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

▶ **Depuis Septembre 2016** CNRS researcher at IRISA

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

▷ **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

▷ **Jan.-Sept.:** at LORIA in Nancy in the team of Michaël Rusinowitch;

▷ **Sept.-Dec.:** at Birmingham University in the team of Mark Ryan.

▶ **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.

▷ **Award "thèse remarquable" from France Télécom R&D.**

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

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

▷ Master and Licence in computer sicence with *high distinction*.

Research

Context. The rise of the Internet and the ubiquity of electronic devices have changed our daily life. For instance, nowadays, it is possible to wave a building access card, a government-issued ID, or even a smartphone in front of a reader to go through a gate, or to pay for some purchase. Unfortunately, this digitalization of the world comes with tremendous risks for our security and privacy. To secure the applications mentioned above and to protect our privacy, some specific *cryptographic protocols* are deployed. These protocols are small distributed programs that make use of cryptographic primitives, such as encryption or digital signature, and they aim at keeping our transactions and personal data secure. As an illustrative purpose, two applications are described below.

- *Electronic passport.* Passports are no longer pure paper documents. Instead, they contain a chip that stores additional information such as pictures and fingerprints of its holder. In order to ensure privacy and confidentiality of our personal data, these chips include a mechanism that does not let the passport disclose private information to external users. However, it has been shown that it is nonetheless possible to recognize a previously observed passport, potentially tracing passport holders. This is just a single example but of course privacy appears in many other contexts such as RFIDs technologies or electronic voting.
- *E-commerce.* According to the FEVAD (the French federation of e-commerce), 51.1 billions € have been spent through e-commerce in 2013 (in France). This represents more than 600 millions of transactions. The fraud is estimated to 2 billion € for 2013 alone with an increasing number of identity thefts according to an article

published in June 2014 in *Journal du Net*. To stop the explosion of this costly fraud, new cryptographic protocols (*e.g.* Verified-by-Visa or SecureCode protocols) have been designed and deployed. They aim at improving the authentication process.

In view of the numerous attacks, with more or less dramatic consequences, the security of computer and communications is currently an important challenge. How can we get more confidence in the security of the primitives/the protocols that we are using every day?

Compared to the general safety/liveness properties, security is a specific challenge since it requires to consider any possible adversary interacting with the program. Furthermore, this adversary is malicious; for instance statistical testing of a program is irrelevant since the attacker is likely to exploit any single flaw in a program. That is why security protocols are notoriously difficult to design and analyse. Therefore formal methods play an important role. In the last decades, many works have been devoted to the use of formal methods in order to automate the proof or the existence of logical attacks on such protocols. I am contributing to this line of research.

The thrust of my research (and more generally of the SECSI group in which I am working) is towards *more realism, more security properties, and more automation*. I contributed to these three lines by developing some techniques to analyse up-to-date protocols integrated in their environment. From the point of view of the applications, I am especially interested in electronic voting, RFID protocols such as those embedded in the e-passport application, mobile ad-hoc networks, and hardware security modules such as those present in cash machines.

Publications: 18 papers in international journals and 47 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://www.lsv.ens-cachan.fr/~delaune/publis.php`.

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

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

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

International Journals

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

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.

Teaching, and invited talks

Lectures

- Course « *Regards Croisés* » (level L3), ENS Cachan, (3h, 2008-2014);
- Master course at MPRI « *Cryptographic protocols: formal and computational proof* », (9h, 2008) & (15h, 2010) & (12h, 2011) & (24h, 2014).

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

`http://www.lsv.ens-cachan.fr/~delaune/expose.php`

Some talks

- Invited talk at the TRENDS workshop, Roma, Italy, « A process algebraic analysis of privacy-type properties in cryptographic protocols », Sept. 2014;
- Invited talk at the MOVEP summer school, Nantes « Verification of Security Protocols: from Confidentiality to Privacy », July 2014;
- CAPPRIS meeting, Paris, « APTE: an automatic tool for verifying privacy-type security properties », Mar. 2014;
- CAPPRIS meeting, Paris, « Analysing privacy-type properties using formal methods », Mar. 2012;
- Dagstuhl seminar, Germany, « Trace equivalence via constraint solving », August 2011;
- Seminar Verimag, Grenoble, « Formal analysis of protocols based on TPM state registers », June 2011;
- Course at the SecVote summer school « *Analysis of privacy-type properties* », Sept. 2010.

Popularization

- Intervention au Lycée Corot à Savigny-sur-Orge « Les protocoles cryptographiques: comment sécuriser nos communications ? », Mar. 2014;
- Exposé lors de la réunion plénière de l'INS2I à Paris « Les protocoles cryptographiques: sommes nous bien protégés ? », June 2014;
- Exposé lors de la conférence de rentrée, ENS Cachan « Ces protoccoles qui nous protègent », Sept. 2012;
- Séminaire lors des Journées Régionales de l'APMEP, Rouen « Ces protocoles qui nous protègent », April 2012
- Atelier lors des Journées Nationales de l'APMEP, Grenoble « Les protocoles cryptographiques: comment sécuriser nos communications ? », Oct. 2011;
- Exposé Unithé ou Café?, Parc Orsay Université « Big Brother won't watch us », Nov. 2011;
- Interview sur le vote électronique dans le magazine « La Recherche », Sept. 2010.

Supervision of students

Master students

- Antoine Dallon, *Reducing the nomber of agents for equivalence-based properties*, 2015 (with co-advisor Véronique Cortier);
- Ludovic Robin, « *Verification of cryptographic protocols using low-entropy secrets* », 2014 (with co-advisor Steve Kremer);
- Lucca Hirschi, « *Réduction d'entrelacements pour l'équivalence de traces* », 2013 (with co-advisor David Baelde);
- Apoorvaa Deshpande, « *Automated verification of equivalence properties* », 2012 (with co-advisor Steve Kremer);
- Rémy Chrétien, « *Trace equivalence of protocols for an unbounded number of sessions* », 2012 (with co-advisor Véronique Cortier);
- Jan Degrieck, « *Graphs reduction for analysing secure routing protocols* », 2011 (with co-advisor Véronique Cortier);
- Daniel Pasaila, « *Algorithms for deciding symbolic equivalence* », 2011 (with co-advisor Steve Kremer);
- Vincent Cheval, « *Decision algorithms for symbolic equivalence of contraint systems* », 2009 (with co-advisor Hubert Comon-Lundh);
- Ştefan Ciobaca, « *Automatic Verification on anonymity properties in e-voting protocols* », 2007 (with co-advisor Steve Kremer);
- Jérémie Delaitre, « *Composition of security protocols* », 2007 (with co-advisor Véronique Cortier).

PhD students

- Antoine Dallon, *Deciding equivalence-based properties using SAT solvers*, 2015- (with co-advisor Véronique Cortier);
- Ludovic Robin, *Verification of cryptographic protocols that rely on out of band channels*, 2014- (with co-advisor Steve Kremer);
- Lucca Hirschi, « *Propriétés d'anonymat, passage à l'échelle*», 2013- (with co-advisor David Baelde);
- Rémy Chrétien, « *Verification of equivalence properties* », 2012-Jan. 2016 (with co-advisor Véronique Cortier);
- Vincent Cheval, « *Decision algorithms for equivalence based properties* », 2009-2012 (with co-advisor Hubert Comon-Lundh);

- Mathilde Arnaud, « *Verification of secure routing protocols* », 2008-2011 (with co-advisor Véronique Cortier);
- Sergiu Bursuc, « *Verification of security protocols and equational theories* », 2007-2009 (with co-advisor Hubert Comon-Lundh).

PhD Defense committee

- Miriam Paiola (reviewer): « *Verification of cryptographic protocols with lists of unbounded lengths* », May 2014;
- Mario Alvim (jury member): « *Formal approaches to information hiding* », Oct. 2011;
- Myrto Arapinis (jury member): « *Sécurité des protocoles cryptographiques : décidabilité et résultats de réduction* », Nov. 2008.

Participation to projects, and committees

Participation to projects

- PI of the ERC Starting Grant POPSTAR, *Reasoning about Physical properties Of Security Protocols with an Application To contactless Systems*, (2017-2021);
- Head of the ANR JCJC project VIP « *Verification of Indistinguishability properties* », 2011- June 2016;
- Member of the ANR project ProSe, « *Protocoles de sécurité: modèle formel, modèle calculatoire, et implémentations* », 2010-2014;
- Member of the ANR project AVOTÉ, « *Analyse formelle de protocoles de vote électronique* », 2008-2011;
- Member of the ARA SSIA FormaCrypt, 2006-2009;
- Member of the French-Tunisian project DGRST/INRIA on electronic voting, 2007;
- Member of the project RNTL Posé, 2007;
- Co-head of the project EPSRC EP/E029833, « *Verifying properties in electronic voting protocols* » (Sept. 2006 - Dec. 2006);
- Member of ACI Rossignol, « *Semantic of cryptographic protocols verification: theory and applications* », 2003-2006;
- Member of the project RNTL PROUVÉ, « *PRotocoles cryptographiques: OUtils de VÉrification automatique* », 2003-2006.

Program committees for International Conferences

- 12th International Computer Science Symposium in Russia (CSR), Kazan, Russia, 8-12 June 2017;
- 6th Conference on Principles of Security and Trust (POST), Uppsala, Sweden, 23-29 April 2017;
- 8th International Joint Conference on Automated Reasoning (IJCAR), Portugal, June 27-30, 2016;
- 35th Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS), Bangalore, India, December 16-18, 2015;
- 25th International Conference on Rewriting Techniques and Applications (RTA), Warsaw, Poland, 29 June - 1st July 2015;
- FORTE 2015, Grenoble, France, June 2-5 2015;
- 25th jubilee edition of the International Conference on Automated Deduction (CADE), Berlin, Germany, 2015;
- 26th International Conference on Rewriting Techniques and Applications (RTA), Warsaw, Poland, 2015;
- 41st International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM), Pec pod Snezkou, Czech Republic, 2015;
- 3rd Conference on Principles of Security and Trust (POST), Grenoble, France, 2014;
- 7th International Joint Conference on Automated Reasoning (IJCAR), Vienna, Austria, 2014;
- 9th International Symposium on Trustworthy Global Computing (TGC), Roma, Italy, 2014;
- 25th International Conference on Concurrency Theory (CONCUR), Roma, Italy, 2014;
- 24th International Conference on Automated Deduction (CADE), Lake Placid, New York, USA, 2013;
- 26th IEEE Computer Security Foundations Symposium (CSF), Tulane University, New Orleans LA, USA, 2013;
- 24th International Conference on Rewriting Techniques and Applications (RTA), Eindhoven, The Netherlands, 2013;
- 8th International Conference on Information Security Practice and Experience (ISPEC), Hangzhou, China, 2012;

- 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS), Bombay, India, 2011;
- 18th ACM Conference on Computer and Communications Security (CCS), Chicago, USA, 2011;
- 24th IEEE Computer Security Foundations Symposium (CSF), Domaine de l'Abbaye des Vaux de Cernay, France, 2011;
- 23rd International Conference on Automated Deduction (CADE), Wroclaw, Poland, 2011;

Conference organization

- Member of the organization committee of the 24th IEEE Computer Security Foundations Symposium (CSF'11) (90 attendees) , June 2011;
- Member of the organization committee of the 37th Spring School on theoretical computer science and French-Japanese collaboration workshop, CoSyProofs'10 (60 attendees);
- Member of the organization committee of the Workshop in honour of Hubert Comon-Lundh (150 attendees);
- Member of the organization committee of the Workshop « *10 Years of Verification in Cachan* » (150 attendees);
- Member of the organization committee of the Workshop VETO'07 (Tunis).

Administrative tasks

- Member of the « conseil de l'école doctorale EDSP » since 2012;
- Déléguée aux thèses in computer science at EDSP since 2012;
- Member of the scientific committee at Inria Saclay since 2012;
- Hiring committees: Chaire X/CNRS (2011), University of Lille I (2009);
- Organizer of the SECSI internal seminar from (2008-2010);
- Organizer of the 3-day annual internal seminar of the lab from 2008 to 2012 (around 50 attendees);
- Member of the management committees of the laboratory.