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)** in the EMSEC/SPICY team.

⟶ **Head of the SPICY team** (Security & PrIvaCY) since its official creation in May 2021. This team results from the restructuring of the EMSEC team which gave birth to two new teams SPICY and Capsule.

⟶ Member of the executive board of the **EUR CyberSchool** since September 2020.

⟶ Head of the **Cybersecurity axis** of IRISA since 2019.

⟶ PI of the **ERC project POPSTAR** (2017-2022).

▶ **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.

Awards

- **Best paper award at ToSC 2020** with P. Derbez and M. Vavrille.
- **Best paper award at ESORICS 2020** with V. Cortier and J. Dreier.
- **Distinguished paper at CSF 2020** with D. Baelde and S. Moreau.
- **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 research area is the formal analysis and design of **security protocols**. I use techniques from automated reasoning, rewriting, model-checking and concurrency theory to model and analyze **cryptographic protocols**. After my PhD, I led an effort to formally define and analyze the security properties in electronic electronic voting protocols, and in particular those related to **privacy**, such as vote confidentiality and different types of coercion resistance. These techniques have also been applied to analyze several protocols deployed in **contactless systems** such as electronic passports and cell phones. All of this research has been carried out in the so-called symbolic model. More recently, I have been working on the development of a new a new approach allowing to obtain security guarantees in the so-called computational model (the model used by cryptographers).

Finally, since September 2016, I am also interested in the use of formal methods (CP solvers, SAT solvers) to carry out work in the field of **cryptanalysis**, i.e. the study of the robustness of cryptographic primitives used as building blocks in the design of of security protocols.

Publications

26 international journals, **62** international conferences, 4 book chapters, and 7 popularization articles. The full list of my publications is available on my web page together with the list of my scientific talks.

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

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:

- Tristan Claverie (nov. 2021-) with co-advisor G. Avoine. CIFRE grant with ANSSI.
- Arthur Gontier (sept. 2020-) with co-advisor P. Derbez and C. Prud'homme.
- Joshua Peignier (sept. 2019-sept 2020) with co-advisor V. Cortier. Discontinuated.
- Solène Moreau (sept. 2018- nov. 2021) with co-advisor D. Baelde.
- Alexandre Debant (sept. 2017-nov. 2020), now post-doc at LORIA.
- Tristan Ninet (sept. 2018- mars 2020), with co-advisor O. Zendra. CIFRE grant with Thalès. I took the direction in the course (after 2 years of thesis) following the departure of the officiel PhD thesis advisor. Now, engineer at Thalès.
- 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, now engineer in the start-up Cyber-Detect.
- 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 Inria Paris (Prosecco team).
- 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 the University of Luxembourg.

Postdocs/Engineers:

- Clément Hérouard (sept. 2021-), engineer on the ERC POPSTAR.
- Nguyen Le Thanh Dung (sept. 2021-), engineer on the ERC POPSTAR.
- Vaishnavi Sundararajan (nov. 2018-nov. 2019), now post-doc at University of California, Santa Cruz.
- 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 & 2020), and MRI Rennes (10h, 2017 & 2018 & 2019 & 2020).
- 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:

I have a regular activity in scientific mediation: seminars for students, meetings with politicians, articles in the written press (e.g. blog binaire, interstices, CNRS journal, magazines *Pour La Science*, *La Recherche*), interview in the oral press (e.g. podcast for interstices, television interview, radio intervention). I list below some of my contributions with the aim of being exhaustive on those done since 2016:

- Article in the **journal of the CNRS**, *Between transparency and confidentiality, the challenges of electronic voting*, with Véronique Cortier, April 2021;
- Conference for the students of the ENS Lyon, online event, October 2020;
- Blog Binaire, **Le Monde**, *How to ensure that a cryptographic cryptographic protocol has no flaws? Une histoire de logique !*, with Steve Kremer, February 2020;

- Meeting with Nathalie Loiseau (Minister of European Affairs) and Jean-Yves Le Drian (Minister of Foreign Affairs), during a visit on the Rennes site, May 2019;
- Meeting with Frédérique Vidal (Minister of Higher Education Education, Research and Innovation), during her visit on the Rennes site, January 2019;
- Welcoming a group of 12 students (stagiaires de 3ème) to explain my research and the job of a researcher (2018 & 2019).
- SigLog Newsletter, ACM Special Interest Group on Logic and Computation, *POPSTAR – So near and yet so far*, 2018;
- TV interview for TVR (broadcast on 11/13/2017), November 2017;
- Article in Sciences Ouest, In the network of Europe, May 2017;
- Article in the CNRS Journal, December 2016 is not enough, December 2016;
- Presentation at the *Colloque Sécurité informatique: mythes et réalité* organized in Paris at the CNRS headquarters, December 2016;
- Conference at the ENS Rennes for students of 1st year, September 2016;
- Podcast **Interstices**, *How to secure our communicating communicating?* , September 2016;
- **France Inter**, Émission *chercheurs d'avenir* with Gérard Berry and Jérôme Nika, July 2016;
- Guest lecture at the final of the Alkindi competition (for high school students), *The cryptographic protocols cryptographic protocols: encryption is good but not enough!, Hotel des Invalides, Paris, May 2016.*
- *Seminary at the Collège de France*, *Formal verification applied to applied to cryptographic protocols*, Paris, April 2016.
- Article on the site **Interstices**, *Le bitcoin, une monnaie 100% numérique*, with Rémy Chrétien, September 2014;
- Pour La Science, 433:70-77, Belin, *La protection des informations sensibles*, with Rémy Chrétien, November 2013;
- **La Recherche Magazine**, *Le vote électronique*, September 2010.
- Public debate at the University of Paris 7 on voting machines as part of the Fête de la Science, October 2007.

Participation to committees

Editorships
- ACM Transactions on Privacy and Security (TOPS), editorial board since 2020.
- Information Processing Letters (IPL), editorial board (2019-2021).
- 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 (2017-2021)
- Formal methods for security – working group GDR Sécurité Informatique, **co-head** (2017-2021).
- IFIP Wg-1.7 Foundations of Security Analysis, member since 2016.

Program committees: 11 international workshops and **37 international conferences** that are listed below:
- *2022:* CSF
- *2021:* ACNS, LICS, CCS
- *2020:* DATE, ESORICS
- *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 the annual meeting for the GT-MFS working group of the GdR Sécurité Informatique from 2017 to 2021 (about 100 participants).
- **Cyber in Saclay School** (100 participants). I co-organized with S. Bardin the thematic school for young researchers, February 2021. The school gathered about a hundred participants among which about forty participated to online practical sessions.
- 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:

- Adelaine Roux-Langlois as president, June 2021.
- 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 the hiring committee CR Inria Sophia-Antipolis in 2020.
- Member of several hiring committees (professor position): IMT Atlantique (2020 & 2021), ENS Ulm (2018), Polytechnique (2018).
- Member of several hiring committees (assistant professor position): Marseille (2020), IMT Atlantique (2021), Paris Denis Diderot (2018 & 2020), 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:

- Committee member for the FWO in Belgium in 2020 & 2021.
  $\longrightarrow$ *1-day meeting to evaluate and rank about 30 proposals.*
- Committee member for the ANR generic call in 2015 & 2016.
  $\longrightarrow$ *2-day meeting to evaluate and rank about 60 proposals.*
- Reviewer for several national projects: French ANR (2012 & 2014), Luxembourguish FNR (2015), Austria (2019), Germany (2019).
- Reviewer for the ERC in 2020 & 2021.

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 executive boad GdR Sécurité Informatique (2016-2021).
- Co-Head of the working group GT-MFS "Méthodes Formelles pour la Sécurité" from GdR Sécurité Informatique (2017-2021).
- Member of the laboratory council at IRISA (2017-2021).
- 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).