwan, March 3-5, 2008.

WITS'07, 7th International Workshop on Issues in the Theory of Security, Braga, Portugal, Mars 24th, 2007. (co-located with ETAPS).

AVOCS'06, International Workshop on Automated Verification of Critical Systems, Nancy, France, Septembre 19th, 2006.

Information-MFCSIT'06, International Conference on Information and Irish Conference on the Mathematical Foundations of Computer Science and Information Technology, Cork, Irland, August 4th, 2006, Special Session on Formal Approaches to Security.

Publications

Most of the papers can be downloaded on my webpage :
https ://members.loria.fr/VCortier/files/Publications/

International Journals

[CDS21] Véronique Cortier, Stéphanie Delaune, and Vaishnavi Sundararajan. A decidable class of security protocols for both reachability and equivalence properties. *Journal of Automated Reasoning*, 65 :479–520, April 2021.

[CCDD19] Rémy Chrétien, Véronique Cortier, Antoine Dallon, and Stéphanie Delaune. Typing messages for free in security protocols. *ACM Transactions on Computational Logic*, 21(1), October 2019.

[CW17] Véronique Cortier and Cyrille Wiedling. A formal analysis of the norwegian e-voting protocol. *Journal of Computer Security*, 25(15777) :21–57, 2017.

[CCD15c] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. From security protocols to pushdown automata. *ACM Transactions on Computational Logic*, 17(3), November 2015.

[Cor15b] Véronique Cortier. Formal verification of e-voting : solutions and challenges. *3rd SigLog Newsletter, ACM Special Interest Group on Logic and Computation*, 2(1) :25–34, January 2015.

[CK14] Véronique Cortier and Steve Kremer. Formal models and techniques for analyzing security protocols : A tutorial. *Foundations and Trends in Programming Languages*, 1(3) :151–267, 2014.

[ACD14] Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Modeling and verifying ad hoc routing protocols. *Information and Computation*, 238(0) :30–67, 2014.

[CS14] Véronique Cortier and Graham Steel. A generic security API for symmetric key management on cryptographic devices. *Information and Computation*, 238 :208–232, 2014.

[CCD13a] Vincent Cheval, Véronique Cortier, and Stéphanie Delaune. Deciding equivalence-based properties using constraint solving. *Theoretical Computer Science*, 492 :1–39, 2013.

[CS13] Véronique Cortier and Ben Smyth. Attacking and fixing Helios : An analysis of ballot secrecy. *Journal of Computer Security*, 21(1) :89–148, 2013.

[BCD13] Mathieu Baudet, Véronique Cortier, and Stéphanie Delaune. YAPA : A generic tool for computing intruder knowledge. *ACM Transactions on Computational Logic*, 14, 2013.

[CD12] Véronique Cortier and Stéphanie Delaune. Decidability and combination results for two notions of knowledge in security protocols. *Journal of Automated Reasoning*, 48, 2012.

[BBC11] Mouhebeddine Berrima, Narjes Ben Rajeb, and Véronique Cortier. Deciding knowledge in security protocols under some e-voting theories. *Theoretical Informatics and Applications (RAIRO-ITA)*, 45 :269–299, 2011.

[CKW10] Véronique Cortier, Steve Kremer, and Bogdan Warinschi. A survey of symbolic methods in computational analysis of cryptographic systems. *Journal of Automated Reasoning*, 46(3-4) :225–259, April 2010.

[CCZ10] Hubert Comon-Lundh, Véronique Cortier, and Eugen Zălinescu. Deciding security properties for cryptographic protocols. application to key cycles. *ACM Transactions on Computational Logic*, 11(2), January 2010.

[BCK09] Mathieu Baudet, Véronique Cortier, and Steve Kremer. Computationally sound implementations of equational theories against passive adversaries. *Information and Computation*, 207(4) :496–520, April 2009.

[CD09b] Véronique Cortier and Stéphanie Delaune. Safely composing security protocols. *Formal Methods in System Design*, 34(1) :1–36, February 2009.

[CRZ07] Véronique Cortier, Michael Rusinowitch, and Eugen Zalinescu. Relating two standard notions of secrecy. *Logical Methods in Computer Science*, 3(3), July 2007.

[AC06] Martin Abadi and Véronique Cortier. Deciding knowledge in security protocols under equational theories. *Theoretical Computer Science*, 387(1-2) :2–32, November 2006. **Top cited article 2005-2010 TCS paper award**.

[CGLN06] Véronique Cortier, Xavier Goaoc, Mira Lee, and Hyeon-Suk Na. A note on maximally repeated sub-patterns of a point set. *Discrete Mathematics*, 306(16) :1965–1968, August 2006.

[CDL06] Véronique Cortier, Stéphanie Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1) :1–43, 2006.

[CC05] Hubert Comon and Véronique Cortier. Tree automata with one memory, set constraints and cryptographic protocols. *Theoretical Computer Science*, 331(1) :143–214, February 2005.

[CC04] Hubert Comon-Lundh and Véronique Cortier. Security properties : Two agents are sufficient. *Science of Computer Programming*, 50(1-3) :51–71, March 2004.

[Cor02a] Véronique Cortier. About the decision of reachability for register machines. *Theoretical Informatics and Applications*, 36(4) :341–358, Oct. - Dec. 2002.

National Journals

[Cor05] Véronique Cortier. Vérifier les protocoles cryptographiques. *Technique et Science Informatique, Hermes Science*, 24(1) :115–140, 2005.

Edited books

[CK11] Véronique Cortier and Steve Kremer, editors. *Formal Models and Techniques for Analyzing Security Protocols*, volume 5 of *Cryptology and Information Security Series*. IOS Press, 2011.

[CKOS09] Véronique Cortier, Claude Kirchner, Mitsuhiro Okada, and Hideki Sakurada, editors. *Formal to practical Security*, volume 5458 of *Lecture Notes in Computer Science*. Springer, springer edition, 2009.

Book chapters

[Cor06b] Véronique Cortier. *Cryptographie et codes secrets*, chapter Les protocoles cryptographiques, pages 106–113. Bibliothèque Tangente, POLE edition, 2006. Hors-série 26.

[Cor06e] Véronique Cortier. *Sur les chemins de la découverte*, chapter Sécuriser les réseaux, les protocoles cryptographiques, pages 107–118. Presses Universitaires de France, January 2006.

International Conferences

[CDG22] Véronique Cortier, Alexandre Debant, and Pierrick Gaudry. A privacy attack on the Swiss Post e-voting system. In *Real World Crypto Symposium (RWC'22)*, Amsterdam, Netherlands, 2022. IACR.

[CDD22] Véronique Cortier, Antoine Dallon, and Stéphanie Delaune. A small bound on the number of sessions for security protocols. In *35th IEEE Computer Security Foundations Symposium (CSF'22)*, Haifa, Israel, August 2022.

[BCC22] Bruno Blanchet, Vincent Cheval, and Véronique Cortier. Proverif with lemmas, induction, fast subsumption, and much more. In *Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P'22)*. IEEE Computer Society Press, 2022.

[CGY20] Véronique Cortier, Pierrick Gaudry, and Quentin Yang. How to fake zero-knowledge proofs, again. In *Fifth International Joint Conference on Electronic Voting (E-Vote-ID 2020)*, Bregenz / virtual, Austria, 2020.

[CLW20] Véronique Cortier, Joseph Lallemand, and Bogdan Warinschi. Fifty shades of ballot privacy : Privacy against a malicious board. In *33rd IEEE Computer Security Foundations Symposium (CSF'20)*, Boston / virtual, USA, June 2020. **CSF distinguished paper award**.

[CDD20] Véronique Cortier, Stéphanie Delaune, and Jannik Dreier. Automatic generation of sources lemmas in Tamarin : towards automatic proofs of security protocols. In *25th European Symposium on Research in Computer Security (ESORICS 2020)*, Guilford / virtual, United Kingdom, September 2020. **Esorics best paper award**.

[CGY20] Véronique Cortier, Pierrick Gaudry, and Quentin Yang. How to fake zero-knowledge proofs, again. In *Fifth International Joint Conference on Electronic Voting (E-Vote-ID 2020)*, Bregenz / virtual, Austria, 2020.

[CFL19] Véronique Cortier, Alicia Filipiak, and Joseph Lallemand. BeleniosVS : Secrecy and verifiability against a corrupted voting device. In *32nd IEEE Computer Security Foundations Symposium (CSF'19)*, Hoboken, USA, June 2019.

[CGG19] Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu. *Belenios : A Simple Private and Verifiable Electronic Voting System*, pages 214–238. Springer International Publishing, 2019.

[CL18] Véronique Cortier and Joseph Lallemand. Voting : You can't have privacy without individual verifiability. In *25th ACM Conference on Computer and Communications Security (CCS'18)*, pages 53–66. ACM, 2018.

[CDD18] Véronique Cortier, Stéphanie Delaune, and Antoine Dallon. Efficiently deciding equivalence for standard primitives and phases. In *Proceedings of the 23rd European Symposium on Research in Computer Security (ESORICS'18)*, pages 491–511. LNCS, 2018.

[CDS+18] Véronique Cortier, Constantin Catalin Dragan, Pierre-Yves Strub, Francois Dupressoir, and Bogdan Warinschi. Machine-checked proofs for electronic voting : privacy and verifiability for belenios. In *Proceedings of the 31st IEEE Computer Security Foundations Symposium (CSF'18)*, pages 298–312, 2018.

[CCT18] 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 31st IEEE Computer Security Foundations Symposium (CSF'18)*, pages 344–358, 2018.

[CGLM18] Véronique Cortier, Niklas Grimm, Joseph Lallemand, and Matteo Maffei. Equivalence properties by typing in cryptographic branching protocols. In *Proceedings of the 7th International Conference on Principles of Security and Trust (POST'18)*, pages 160–187, April 2018.

[CGT18] Véronique Cortier, David Galindo, and Mathieu Turuani. A formal analysis of the neuchâtel e-voting protocol. In *3rd IEEE European Symposium on Security and Privacy (EuroSP'18)*, pages 430–442, London, UK, April 2018.

[CGLM17] Véronique Cortier, Niklas Grimm, Joseph Lallemand, and Matteo Maffei. A type system for privacy properties. In *24th ACM Conference on Computer and Communications Security (CCS'17)*, pages 409–423, Dallas, USA, October 2017. ACM.

[CCW17] 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)*, pages 144 – 158. IEEE Computer Society Press, August 2017.

[CSD+17] Véronique Cortier, Benedikt Schmidt, Constantin Catalin Dragan, Pierre-Yves Strub, Francois Dupressoir, and Bogdan Warinschi. Machine-checked proofs of privacy for electronic voting protocols. In *Proceedings of the 37th IEEE Symposium on Security and Privacy (S&P'17)*, pages 993–1008. IEEE Computer Society Press, 2017.

[CFF+17] Véronique Cortier, Alicia Filipiak, Jan Florent, Said Gharout, and Jacques Traoré. Designing and proving an EMV-compliant payment protocol for mobile devices. In *2nd IEEE European Symposium on Security and Privacy (EuroSP'17)*, pages 467–480, 2017.

[CCFG16] Pyrros Chaidos, Véronique Cortier, Georg Fuchsbauer, and David Galindo. BeleniosRF : A non-interactive receipt-free electronic voting scheme. In *23rd ACM Conference on Computer and Communications Security (CCS'16)*, pages 1614–1625, Vienna, Austria, October 2016. ACM.

[ACK16] Myrto Arapinis, Véronique Cortier, and Steve Kremer. When are three voters enough for privacy properties ? In Ioannis Askoxylakis, Sotiris Ioannidis, Sokratis Katsikas, and Catherine Meadows, editors, *Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS'16)*, Lecture Notes in Computer Science, pages 241–260, Heraklion, Crete, September 2016. Springer.

[CGK+16b] Véronique Cortier, David Galindo, Ralf Küsters, Johannes Müller, and Tomasz Truderung. Sok : Verifiability notions for e-voting protocols. In *Proceedings of the 36th IEEE Symposium on Security and Privacy (S&P'16)*, San Jose, CA, USA, May 2016. IEEE Computer Society Press.

[CDD16] Véronique Cortier, Antoine Dallon, and Stéphanie Delaune. Bounding the number of agents, for equivalence too. In Frank Piessens and Luca Viganó, editors, *Proceedings of the 5th International Conference on Principles of Security and Trust (POST'16)*, volume 9635 of *Lecture Notes in Computer Science*, pages 211–232, Eindhoven, The Netherlands, April 2016. Springer. **EASST best paper award of the ETAPS conference**.

[CClM15] Vincent Cheval, Véronique Cortier, and Eric le Morvan. Secure Refinements of Communication Channels. In Prahladh Harsha and G. Ramalingam, editors, *35th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2015)*, volume 45 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 575–589, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[CCD15a] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. Checking trace equivalence : How to get rid of nonces ? In *Proceedings of the 20th European Symposium on Research in Computer Security (ESORICS'15)*, Lecture Notes in Computer Science, Vienna, Austria, 2015. Springer.

[CCD15b] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. Decidability of trace equivalence for protocols with nonces. In *Proceedings of the 28th IEEE Computer Security Foundations Symposium (CSF'15)*. IEEE Computer Society Press, July 2015.

[BCG+15a] David Bernhard, Veronique Cortier, David Galindo, Olivier Pereira, and Bogdan Warinschi. A comprehensive analysis of game-based ballot privacy definitions. In *Proceedings of the 36th IEEE Symposium on Security and Privacy (S&P'15)*, pages 499–516, San Jose, CA, USA, May 2015. IEEE Computer Society Press.

[CC15] Vincent Cheval and Véronique Cortier. Timing attacks in security protocols : symbolic framework and proof techniques. In *Proceedings of the 4th Conference on Principles of Security and Trust (POST'15)*, volume 9036 of *Lecture Notes in Computer Science*, pages 280–299, London, UK, April 2015. Springer.

[CEK+15a] Véronique Cortier, Fabienne Eigner, Steve Kremer, Matteo Maffei, and Cyrille Wiedling. Type-based verification of electronic voting protocols. In *Proceedings of the 4th Conference on Principles of Security and Trust (POST'15)*, volume 9036 of *Lecture Notes in Computer Science*, pages 303–323, London, UK, April 2015. Springer.

[CCD14a] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. Typing messages for free in security protocols : the case of equivalence properties. In *Proceedings of the 25th International Conference on Concurrency Theory (CONCUR'14)*, volume 8704 of *Lecture Notes in Computer Science*, pages 372–386, Rome, Italy, September 2014. Springer.

[CGGI14] Véronique Cortier, David Galindo, Stéphane Glondu, and Malika Izabachene. Election verifiability for Helios under weaker trust assumptions. In *Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS'14)*, volume 8713 of *LNCS*, pages 327–344, Wroclaw, Poland, September 2014. Springer.

[Cor14] Véronique Cortier. Electronic voting : How logic can help. In *Proceegings of the 12th International Joint Conference on Automated Reasoning (IJCAR 2014)*, volume 8562 of *LNAI*, pages 16–26, Vienna, Austria, 2014.

[CGGI13a] Véronique Cortier, David Galindo, Stéphane Glondu, and Malika Izabachene. Distributed ElGamal à la Pedersen - Application to Helios. In *Workshop on Privacy in the Electronic Society (WPES 2013)*, Berlin, Germany, 2013.

[ACW13] Mathilde Arnaud, Véronique Cortier, and Cyrille Wiedling. Analysis of an electronic boardroom voting system. In *4th International Conference on e-Voting and Identity (VoteID'13)*, volume 7985 of *Lecture Notes in Computer Science*, Surrey, UK, July 2013. Springer.

[BCW13a] Florian Böhl, Véronique Cortier, and Bogdan Warinschi. Deduction soundness : Prove one, get five for free. In *20th ACM Conference on Computer and Communications Security (CCS'13)*, Berlin, Germany, 2013.

[CCP13] 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 8043 of *Lecture Notes in Computer Science*, pages 708–723, St Petersburg, Russia, July 2013. Springer.

[CLCS13] Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. Tractable inference systems : an extension with a deducibility predicate. In *Proceedings of the 25th International Conference on Automated Deduction (CADE'13)*, volume 7898 of *Lecture Notes in Computer Science*, pages 91–108, Lake Placid, USA, June 2013. Springer.

[CCD13b] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. From security protocols to pushdown automata. In *Proceedings of the 40th International Colloquium on Automata, Languages and Programming (ICALP'13)*, volume 7966 of *Lecture Notes in Computer Science*, pages 137–149, Riga, Lituania, July 2013. Springer.

[ACKR13] Myrto Arapinis, Véronique Cortier, Steve Kremer, and Mark D. Ryan. Practical Everlasting Privacy. In David Basin and John Mitchell, editors, *Proceedings of the 2nd Conferences on Principles of Security and Trust (POST'13)*, volume 7796 of *Lecture Notes in Computer Science*, pages 21–40, Rome, Italy, March 2013. Springer.

[BCPW12] David Bernhard, Véronique Cortier, Olivier Pereira, and Bogdan Warinschi. Measuring vote privacy, revisited. In *19th ACM Conference on Computer and Communications Security (CCS'12)*, pages 941–952, Raleigh, USA, October 2012. ACM.

[CSW12] Véronique Cortier, Graham Steel, and Cyrille Wiedling. Revoke and let live : A secure key revocation api for cryptographic devices. In *19th ACM Conference on Computer and Communications Security (CCS'12)*, pages 918–928, Raleigh, USA, October 2012. ACM.

[CCS12] Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. Security proof with dishonest keys. In *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)*, volume 7215 of *Lecture Notes in Computer Science*, pages 149–168, Tallinn, Estonia, March 2012. Springer.

[CDD12] Véronique Cortier, Jan Degrieck, and Stéphanie Delaune. Analysing routing protocols : four nodes topologies are sufficient. In *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)*, volume 7215 of *Lecture Notes in Computer Science*, pages 30–50, Tallinn, Estonia, March 2012. Springer.

[CW12] Véronique Cortier and Cyrille Wiedling. A formal analysis of the norwegian e-voting protocol. In *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)*, volume 7215 of *Lecture Notes in Computer Science*, pages 109–128, Tallinn, Estonia, March 2012. Springer.

[CW11a] Véronique Cortier and Bogdan Warinschi. A composable computational soundness notion. In *18th ACM Conference on Computer and Communications Security (CCS'11)*, pages 63–74, Chicago, USA, October 2011. ACM.

[BCP+11] David Bernhard, Véronique Cortier, Olivier Pereira, Ben Smyth, and Bogdan Warinschi. Adapting helios for provable ballot secrecy. In Springer, editor, *Proceedings of the 16th European Symposium on Research in Computer Security (ESORICS'11)*, volume 6879 of *Lecture Notes in Computer Science*, 2011.

[CC11] Hubert Comon-Lundh and Véronique Cortier. How to prove security of communication protocols ? a discussion on the soundness of formal models w.r.t. computational ones. In Christoph Dürr and Thomas Schwentick, editors, *Proceedings of the 28th Annual Symposium on Theoretical Aspects of Computer Science (STACS'11)*, volume 9 of *Leibniz International Proceedings in Informatics*, pages 29–44, Dortmund, Germany, March 2011. Leibniz-Zentrum für Informatik.

[CS11] Véronique Cortier and Ben Smyth. Attacking and fixing helios : An analysis of ballot secrecy. In *Proceedings of the 24th IEEE Computer Security Foundations Symposium (CSF'11)*. IEEE Computer Society Press, June 2011.

[ACD11a] Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Deciding security for protocols with recursive tests. In Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors, *Proceedings of the 23rd International Conference on Automated Deduction (CADE'11)*, Lecture Notes in Artificial Intelligence, pages 49–63, Wrocław, Poland, July 2011. Springer.

[CC10] Ştefan Ciobâcă and Véronique Cortier. Protocol composition for arbitrary primitives. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 322–336, Edinburgh, Scotland, UK, July 2010. IEEE Computer Society Press. Erratum.

[ACD10] Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Modeling and verifying ad hoc routing protocols. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 59–74, Edinburgh, Scotland, UK, July 2010. IEEE Computer Society Press.

[CS09a] Véronique Cortier and Graham Steel. A generic security API for symmetric key management on cryptographic devices. In Michael Backes and Peng Ning, editors, *Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS'09)*, volume 5789 of *Lecture Notes in Computer Science*, pages 605–620, Saint Malo, France, September 2009. Springer.

[CD09a] Véronique Cortier and Stéphanie Delaune. A method for proving observational equivalence. In *Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF'09)*, pages 266–276, Port Jefferson, NY, USA, July 2009. IEEE Computer Society Press.

[BCD09] Mathieu Baudet, Véronique Cortier, and Stéphanie Delaune. YAPA : A generic tool for computing intruder knowledge. In Ralf Treinen, editor, *Proceedings of the 20th International Conference on Rewriting Techniques and Applications (RTA'09)*, volume 5595 of *Lecture Notes in Computer Science*, pages 148–163, Brasília, Brazil, 2009. Springer.

[Cor09b] Véronique Cortier. Verification of security protocols. In *10th Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI'09)*, volume 5403 of *Lecture Notes in Computer Science*, pages 5–13, Savanah, USA, January 2009. Springer. (Invited Tutorial).

[CC08] Hubert Comon-Lundh and Véronique Cortier. Computational soundness of observational equivalence. In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS'08)*, pages 109–118, Alexandria, Virginia, USA, October 2008. ACM Press.

[CDD07a] Véronique Cortier, Jérémie Delaitre, and Stéphanie Delaune. Safely composing security protocols. In V. Arvind and Sanjiva Prasad, editors, *Proceedings of the 27th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'07)*, volume 4855 of *Lecture Notes in Computer Science*, pages 352–363, New Delhi, India, December 2007. Springer.

[CWZ07b] Véronique Cortier, Bogdan Warinschi, and Eugen Zalinescu. Synthetizing secure protocols. In *Proceedings of the 12th European Symposium On Research In Computer Security (ESORICS'07)*, volume 4734, pages 406–421, Dresden, Germany, September 2007. Springer.

[CKW07a] Véronique Cortier, Ralf Küsters, and Bogdan Warinschi. A cryptographic model for branching time security properties – the case of contract signing protocols. In *Proceedings of the 12th European Symposium On Research In Computer Security (ESORICS'07)*, volume 4734, pages 422–437, Dresden, Germany, September 2007. Springer.

[CD07a] Véronique Cortier and Stéphanie Delaune. Deciding knowledge in security protocols for monoidal equational theories. In Nachum Dershowitz and Andrei Voronkov, editors, *Proceedings of the 14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'07)*, volume 4790 of *Lecture Notes in Artificial Intelligence*, pages 196–210, Yerevan, Armenia, October 2007. Springer.

[ACD07a] Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Combining algorithms for deciding knowledge in security protocols. In Franck Wolter, editor, *Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS'07)*, volume 4720 of *Lecture Notes in Artificial Intelligence*, pages 103–117, Liverpool, UK, September 2007. Springer.

[CDS07b] Véronique Cortier, Stéphanie Delaune, and Graham Steel. A formal theory of key conjuring. In *Proceedings of the 20th IEEE Computer Security Foundations Symposium (CSF'07)*, pages 79–93, Venice, Italy, July 2007. IEEE Computer Society Press.

[CKS07] Véronique Cortier, Gavin Keighren, and Graham Steel. Automatic analysis of the security of XOR-based key management schemes. In Orna Grumberg and Michael Huth, editors, *Proceedings of the 13th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'07)*, volume 4424 of *Lecture Notes in Computer Science*, pages 538–552, Braga, Portugal, March 2007. Springer.

[CKKW06] Véronique Cortier, Steve Kremer, Ralf Küsters, and Bogdan Warinschi. Computationally sound symbolic secrecy in the presence of hash functions. In Naveen Garg and S. Arun-Kumar, editors, *Proceedings of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'06)*, volume 4337 of *Lecture Notes in Computer Science*, pages 176–187, Kolkata, India, December 2006. Springer.

[CZ06] V. Cortier and E. Zalinescu. Deciding key cycles for security protocols. In *Proceedings of the 13th Int. Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'06)*, volume 4246 of *Lecture Notes in Artificial Intelligence*, pages 317–331, Phnom Penh, Cambodia, November 2006. Springer.

[CRZ06] V. Cortier, M. Rusinowitch, and E. Zalinescu. Relating two standard notions of secrecy. In Zoltan Esik, editor, *Proceedings of 20th Int. Conference on Computer Science Logic (CSL'06)*, volume 4207 of *Lecture Notes in Computer Science*, pages 303–318, Szeged, Hungary, September 2006. Springer.

[BCK05] Mathieu Baudet, Véronique Cortier, and Steve Kremer. Computationally sound implementations of equational theories against passive adversaries. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, volume 3580 of *Lecture Notes in Computer Science*, pages 652–663, Lisboa, Portugal, July 2005. Springer.

[CRZ05] V. Cortier, M. Rusinowitch, and E. Zalinescu. A resolution strategy for verifying cryptographic protocols with CBC encryption and blind signatures. In *Proceedings of the 7th ACM-SIGPLAN International Conference on Principles and Practice of Declarative Programming (PPDP'05)*, pages 12–22, Lisboa, Portugal, July 2005. ACM press.

[AC05] M. Abadi and V. Cortier. Deciding knowledge in security protocols under (many more) equational theories. In *Proc. 18th IEEE Computer Security Foundations Workshop (CSFW'05)*, pages 62–76, Aix-en-Provence, France, June 2005. IEEE Comp. Soc. Press.

[CW05] V. Cortier and B. Warinschi. Computationally sound, automated proofs for security protocols. In *Proceedings of the 14th European Symposium on Programming (ESOP'05)*, volume 3444 of *Lecture Notes in Computer Science*, pages 157–171, Edinburgh, U.K, April 2005. Springer.

[AC04a] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. In *Proceedings of the 31st Int. Coll. Automata, Languages, and Programming (ICALP'2004)*, volume 3142 of *Lecture Notes in Computer Science*, pages 46–58, Turku, Finland, July 2004. Springer.

[CC03a] Hubert Comon-Lundh and Véronique Cortier. New decidability results for fragments of first-order logic and application to cryptographic protocols. In Robert Nieuwenhuis, editor, *Proceedings of the 14th International Conference on Rewriting Techniques and Applications (RTA'03)*, volume 2706 of *Lecture Notes in Computer Science*, pages 148–164, Valencia, Spain, June 2003. Springer.

[CC03b] Hubert Comon-Lundh and Véronique Cortier. Security properties : two agents are sufficient. In Pierpaolo Degano, editor, *Proceedings of the 12th European Symposium on Programming (ESOP'03)*, volume 2618 of *Lecture Notes in Computer Science*, pages 99–113, Warsaw, Poland, April 2003. Springer.

[CCM01] Hubert Comon, Véronique Cortier, and John Mitchell. Tree automata with one memory, set constraints and ping-pong protocols. In Fernando Orejas, Paul G. Spirakis, and Jan van Leeuwen, editors, *Proceedings of the 28th International Colloquium on Automata, Languages and Programming (ICALP'01)*, volume 2076 of *Lecture Notes in Computer Science*, pages 682–693, Heraklion, Crete, Grece, July 2001. Springer.

[CMR01] Véronique Cortier, Jonathan K. Millen, and Harald Rueß. Proving secrecy is easy enough. In *Proceedings of the 14th IEEE Computer Security Foundations Workshop (CSFW'01)*, pages 97–110, Cape Breton, Nova Scotia, Canada, June 2001. IEEE Computer Society Press.

[CC00] Hubert Comon and Véronique Cortier. Flatness is not a weakness. In Peter Clote and Helmut Schwichtenberg, editors, *Proceedings of the 14th International Workshop*

on Computer Science Logic (CSL 2000), volume 1862 of *Lecture Notes in Computer Science*, pages 262–276, Fischbachau, Germany, August 2000. Springer.

[CGJV99] Véronique Cortier, Harald Ganzinger, Florent Jacquemard, and Margus Veanes. Decidable fragments of simultaneous rigid reachability. In Jirí Wiedermann, Peter van Emde Boas, and Mogens Nielsen, editors, *Proceedings of the 26th International Colloquium on Automata, Languages and Programming (ICALP'99)*, volume 1644 of *Lecture Notes in Computer Science*, pages 250–260, Prague, Czech Republic, July 1999. Springer.

Workshops

[CLCS14] Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. A tool for automating the computationally complete symbolic attacker (extended abstract). In *Joint Workshop on Foundations of Computer Security and Formal and Computational Cryptography (FCS-FCC'14)*, Vienna, Austria, July 2014.

[CDG+11] Véronique Cortier, Jérémie Detrey, Pierrick Gaudry, Frédéric Sur, Emmanuel Thomé, Mathieu Turuani, and Paul Zimmermann. Ballot stuffing in a postal voting system. In *Revote 2011 - International Workshop on Requirements Engineering for Electronic Voting Systems*, Trento, Italie, 2011. IEEE.

[CW11b] Véronique Cortier and Bogdan Warinschi. A composable computational soundness notion (abstract). In *7th Workshop on Formal and Computational Cryptography (FCC 2011)*, Paris, France, June 2011.

[ACD09] Mathilde Arnaud, Véronique Cortier, and Stéphanie Delaune. Modeling and verifying ad hoc routing protocol. In Hubert Comon-Lundh and Catherine Meadows, editors, *Preliminary Proceedings of the 4th International Workshop on Security and Rewriting Techniques (SecReT'09)*, pages 33–46, Port Jefferson, NY, USA, July 2009.

[CD07b] Véronique Cortier and Stéphanie Delaune. Deciding knowledge in security protocols for monoidal equational theories. In Pierpaolo Degano, Ralf Küsters, Luca Viganò, and Steve Zdancewic, editors, *Proceedings of the Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA'07)*, pages 63–80, Wrocław, Poland, July 2007.

[CKW07b] Véronique Cortier, Ralf Küsters, and Bogdan Warinschi. A cryptographic model for branching time security properties – the case of contract signing protocols. In *3rd Workshop on Formal and Computational Cryptography (FCC 2007)*, Venice, Italy, July 2007.

[CZ07] Véronique Cortier and Eugen Zalinescu. Deciding key cycles for security protocols. In *3rd Workshop on Formal and Computational Cryptography (FCC 2007)*, Venice, Italy, July 2007.

[CS06] Véronique Cortier and Graham Steel. On the decidability of a class of xor-based key-management APIs. In *Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA'06)*, Seattle, Washington, August 2006.

[CHW07] Véronique Cortier, Heinrich Hördegen, and Bogdan Warinschi. Explicit randomness is not necessary when modeling probabilistic encryption. In *Workshop on Information and Computer Security (ICS 2006)*, volume 186 of *Electronic Notes Theoretical Computer Science*, pages 49–65, Timisoara, Romania, September 2007.

Scientific Popularization (in French)

[BCC+20] Xavier Bonnetain, Anne Canteaut, Véronique Cortier, Pierrick Gaudry, Lucca Hirschi, Steve Kremer, Stéphanie Lacour, Matthieu Lequesne, Gaëtan Leurent, Léo Perrin, André Schrottenloher, Emmanuel Thomé, Serge Vaudenay, and Christophe Vuillot. Le traçage anonyme, dangereux oxymore. April 2020.

[CGG18] Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu. (a voté) euh non : a cliqué. In *Blog Binaire*. Le Monde, March 2018.

[Cor16] Véronique Cortier. Vote électronique. In *1024 – Bulletin de la société informatique de France*, number 9. November 2016.

[Cor15e] Véronique Cortier. Vote électronique : un scrutin à sécuriser. *La Recherche*, 504 :70–73, October 2015.

[Cor15a] Véronique Cortier. Attaque à l'italienne. In *Blog Binaire*. Le Monde, August 2015.

[CK15] Véronique Cortier and Steve Kremer. Les bonnes propriétés d'un système de vote électronique - exemple d'Helios. In *Blog Binaire*. Le Monde, March 2015.

[Cor15c] Véronique Cortier. Le vote papier est-il réellement plus sûr que l'électronique ? In *Blog Binaire*. Le Monde, January 2015.

[Cor15d] Véronique Cortier. Qu'est-ce qu'un bon système de vote ? In *Blog Binaire*. Le Monde, January 2015.

[CK13] Véronique Cortier and Steve Kremer. Vote par internet. In *Interstices*. January 2013. Updated in March 2017.

[Cor06a] Véronique Cortier. Ces protocoles qui nous protègent. *Tangente*, Hors-série 26 :42–44, July 2006.

[Cor06c] Véronique Cortier. Divers protocoles couramment utilisés en informatique. *Tangente*, Hors-série 26 :45, July 2006.

[Cor06d] Véronique Cortier. Protocoles cryptographiques : analyse par méthodes formelles. In *Techniques de l'ingénieur*, volume dossier AF176, chapter Bases documentaires "Mathématiques pour l'ingénieur". April 2006.

Other Publications

[Cor09a] Véronique Cortier. *Analysis of cryptographic protocols : from symbolic to computational models*. Habilitation à diriger des recherches (habilitation to conduct research), Institut National Polytechnique de Lorraine, November 2009.

[Cor03b] Véronique Cortier. *Vérification automatique des protocoles cryptographiques*. Thèse de doctorat (PhD thesis), Laboratoire Spécification et Vérification, ENS Cachan, France, March 2003.