Stéphanie Delaune

☎ *(+33) 2 99 84 75 27*
✉ *stephanie.delaune@irisa.fr*
http://people.irisa.fr/Stephanie.Delaune

IRISA - Campus universitaire de Beaulieu
263 Avenue du Général Leclerc
35042 Rennes Cedex - France

Birth date: September 26th, 1980
French citizen
2 children

Curriculum Vitae

▶ **Since Sept. 2016** CNRS researcher at IRISA, UMR 6074 **(DR2 since 2017)**

▶ **2007-2016** CNRS researcher (CR1 since 2011) at LSV, UMR 8643, ENS Cachan

▷ **March 2011: Habilitation thesis** on

« *Verification of security protocols: from confidentiality to privacy* »

Jury members: Martìn Abadi, David Basin, Gérard Berry, Bruno Blanchet, Hubert Comon-Lundh, Claude Kirchner, Ralf Küsters, and John Mitchell.

▶ **2006-2007** Post-doctoral researcher at LORIA in Nancy (9 months) and at Birmingham University (4 months)

▶ **2003-2006** PhD student (CIFRE grant) at:

- Laboratoire Spécification et Vérification (LSV), ENS Cachan & CNRS,
- Laboratoire Middleware et Plates-Formes Avancées (MAPS), France Télécom R&D.

« *Verification of Cryptographic Protocols with algebraic properties* »

Co-advisors Hubert Comon-Lundh and Francis Klay.

▷ 2004-2006: "Monitorat" at the University Denis Diderot (Paris VII)

▶ **1998-2003** Student at the University Denis Diderot (Paris VII).

Awards:

- **Outstanding community service award** from the IEEE technical committee on Security and Privacy, 2019.
- EASST **best paper award** at ETAPS 2016 with V. Cortier and A. Dallon.
- **Outstanding PhD thesis** from France Télécom R&D in 2006.

Research themes: My area of research is the formal analysis and design of security protocols. I use techniques issued from automated reasoning, rewriting, model-checking, and concurrency theory to model and analyse the *cryptographic protocols*. After my Ph.D., I led an effort to formally define and analyse security properties in electronic voting protocols, and especially those related to *privacy*, such as vote-privacy and different flavours of coercion-resistance. These techniques have also been applied to analyse several protocols that are deployed in *contactless systems* like e-passport, and mobile phones.

Publications: **23** international journals, **55** international conferences, and 3 book chapters.

Management and participation in research projects

Ongoing projects:

- ANR DeCrypt, member (2019-2023)
  Declarative approach for Symmetric Cryptography
- ANR TECAP, **local PI** (2018-2022)
  Protocol Analysis - Combining Existing Tools
- ERC Starting Grant POPSTAR, **PI** (2017-2022)
  Reasoning about Physical properties Of security Protocols with an Application To contactless Systems

Some past projects:

- ANR Sequoia, member (2014-2019)
  Security properties, process equivalences and automated verification
- Inria Project Lab on Privacy Cappris, member (2013-2016)
  Collaborative Action on the Protection of Privacy Rights in the Information Society
- ANR JCJC VIP, **PI** (2012-2016), *Verification of Indistinguishability Properties.*
- ANR ProSe member, (2010-2014), *Security Protocols : formal model, computational model, and implementations.*
- ANR AVOTE, member (2008-2011), *Analyse formelle de protocoles de vote électronique.*
- ARA SSIA FormaCrypt, member (2006-2009).
- EPSRC EP/E029833 project, **co-head** (2006), *Verifying properties in electronic voting protocols.*
- ACI Rossignol, member (2003-2006),
  Sémantique de la vérification des protocoles cryptographiques: théorie et applications.
- RNTL PROUVE, member (2003-2006), *PRotocoles cryptographiques: OUtils de VErification automatique.*

Supervision of students

PhD Students:

- Joshua Peignier (sept. 2019-) with co-advisor V. Cortier.
- Solène Moreau (sept. 2018-) with co-advisor D. Baelde.
- Alexandre Debant (sept. 2017-).
- Antoine Dallon (nov. 2015-nov. 2018) with co-advisor V. Cortier, now scientific expert at DGA-MI.
- Ludovic Robin (sept. 2014-feb. 2018) with co-advisor S. Kremer.
- Lucca Hirschi (sept. 2013-april 2016) with co-advisor D. Baelde, now CR Inria at LORIA.
- Rémy Chrétien (oct. 2012-jan. 2016) with co-advisor V. Cortier, now scientific expert at the Ministery of Defense.
- Vincent Cheval (sept. 2009-dec. 2012) with co-advisor H. Comon-Lundh, now CR Inria at LORIA.
- Mathilde Arnaud (sept. 2008-oct. 2011) with co-advisor V. Cortier, now engineer at CEA in France.
- Sergiu Bursuc (sept. 2006-dec. 2009) with co-advisor H. Comon-Lundh, now postdoc at LORIA.

Postdocs:

- Vaishnavi Sundararajan (nov. 2018-).
- Cyrille Wiedling (feb. 2017-sept. 2017), now scientific expert at DGA-MI.
- Ivan Gazeau (jun. 2015-jun. 2016) , now postdoc at LORIA.
- Céline Chevalier (sept. 2010-sept. 2011), now assistant professor at University Paris II.
- Myrto Arapinis (sept. 2007-nov. 2008), now lecturer at Edinburgh University.

Master students:

Joshua Peignier (2019), Léo Chartier (2017), Alexandre Debant (2017), Antoine Dallon (2015), Ludovic Robin (2014), Lucca Hirschi (2013), Apoorvaa Desphande (2012), Rémy Chrétien (2012), Jan Degrieck (2011), Daniel Pasaila (2011), Vincent Cheval (2009), Stefan Ciobaca (2008), Jérémie Delaitre (2007).

Teaching activities

Lectures:

- Project at INSA (4ème année) (30h. 2019).
- Master course « *Vérification de protocoles* » at INSA (14h, 2017 & 2018 & 2019), and MRI Rennes (10h, 2017 & 2018 & 2019).
- Course « *Regards Croisés* » (level L3), ENS Cachan, (3h, 2008-2015).
- Master course at MPRI « *Cryptographic protocols* », (9h, 2008) & (15h, 2010) & (12h, 2011) & (24h, 2014).

Summer schools

- Lecture at EJCP summer school, Lyon, France, June 2018.
- Lecture at FOSAD summer school, Bertinoro, Italy, September 2017.
- Lecture at EJCP summer school, Toulouse, France, June 2017.
- Lecture at the 6th Summer School on Formal Techniques, Menlo College, CA, USA, May 2017.
- Lecture at the spring school on Security & Correctness in the IoT, Graz, Austria, May 2017.
- Lecture at EJCP summer school, Lille, France, June 2016.
- Lecture at VTSA summer school, Koblenz, Germany, August 2015.
- Focus talk at MOVEP summer school, Nantes, France, July 2014.
- Lecture at SecVote, Bertinoro, Italy, September 2010.

Popularization

- Invited talk at the Colloquium Sécurité informatique: mythes et réalité, Paris, France, December 2016.
- Invited talk at ENS Rennes, Bruz, France, September 2016.
- Invited talk for the last round of the Alkindi competition, Hotel des Invalides, Paris, May 2016.
- **Seminar at Collège de France**, Paris, April 2016.
- Invited talk at Lycée Corot, Savigny-sur-Orge, France, March 2014.
- Seminar at the plenary session of INS2I, Paris, France, June 2014.
- Seminar (conférence de rentrée), ENS Cachan, France, September 2012.
- Invited talk at the regional annual day of the APMEP, Rouen, France, April 2012.
- Invited talk at Unithé ou Café?, Parc Orsay Université, France, November 2011.
- Invited talk at the national annual days of the APMEP, Grenoble, France, October 2011.
- Invited talk for the ceremony of awards "Olympiades de Mathématiques", Cachan, France, May 2008.
- Public debate on electronic voting machine, « fête de la science », October 2007.

Participation to committees

Editorships

- Information Processing Letters (IPL), editorial board since 2019.
- ACM Transactions on Computational Logic (TOCL), editorial board since 2018.

Steering committees:

- Programming Languages and Analysis for Security (PLAS), member since 2018.
- Principles of Security and Trust (POST), member 2018-2020.
- Computer Security Foundations Symposium (CSF), member since 2017.
- Scientific council GdR-IM, member since 2018.
- Bureau GDR Sécurité Informatique, member since 2017.
- Formal methods for security – working group GDR Sécurité Informatique, **co-head** since 2017.
- IFIP Wg-1.7 Foundations of Security Analysis, member since 2016.

Program committees: 11 international workshops and **31 international conferences** that are listed below:

- *2020:* DATE.
- *2019:* CSF **(PC co-chair)**, SEC@SAC, ESORICS.
- *2018:* POST, CSF **(PC co-chair)**, MFCS, PLAS **(PC co-chair)**, E-VoteID.
- *2017:* POST, CSR, CADE, CSF, FST&TCS.
- *2016:* IJCAR.
- *2015:* SOFSEM, CADE, FORTE, RTA, FST&TCS.
- *2014:* POST, IJCAR, TGC, CONCUR.
- *2013:* CADE, CSF, RTA.

– *2012:* ISPEC.
– *2011:* FST&TCS, CSF, CCS, CADE.

Organization committees:
– member of the organization of *FutureDB - Distance-bounding: past, present, future*, April 2018 *(around 35 attendees)*.
– member of the local organisation of the 24th IEEE Computer Security Foundations symposium (CSF'11), June 2011 *(around 90 attendees)*.
– member of the local organisation of the 37th spring school on theoretical computer science (CoSyProofs'10), April 2010 *(around 60 attendees)*.
– member of the local organisation of several colloquiums that took place in Cachan (Paris area): **1**/ Workshop in honour of Martín Abadi, June 2015 *(around 100 attendees)*; **2**/ SecSI Colloquium, March 2011 *(around 100 attendees)*; **3**/ Workshop in honour of Hubert Comon-Lundh, November 2008 *(around 150 attendees)*; **4**/ Workshop "*10 Years of Verification in Cachan*", November 2007 *(around 150 attendees)*.
– Principal organizer of the 3-day annual internal seminar of the LSV from 2008 to 2012 *(around 50 attendees)*.

HdR Defense committees:
– Céline Chevalier as examiner, December 2017.

PhD Defense committees:
– Jorge Toro-Pozo as reviewer, May 2019.
– Nadim Kobeissi as reviewer, Dec. 2018.
– Maxime Audinot as president, Dec. 2018.
– Alix Trieu as president, Dec. 2018.
– Florian Lugou as reviewer, Feb. 2018.
– Miriam Paiola as reviewer, May 2014.
– Mario Alvim as examiner, Oct. 2011.
– Myrto Arapinis as examiner, Nov. 2008.

Hiring committees:
– Member of several hiring committees (professor position): ENS Ulm (2018), Polytechnique (2018).
– Member of several hiring committees (assistant professor position): Paris Denis Diderot (2018), ENS Ulm (2017), IUT Limoges (2017), University Versailles Saint Quentin (2016), Chaire X/CNRS (2011), University Lille I (2009).
– Member of the committee for evaluating and selecting PhD students at IRISA (2016).
– Member of the committee for evaluating and selecting PhD students at the doctoral school Paris Saclay (2015 & 2016).
– Member of the scientific committee at Inria Saclay (2012-2016) in charge of awarding grants for post-doc and phd positions (around 5 each year).

Reviewing activities

Research articles: I review more than 20 papers each year for leading journals, conferences and workshops.

Research projects:
– Reviewer for several national projects: French ANR (2012 & 2014), Luxembourguish FNR (2015), Austria (2019), Germany (2019).
– Committee member for the ANR generic call in 2015 & 2016.
$\longrightarrow$ *2-day meeting to evaluate and rank about 60 proposals.*

PhD proposals:
– Reviewer of 4 PhD proposals for the national center of excellence in cybersecurity (2016).

- Reviewer of several proposals from the ANRT (CIFRE grants).

Other responsabilities

- Member of the scientific council GdR-IM (since 2017).
- Member of the laboratory council at IRISA (2017-2018).
- Member of the management committees of LSV (2012-2016).
- Member of various committees of the Doctoral School Paris-Saclay (2015-2016).
- Member of the EDSP doctoral school committee (2012-2015).
- Déléguée aux thèses in computer science at EDSP (2012-2014).
- Organizer of the SECSI internal seminar from (2008-2010).

Invited talks and seminars

Below, the talks that I have given since **January 2010**. A full list is available on my web page:

`http://people.irisa.fr/Stephanie.Delaune/talks.html`

- Invited talk at Luxembourg University, May 2019.
- Invited talk at FSCD, Oxford, UK, July 2018.
- Invited talk at FutureDB - Distance-bounding: past, present, future, Azore, Portugal, April 2018.
- Seminar at SoSysec, Rennes, France, March 2017.
- Les rencontres du numérique de l'ANR, Paris, France, November 2016.
- Talk at Security day of the CominLabs, Rennes, France, September 2016.
- Invited talk at the Sasefor meeting, Cachan, France, April 2015.
- Seminar at Deducteam (Inria Rocquencourt), Paris, France, March 2015.
- Seminar at GREYC laboratory, Caen, France, January 2015.
- Invited talk at the TRENDS workshop, Roma, Italy, September 2014.
- Invited talks at the CAPPRIS meeting, Paris, France, March 2012 & March 2014.
- Talk during the Open Day of LSV, ENS Cachan, France, September 2013.
- Talks at the SECSI Working Group, ENS Cachan, France, January & October 2012, & June 2013.
- Talk at the CAPPRIS meeting, Paris, France, March 2012.
- Talk at the SECSI Working Group, ENS Cachan, France, January 2012.
- Dagstuhl seminar, Germany, August 2011.
- Seminar at Verimag, Grenoble, June 2011.

Publications

23 papers in international journals and 55 papers in international conferences. Below the list of my papers that have been accepted and/or published **since January 2010**. The full list of my publications is available on my web page:

`http://people.irisa.fr/Stephanie.Delaune/PUBLICATIONS-HTML/pub_type.html`

Chapters in Book

H. Comon-Lundh and S. Delaune. Formal security proofs. In T. Nipkow, O. Grumberg, and B. Hauptmann, editors, *Software Safety and Security*, volume 33 of *NATO Science for Peace and Security Series – D: Information and Communication Security*, pages 26–63. IOS Press, May 2012.

H. Comon-Lundh, S. Delaune, and J. K. Millen. Constraint solving techniques and enriching the model with equational theories. In V. Cortier and S. Kremer, editors, *Formal Models and Techniques for Analyzing Security Protocols*, volume 5 of *Cryptology and Information Security Series*, pages 35–61. IOS Press, 2011.

S. Delaune, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols: A taster. In D. Chaum, M. Jakobsson, R. L. Rivest, P. Y. A. Ryan, J. Benaloh, M. Kutyłowski, and B. Adida, editors, *Towards Trustworthy Elections – New Directions in Electronic Voting*, volume 6000 of *Lecture Notes in Computer Science*, pages 289–309. Springer, May 2010.

Scientific popularization

S. Delaune. POPSTAR: so near and yet so far. *SIGLOG News*, 5(3):45–51, 2018.

S. Delaune. Protection des donnés: le chiffrement ne suffit pas. *Journal du CNRS*, Dec. 2016.

R. Chrétien and S. Delaune. Le bitcoin, une monnaie 100% numérique. *Interstices*, Sept. 2014.

R. Chrétien and S. Delaune. Le bitcoin, une monnaie 100% numérique. *Blog Binaire*, Apr. 2014.

R. Chrétien and S. Delaune. La protection des informations sensibles. *Pour La Science*, 433:70–77, Nov. 2013.

S. Delaune. Le vote électronique. *La Recherche Magazine*, Sept. 2010.

International Journals

L. Hirschi, D. Baelde, and S. Delaune. A method for unbounded verification of privacy-type properties. *Journal of Computer Security*, 27(3):277–342, 2019.

R. Chrétien, V. Cortier, A. Dallon, and S. Delaune. Typing messages for free in security protocols. *ACM Transactions on Computational Logic (TOCL)*, 2019.

D. Baelde, S. Delaune, and L. Hirschi. A reduced semantics for deciding trace equivalence. *Logical Methods in Computer Science*, 13(2), 2017.

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.

L. Hirschi and S. Delaune. A survey of symbolic methods for establishing equivalence-based properties in cryptographic protocols. *Journal of Logical and Algebraic Methods in Programming*, 87:127–144, 2017.

R. Chrétien, V. Cortier, and S. Delaune. From security protocols to pushdown automata. *ACM Transactions on Computational Logic*, 17(1:3), Sept. 2015.

M. Arapinis, S. Delaune, and S. Kremer. Dynamic tags for security protocols. *Logical Methods in Computer Science*, 10(2:11), June 2014.

M. Arnaud, V. Cortier, and S. Delaune. Modeling and verifying ad hoc routing protocols. *Information and Computation*, 238:30–67, Nov. 2014.

S. Bursuc, H. Comon-Lundh, and S. Delaune. Deducibility constraints and blind signatures. *Information and Computation*, 238:106–127, Nov. 2014.

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

C. Chevalier, S. Delaune, S. Kremer, and M. D. Ryan. Composition of password-based protocols. *Formal Methods in System Design*, 43(3):369–413, Dec. 2013.

M. Baudet, V. Cortier, and S. Delaune. YAPA: A generic tool for computing intruder knowledge. *ACM Transactions on Computational Logic*, 14(1:4), Feb. 2013.

Ş. Ciobâcă, S. Delaune, and S. Kremer. Computing knowledge in security protocols under convergent equational theories. *Journal of Automated Reasoning*, 48(2):219–262, Feb. 2012.

V. Cortier and S. Delaune. Decidability and combination results for two notions of knowledge in security protocols. *Journal of Automated Reasoning*, 48(4):441–487, Apr. 2012.

S. Delaune, S. Kremer, and G. Steel. Formal analysis of PKCS#11 and proprietary extensions. *Journal of Computer Security*, 18(6):1211–1245, Nov. 2010.

International Conferences

A. Debant and S. Delaune. Symbolic verification of distance bounding protocols. In *Proceedings of the 8th International Conference on Principles of Security and Trust (POST'19)*, Lecture Notes in Computer Science, Prague, Czech Republic, 2019. Springer.

A. Debant, S. Delaune, and C. Wiedling. Symbolic analysis of terrorist fraud resistance. In *Proceedings of the 24th European Symposium on Research in Computer Security (ESORICS'19)*, Lecture Notes in Computer Science, Luxembourg, 2019. Springer.

S. Delaune. Analysing privacy-type properties in cryptographic protocols (invited talk). In H. Kirchner, editor, *3rd International Conference on Formal Structures for Computation and Deduction, (FSCD'18)*, volume 108 of *LIPIcs*, Oxford, UK, 2018. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik.

D. Baelde, S. Delaune, and L. Hirschi. POR for security protocol equivalences – beyond action-determinism. In *Proceedings of the 23rd European Symposium on Research in Computer Security (ESORICS'18)*, Lecture Notes in Computer Science, Barcelona, Spain, 2018. Springer.

V. Cortier, A. Dallon, and S. Delaune. Efficiently deciding equivalence for standard primitives and phases. In *Proceedings of the 23rd European Symposium on Research in Computer Security (ESORICS'18)*, Lecture Notes in Computer Science, Barcelona, Spain, 2018. Springer.

A. Debant, S. Delaune, and C. Wiedling. A symbolic framework to analyse physical proximity in security protocols. In *38th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS'18)*, LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

V. Cortier and S. Dallon, Antoine Delaune. Sat-equiv: an efficient tool for equivalence properties. In *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'17)*, Santa Barbara, CA, USA, Aug. 2017. IEEE Computer Society Press.

S. Delaune, S. Kremer, and L. Robin. Formal verification of protocols based on short authenticated strings. In *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'17)*, Santa Barbara, CA, USA, Aug. 2017. IEEE Computer Society Press.

D. Baelde, S. Delaune, I. Gazeau, and S. Kremer. Symbolic verification of privacy-type properties for security protocols with xor. In *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'17)*, Santa Barbara, CA, USA, Aug. 2017. IEEE Computer Society Press.

L. Hirschi, D. Baelde, and S. Delaune. A method for verifying privacy-type properties: the unbounded case. In M. Locasto, V. Shmatikov, and Ú. Erlingsson, editors, *Proceedings of the 37th IEEE Symposium on Security and Privacy (S&P'16)*, San Jose, California, USA, May 2016. IEEE Computer Society Press.

V. Cortier, A. Dallon, and S. Delaune. Bounding the number of agents, for equivalence too. In F. Piessens and L. 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, Apr. 2016. Springer.

R. Chrétien, V. Cortier, and S. Delaune. Checking trace equivalence: How to get rid of nonces? In P. Ryan and E. Weippl, editors, *Proceedings of the 20th European Symposium on Research in Computer Security (ESORICS'15)*, Lecture Notes in Computer Science, pages 230–251, Vienna, Austria, Sept. 2015. Springer.

D. Baelde, S. Delaune, and L. Hirschi. Partial order reduction for security protocols. In L. Aceto and D. de Frutos-Escrig, editors, *Proceedings of the 26th International Conference on Concurrency Theory (CONCUR'15)*, volume 42 of *Leibniz International Proceedings in Informatics*, pages 497–510, Madrid, Spain, Sept. 2015. Leibniz-Zentrum für Informatik.

R. Chrétien, V. Cortier, and S. Delaune. Decidability of trace equivalence for protocols with nonces. In *Proceedings of the 28th IEEE Computer Security Foundations Symposium (CSF'15)*, pages 170–184, Verona, Italy, July 2015. IEEE Computer Society Press.

M. Arapinis, V. Cheval, and S. Delaune. Composing security protocols: from confidentiality to privacy. In R. Focardi and A. Myers, editors, *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, London, UK, Apr. 2015. Springer.

D. Baelde, S. Delaune, and L. Hirschi. A reduced semantics for deciding trace equivalence using constraint systems. In M. Abadi and S. Kremer, editors, *Proceedings of the 3rd International Conference on Principles of Security and Trust (POST'14)*, volume 8414 of *Lecture Notes in Computer Science*, pages 1–21, Grenoble, France, Apr. 2014. Springer.

R. Chrétien, V. Cortier, and S. Delaune. Typing messages for free in security protocols: the case of equivalence properties. In P. Baldan and D. Gorla, editors, *Proceedings of the 25th International Conference on Concurrency Theory (CONCUR'14)*, volume 8704 of *Lecture Notes in Computer Science*, pages 372–386, Rome, Italy, Sept. 2014. Springer.

V. Cheval, S. Delaune, and M. D. Ryan. Tests for establishing security properties. In M. Maffei and E. Tuosto, editors, *Revised Selected Papers of the 9th Symposium on Trustworthy Global Computing (TGC'14)*, volume 8902 of *Lecture Notes in Computer Science*, pages 82–96, Rome, Italy, Dec. 2014. Springer.

R. Chrétien, V. Cortier, and S. Delaune. From security protocols to pushdown automata. In F. V. Fomin, R. Freivalds, M. Kwiatkowska, and D. Peleg, editors, *Proceedings of the 40th International Colloquium on Automata, Languages and Programming (ICALP'13) – Part II*, volume 7966 of *Lecture Notes in Computer Science*, pages 137–149, Riga, Latvia, July 2013. Springer.

R. Chrétien and S. Delaune. Formal analysis of privacy for routing protocols in mobile ad hoc networks. In D. Basin and J. Mitchell, editors, *Proceedings of the 2nd International Conference on Principles of Security and Trust (POST'13)*, volume 7796 of *Lecture Notes in Computer Science*, pages 1–20, Rome, Italy, Mar. 2013. Springer.

V. Cortier, J. Degrieck, and S. Delaune. Analysing routing protocols: four nodes topologies are sufficient. In P. Degano and J. D. Guttman, editors, *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, Mar. 2012. Springer.

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, Cambridge Massachusetts, USA, June 2012. IEEE Computer Society Press.

S. Delaune, S. Kremer, and D. Pasailă. Security protocols, constraint systems, and group theories. In B. Gramlich, D. Miller, and U. Sattler, editors, *Proceedings of the 6th International Joint Conference on Automated Reasoning (IJCAR'12)*, volume 7364 of *Lecture Notes in Artificial Intelligence*, pages 164–178, Manchester, UK, June 2012. Springer-Verlag.

M. Arnaud, V. Cortier, and S. Delaune. Deciding security for protocols with recursive tests. In N. Bjørner and V. 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.

S. Delaune, S. Kremer, M. D. Ryan, and G. Steel. Formal analysis of protocols based on TPM state registers. In *Proceedings of the 24th IEEE Computer Security Foundations Symposium (CSF'11)*, pages 66–82, Cernay-la-Ville, France, June 2011. IEEE Computer Society Press.

M. Dahl, S. Delaune, and G. Steel. Formal analysis of privacy for anonymous location based services. In S. A. Mödersheim and C. Palamidessi, editors, *Revised Selected Papaers of the Workshop on Theory of Security and Applications (TOSCA'11)*, volume 6993 of *Lecture Notes in Computer Science*, pages 98–112, Saarbrücken, Germany, Jan. 2012. Springer.

V. Cheval, H. Comon-Lundh, and S. Delaune. Trace equivalence decision: Negative tests and non-determinism. In Y. Chen, G. Danezis, and V. Shmatikov, editors, *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)*, pages 321–330, Chicago, Illinois, USA, Oct. 2011. ACM Press.

C. Chevalier, S. Delaune, and S. Kremer. Transforming password protocols to compose. In S. Chakraborty and A. Kumar, editors, *Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11)*, volume 13 of *Leibniz International Proceedings in Informatics*, pages 204–216, Mumbai, India, Dec. 2011. Leibniz-Zentrum für Informatik.

S. Delaune, S. Kremer, M. D. Ryan, and G. Steel. A formal analysis of authentication in the TPM. In P. Degano, S. Etalle, and J. Guttman, editors, *Revised Selected Papers of the 7th International Workshop on Formal Aspects in Security and Trust (FAST'10)*, volume 6561 of *Lecture Notes in Computer Science*, pages 111–125, Pisa, Italy, Sept. 2010. Springer.

M. Dahl, S. Delaune, and G. Steel. Formal analysis of privacy for vehicular mix-zones. In D. Gritzalis and B. Preneel, editors, *Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10)*, volume 6345 of *Lecture Notes in Computer Science*, pages 55–70, Athens, Greece, Sept. 2010. Springer.

M. Arnaud, V. Cortier, and S. 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.

V. Cheval, H. Comon-Lundh, and S. Delaune. Automating security analysis: symbolic equivalence of constraint systems. In J. Giesl and R. Haehnle, editors, *Proceedings of the 5th International Joint Conference on Automated Reasoning (IJCAR'10)*, volume 6173 of *Lecture Notes in Artificial Intelligence*, pages 412–426, Edinburgh, Scotland, UK, July 2010. Springer-Verlag.

Habilitation Thesis

S. Delaune. *Verification of security protocols: from confidentiality to privacy*. Mémoire d'habilitation, École Normale Supérieure de Cachan, France, Mar. 2011.