

Stéphanie Delaune

☎ (+33) 1 47 40 75 63

FAX (+33) 1 47 40 75 21

✉ delaine@lsv.ens-cachan.fr

🌐 <http://www.lsv.ens-cachan.fr/~delaine/>



LSV – ENS Cachan
61, avenue du Président Wilson
94235 Cachan

Née le 26 septembre 1980
Nationalité française

Curriculum Vitae

- ▶ **2007-** Chargée de Recherche CNRS au LSV (*Laboratoire Spécification et Vérification*), UMR 8643, ENS Cachan & CNRS & INRIA Saclay Île-de-France.
 - ▷ **Mars 2011 : Thèse d'habilitation** sur le sujet
« *Verification of security protocols : from confidentiality to privacy* »
- ▶ **2006-2007** Post-doctorante
 - ▷ **Jan.-Sept.** : au LORIA à Nancy dans l'équipe de Michaël RUSINOWITCH ;
 - ▷ **Sept.-Déc.** : à l'université de Birmingham, dans l'équipe de Mark RYAN.
- ▶ **2003-2006** Doctorante, allocataire bourse CIFRE, aux :
 - Laboratoire Spécification et Vérification (LSV), ENS Cachan & CNRS,
 - Laboratoire Middleware et Plates-Formes Avancées (MAPS), France Télécom R&D.« *Vérification des protocoles cryptographiques et propriétés algébriques* »
Co-encadré par Hubert COMON-LUNDH et Francis KLAY.
Mention « thèse remarquable » attribuée par France Télécom R&D.
- ▶ **1998-2003** Étudiante à l'université Denis Diderot (Paris VII).
 - ▷ **2003** : Master en informatique, mention *très bien*.
 - ▷ **2001** : Licence en informatique, mention *très bien*.

Activités de recherche

Thématiques de recherche : Vérification de protocoles cryptographiques (approche symbolique)

- applications : vote électronique, protocoles RFID, APIs de sécurité, ...
- propriété de sécurité : confidentialité, authentification, respect de la vie privée, ...

Publications : environ 10 articles dans des revues internationales et 30 articles de conférences internationales. La liste détaillée de mes publications est disponible en annexe.

Enseignement

Écoles jeunes chercheurs

- « *Analysis of privacy-type properties* » cours à l'école d'été SecVote, Septembre 2010.

Cours

- Cours « *Regards Croisés* » (L3), ENS Cachan, (3h, 2008) & (4h, 2010) ;
- Cours M2-30-1 du MPRI « *Protocoles cryptographiques : preuves formelles et calculatoires* », (9h, 2008) & (15h, 2010).

Travaux dirigés & Travaux pratiques

- ▷ **2004-2006** : Monitrice à l'université Denis Diderot (Paris VII) : Automates finis (L1, 32 h) ; programmation en JAVA (L1 & L2, 70 h) ; encadrement d'un projet de programmation en JAVA (L1, 26 h).
- ▷ **2004-2005** : Enseignement à l'ENS Cachan : programmation en Ocaml (L3, 10 h).

- ▷ **2002-2003** : Tutrice à l'université Denis Diderot (Paris VII) : aide au travail personnel des étudiants, programmation en langage C (L1, 50 h).

Encadrement d'étudiants

Étudiants en Master

- Jan DEGRIECK, « *Réduction de graphes pour l'analyse de protocoles de routage sécurisés* », 2011 (co-encadré avec Véronique Cortier) ;
- Daniel PASAILA, « *Algorithmes pour décider l'équivalence symbolique* », 2011 (co-encadré avec Steve Kremer) ;
- Vincent CHEVAL, « *Algorithme de décision pour l'équivalence symbolique de systèmes de contraintes* », 2009 (co-encadré avec Hubert Comon-Lundh) ;
- Ștefan CIOBĂCĂ, « *Vérification automatique de propriétés d'anonymat dans les protocoles de vote électronique* », 2008 (co-encadré avec Steve Kremer) ;
- Jérémie DELAITRE, « *Composition de protocoles de sécurité* », 2007 (co-encadré avec Véronique Cortier).

Étudiants en thèse

- Vincent CHEVAL, « *Algorithme de décision pour les propriétés d'équivalence* », 2009- (co-encadré avec Hubert Comon-Lundh) ;
- Mathilde ARNAUD, « *Vérification de protocoles de routage sécurisés* », 2008- (co-encadré avec Véronique Cortier) ;
- Sergiu BURSUC, « *Vérification des protocoles cryptographiques et théories équationnelles* », 2007-2009 (co-encadré avec Hubert Comon-Lundh).

Autres

- Céline CHEVALIER, ATER à l'ENS Cachan (co-encadré avec Steve Kremer), 2010-2011 ;
- Morten DAHL, étudiant en thèse à l'université d'Aalborg (Danemark) sous la direction de Hans Hüttel. Visite d'une année au LSV pour travailler sur « *Vérification de protocoles dans les réseaux ad-hoc pour automobiles* », (co-encadré avec Graham Steel), 2009-2010 ;
- Myrto ARAPINIS, ATER à l'ENS Cachan (co-encadré avec Steve Kremer), 2007-2008 ;
- Mouhebeddine BERRIMA, stage de recherche de 3 mois.

Jury de thèse

- Sergiu BURSUC (co-directrice de thèse) : « *Contraintes de déductibilité dans une algèbre quotient : réduction de modèles et applications à la sécurité* », Déc. 2009 ;
- Myrto ARAPINIS (examinatrice) : « *Sécurité des protocoles cryptographiques : décidabilité et résultats de réduction* », Nov. 2008.

Exposés et séminaires

Exposés invités

- Workshop Franco-Japonais, LORIA, Nancy « *Safely composing security protocols via Tagging* », Mars 2008 ;
- Workshop à l'UCL, Louvain-La-Neuve « *Safely composing security protocols via Tagging* », Fév. 2008 ;
- Workshop VETO'07, Tunis « *Modelling and verifying privacy-type properties of electroning voting protocols* », Avril 2007.

Vulgarisation

- Interview sur le vote électronique dans le magazine « La Recherche », Sept. 2010 ;
- Exposé grand public lors de la remise des prix des « Olympiades Mathématiques » à Cachan, « *Les protocoles cryptographiques : comment sécuriser nos communications ?* », 2008 ;
- Participation à une table ronde sur les machines à voter dans le cadre de la fête de la science, Octobre 2007.

Séminaires : LMNO/ GREYC (Caen), Université de Clarkson (Postdam, New-York, USA), LIAFA (Université Paris VII), LACL (Université de Créteil), School of Computer Science (Université de Birmingham), LORIA (Université de Nancy), Université de Trier (Allemagne), Verimag (Grenoble), . . .

Conférences : SPV'03, CSFW'04, JDIR'04, RTA'05, CSFW'06, FCS-ARSPA'07, FroCoS'07, FSTTCS'07, SecCo'10, FAST'10, ...

Plusieurs exposés à différents groupes de travail : LSV, France Télécom (Département, Pôle Sécurité), LORIA, ...

Projets

- Responsable du projet ANR JCJC VIP « *Verification of Indistinguishability properties* », 2011-2015 ;
- Membre du projet ANR ProSe, « *Protocoles de sécurité : modèle formel, modèle calculatoire, et implémentations* », 2010-2014 ;
- Membre du projet ANR AVOTÉ, « *Analyse formelle de protocoles de vote électronique* », 2008-2011 ;
- Membre du projet ARA SSI FormaCrypt, 2006-2009 ;
- Membre du programme d'échange entre la France et la Tunisie initié dans le cadre du projet DGRST/INRIA, intitulé « *Conception et implémentation de systèmes de vote électronique et d'outils de vérification des protocoles de vote électronique* », 2007 ;
- Membre du projet RNTL POSÉ, 2007 ;
- Co-responsable du Projet EPSRC EP/E029833, « *Verifying properties in electronic voting protocols* » (sept. 2006 - déc. 2006) ;
- Membre de l'ACI Rossignol, « *Sémantique de la vérification des protocoles cryptographiques : théorie et applications* », 2003-2006 ;
- Membre du projet RNTL PROUVÉ, « *Protocoles cryptographiques : Outils de Vérification automatique* », 2003-2006.

Workshops et Conférences

Comités de programme

- 9th International Workshop on Security Issues in Concurrency (SecCo), Aachen, Germany, 2011 ;
- 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS'11), Bombay, India, 2011 ;
- 18th ACM Conference on Computer and Communications Security (CCS'11), Chicago, USA, 2011 ;
- 24th IEEE Computer Security Foundations Symposium (CSF'11), Domaine de l'Abbaye des Vaux de Cernay, France, 2011 ;
- 23rd International Conference on Automated Deduction (CADE'11), Wroclaw, Poland, 2011 ;
- Workshop on Foundations of Security and Privacy (FCS-PrivMod'10) ;
- Édition 2009 des workshops SecCo (Security Issues in Concurrency), FCS (Foundations of Security and Privacy), and SecRet (Security and Rewriting Techniques) ;
- Workshop Formal Methods in Security Engineering (FMSE'08) ;
- IAVoSS Workshop On Trustworthy Elections, (WOTE'07) et (WOTE'08).

Organisation de conférence

- Membre du comité d'organisation du 24^{ème} IEEE Computer Security Foundations Symposium (CSF'11) (90 participants), Juin 2011 ;
- Membre du comité d'organisation de la 37^{ème} école de printemps et du workshop Franco-Japonais, CosyProofs'10 (60 participants) ;
- Membre du comité d'organisation du Workshop en l'honneur d'Hubert Comon-Lundh (150 participants) ;
- Membre du comité d'organisation du Workshop « *10 Years of Verification in Cachan* » (150 participants) ;
- Membre du comité d'organisation du Workshop sur la Sécurité Informatique et le Vote ElecTrOnique (VETO'07).

Relecture d'articles

- Rapports de lecture pour les conférences suivantes : TACAS'05, CSFW'05, ICALP'05, CSFW'06, IJCAR'06, ICTAC'06, FOSSACS'07, LPAR'07, FCS-ARSPA'07, ICICS'07, AMAST'08, CSF'08, FOSSACS'08, FSTTCS'08, LPAR'08, RTA'08, CSF'09, FOSSACS'10, CSF'10, ...
- Rapports de lecture pour les journaux suivants : Information Processing Letters, Information and

Computation, Journal of Formal Aspects of Computing, and Software Testing, Verification and Reliability, Journal of Automated Reasoning, ...

Responsabilités administratives

- Comité de sélection : Chaire X/CNRS (2011), Université de Lille I (2009) ;
- Responsable du groupe de travail de l'axe SECSI (2008 -2010) ;
- Organisatrice du séminaire annuel du laboratoire depuis 2008 (3 jours, 50 participants) ;
- Membre du conseil de laboratoire et du comité de direction du laboratoire.

Séjours à l'étranger

- Août 2005 : Séjour d'une semaine à l'université de Clarkson à Postdam (New-York, USA), dans l'équipe de Chris Lynch.
- Septembre 2006 - Décembre 2006 : Post-doctorat de 4 mois à l'université de Birmingham (UK), dans l'équipe de Mark Ryan.
- Plusieurs séjours à l'université de Birmingham dans l'équipe de Mark Ryan : Octobre 2005 (1 semaine), Juillet 2007 (2 semaines), Septembre 2007 (2 semaines).

Autres activités

- Représentante des doctorants du LSV (2004-2005) ;
- Représentante des doctorants de l'EDSP, *École Doctorale Sciences Pratiques*, (2004-2005) ;
- Participation à l'organisation des RED, *Rencontres pour l'Emploi des Docteurs*, (2005).

Chapitres de Livre

- [CDM11] Hubert Comon-Lundh, Stéphanie Delaune, and Jonathan Millen. Constraint solving techniques and enriching the model with equational theories. In Véronique Cortier and Steve Kremer, editors, *Formal Models and Techniques for Analyzing Security Protocols*, volume 5 of *Cryptology and Information Security Series*, pages 35–61. IOS Press, 2011. To appear.
- [DKR10b] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Verifying privacy-type properties of electronic voting protocols: A taster. In David Chaum, Markus Jakobsson, Ronald L. Rivest, Peter Y. A. Ryan, Josh Benaloh, Mirosław Kutylowski, and Ben Adida, editors, *Towards Trustworthy Elections – New Directions in Electronic Voting*, volume 6000 of *Lecture Notes in Computer Science*, pages 289–309. Springer, May 2010.

Revue Internationale

- [CDK11] Ștefan Ciobâcă, Stéphanie Delaune, and Steve Kremer. Computing knowledge in security protocols under convergent equational theories. *Journal of Automated Reasoning*, 2011. To appear.
- [CD11] Véronique Cortier and Stéphanie Delaune. Decidability and combination results for two notions of knowledge in security protocols. *Journal of Automated Reasoning*, 2011. To appear.
- [DKR10a] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Symbolic bisimulation for the applied pi calculus. *Journal of Computer Security*, 18(2):317–377, March 2010.
- [DKS10] Stéphanie Delaune, Steve Kremer, and Graham Steel. Formal analysis of PKCS#11 and proprietary extensions. *Journal of Computer Security*, 18(6):1211–1245, November 2010.
- [DKR09] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4):435–487, July 2009.
- [CD09b] Véronique Cortier and Stéphanie Delaune. Safely composing security protocols. *Formal Methods in System Design*, 34(1):1–36, February 2009.
- [DLLT08] Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis for monoidal equational theories. *Information and Computation*, 206(2-4):312–351, February-April 2008.
- [Del06b] Stéphanie Delaune. An undecidability result for AGh. *Theoretical Computer Science*, 368(1-2):161–167, December 2006.
- [Del06a] Stéphanie Delaune. Easy intruder deduction problems with homomorphisms. *Information Processing Letters*, 97(6):213–218, March 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.
- [DJ06] Stéphanie Delaune and Florent Jacquemard. Decision procedures for the security of protocols with probabilistic encryption against offline dictionary attacks. *Journal of Automated Reasoning*, 36(1-2):85–124, January 2006.

Conférences Internationales

— 2011 —

- [ACD11] 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, Wrocław, Poland, July 2011. Springer. To appear.
- [DKRS11] Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel. Formal analysis of protocols based on TPM state registers. In *Proceedings of the 24th IEEE Computer Security Foundations Symposium (CSF'11)*, Cernay-la-Ville, France, June 2011. IEEE Computer Society Press. To appear.
- [DDS11] Morten Dahl, Stéphanie Delaune, and Graham Steel. Formal analysis of privacy for anonymous location based services. In *Proceedings of the Workshop on Theory of Security and Applications (TOSCA'11)*, Saarbrücken, Germany, March-April 2011. To appear.

— 2010 —

- [DKRS10] Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel. A formal analysis of authentication in the TPM. In Pierpaolo Degano, Sandro Etalle, and Joshua 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, September 2010. Springer.
- [DDS10] Morten Dahl, Stéphanie Delaune, and Graham Steel. Formal analysis of privacy for vehicular mix-zones. In Dimitris Gritzalis and Bart 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, September 2010. Springer.
- [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.
- [CCD10] Vincent Cheval, Hubert Comon-Lundh, and Stéphanie Delaune. Automating security analysis: symbolic equivalence of constraint systems. In Jürgen Giesl and Reiner 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.

— 2009 —

- [DKP09] Stéphanie Delaune, Steve Kremer, and Olivier Pereira. Simulation based security in the applied pi calculus. In Ravi Kannan and K. Narayan Kumar, editors, *Proceedings of the 29th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'09)*, volume 4 of *Leibniz International Proceedings in Informatics*, pages 169–180, Kanpur, India, December 2009. Leibniz-Zentrum für Informatik.
- [BDC09] Sergiu Bursuc, Stéphanie Delaune, and Hubert Comon-Lundh. Deducibility constraints. In Anupam Datta, editor, *Proceedings of the 13th Asian Computing Science Conference (ASIAN'09)*, volume 5913 of *Lecture Notes in Computer Science*, pages 24–38, Seoul, Korea, December 2009. Springer.
- [CDK09b] Ștefan Ciobăcă, Stéphanie Delaune, and Steve Kremer. Computing knowledge in security protocols under convergent equational theories. In Renate Schmidt, editor,

Proceedings of the 22nd International Conference on Automated Deduction (CADE'09), Lecture Notes in Artificial Intelligence, pages 355–370, Montreal, Canada, August 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, June–July 2009. Springer.
- [CDK09a] Rohit Chadha, Stéphanie Delaune, and Steve Kremer. Epistemic logic for the applied pi calculus. In David Lee, Antónia Lopes, and Arnd Poetzsch-Heffter, editors, *Proceedings of IFIP International Conference on Formal Techniques for Distributed Systems (FMOODS/FORTE'09)*, volume 5522 of *Lecture Notes in Computer Science*, pages 182–197, Lisbon, Portugal, June 2009. Springer.

— 2008 —

- [ADK08] Myrto Arapinis, Stéphanie Delaune, and Steve Kremer. From one session to many: Dynamic tags for security protocols. In Iliano Cervesato, Helmut Veith, and Andrei Voronkov, editors, *Proceedings of the 15th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'08)*, volume 5330 of *Lecture Notes in Artificial Intelligence*, pages 128–142, Doha, Qatar, November 2008. Springer.
- [DKR08] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Composition of password-based protocols. In *Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08)*, pages 239–251, Pittsburgh, PA, USA, June 2008. IEEE Computer Society Press.
- [DKS08] Stéphanie Delaune, Steve Kremer, and Graham Steel. Formal analysis of PKCS#11. In *Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08)*, pages 331–344, Pittsburgh, PA, USA, June 2008. IEEE Computer Society Press.
- [DRS08] Stéphanie Delaune, Mark D. Ryan, and Ben Smyth. Automatic verification of privacy properties in the applied pi-calculus. In Yuecel Karabulut, John Mitchell, Peter Herrmann, and Christian Damsgaard Jensen, editors, *Proceedings of the 2nd Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM'08)*, volume 263 of *IFIP Conference Proceedings*, pages 263–278, Trondheim, Norway, June 2008. Springer.

— 2007 —

- [CDD07] 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.
- [DKR07] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Symbolic bisimulation for the applied pi-calculus. 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 133–145, New Delhi, India, December 2007. Springer.
- [DLL07] Stéphanie Delaune, Hai Lin, and Christopher Lynch. Protocol verification via rigid/flexible resolution. 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 242–256, Yerevan, Armenia, October 2007. Springer.

- [CD07] 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.
- [BCD07b] Sergiu Bursuc, Hubert Comon-Lundh, and Stéphanie Delaune. Deducibility constraints, equational theory and electronic money. In Hubert Comon-Lundh, Claude Kirchner, and Hélène Kirchner, editors, *Rewriting, Computation and Proof — Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of his 60th Birthday*, volume 4600 of *Lecture Notes in Computer Science*, pages 196–212, Cachan, France, June 2007. Springer.
- [ACD07] 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.
- [CDS07] 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.
- [BCD07a] Sergiu Bursuc, Hubert Comon-Lundh, and Stéphanie Delaune. Associative-commutative deducibility constraints. In Wolfgang Thomas and Pascal Weil, editors, *Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS'07)*, volume 4393 of *Lecture Notes in Computer Science*, pages 634–645, Aachen, Germany, February 2007. Springer.

— 2006 —

- [DKR06] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06)*, pages 28–39, Venice, Italy, July 2006. IEEE Computer Society Press.
- [DLLT06] Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis in presence of a homomorphism operator and *exclusive or*. In Michele Buglesì, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06) — Part II*, volume 4052 of *Lecture Notes in Computer Science*, pages 132–143, Venice, Italy, July 2006. Springer.

— 2005 —

- [CD05] Hubert Comon-Lundh and Stéphanie Delaune. The finite variant property: How to get rid of some algebraic properties. In Jürgen Giesl, editor, *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307, Nara, Japan, April 2005. Springer.

— 2004 —

- [DJ04a] Stéphanie Delaune and Florent Jacquemard. A decision procedure for the verification of security protocols with explicit destructors. In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick McDaniel, editors, *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS'04)*, pages 278–287, Washington, D.C., USA, October 2004. ACM Press.
- [DJ04b] Stéphanie Delaune and Florent Jacquemard. A theory of dictionary attacks and its complexity. In *Proceedings of the 17th IEEE Computer Security Foundations Workshop*

(CSFW'04), pages 2–15, Asilomar, Pacific Grove, California, USA, June 2004. IEEE Computer Society Press.

Thèses

- [Del11b] Stéphanie Delaune. *Verification of security protocols: from confidentiality to privacy*. Mémoire d'habilitation, École Normale Supérieure de Cachan, France, March 2011.
- [Del06c] Stéphanie Delaune. *Vérification des protocoles cryptographiques et propriétés algébriques*. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2006.

Rapports de Contract

— AVOTÉ projet —

- [DK09] Stéphanie Delaune and Steve Kremer. Spécificités des protocoles de vote électronique. Deliverable AVOTE 1.1 (ANR-07-SESU-002), January 2009. 8 pages.
- [DK10] Stéphanie Delaune and Steve Kremer. Formalising security properties in electronic voting protocols. Deliverable AVOTE 1.2, (ANR-07-SESU-002), April 2010. 17 pages.
- [Del11a] Stéphanie Delaune. Algorithms for observational equivalence. Deliverable AVOTE 2.2, (ANR-07-SESU-002), January 2011. 118 pages.

— PROUVÉ projet —

- [BDKT04] Liana Bozga, Stéphanie Delaune, Francis Klay, and Ralf Treinen. Spécification du protocole de porte-monnaie électronique. Technical Report 1, projet RNTL PROUVÉ, June 2004. 12 pages.
- [CDL04] Véronique Cortier, Stéphanie Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. Technical Report 2, projet RNTL PROUVÉ, June 2004. 19 pages.
- [BCC⁺04] Vincent Bernat, Hubert Comon-Lundh, Véronique Cortier, Stéphanie Delaune, Florent Jacquemard, Pascal Lafourcade, Yassine Lakhnech, and Laurent Mazaré. Sufficient conditions on properties for an automated verification: theoretical report on the verification of protocols for an extended model of the intruder. Technical Report 4, projet RNTL PROUVÉ, December 2004. 33 pages.
- [BDKV05] Liana Bozga, Stéphanie Delaune, Francis Klay, and Laurent Vigneron. Retour d'expérience sur la validation du porte-monnaie électronique. Technical Report 5, projet RNTL PROUVÉ, March 2005. 29 pages.
- [DKK05] Stéphanie Delaune, Francis Klay, and Steve Kremer. Spécification du protocole de vote électronique. Technical Report 6, projet RNTL PROUVÉ, November 2005. 19 pages.
- [KBL⁺06] Francis Klay, Liana Bozga, Yassine Lakhnech, Laurent Mazaré, Stéphanie Delaune, and Steve Kremer. Retour d'expérience sur la validation du vote électronique. Technical Report 9, projet RNTL PROUVÉ, November 2006. 47 pages.
- [DK07] Stéphanie Delaune and Francis Klay. Synthèse des expérimentations. Technical Report 10, projet RNTL PROUVÉ, May 2007. 10 pages.