

# Steve Kremer | Curriculum Vitæ

Inria Nancy - Grand Est

615 rue du Jardin Botanique, 54600 Villers-lès-Nancy, France

☎ +33 (0)3 54 95 86 60 • 📠 +33 (0)3 83 27 83 19

✉ [Steve.Kremer@inria.fr](mailto:Steve.Kremer@inria.fr) • 🌐 <https://members.loria.fr/SKremer/>

born on 28/08/1976 at Luxembourg

Luxembourg citizenship

married, three children

## Positions

---

### **Inria Nancy Grand-Est and LORIA (Université de Lorraine, CNRS)**

*Inria senior research scientist (Directeur de Recherche 2<sup>e</sup> classe)* 2013 –

*Inria experienced research scientist (Chargé de Recherche 1<sup>ère</sup> classe)* 2011 – 2013

### **Inria Saclay-Île-de-France and LSV (ENS Cachan, CNRS)**

*Inria experienced research scientist (Chargé de Recherche 1<sup>ère</sup> classe)* 2006 – 2011

*Inria junior research scientist (Chargé de Recherche 2<sup>e</sup> classe)* 2004 – 2006

### **Université du Mons-Hainaut**

*Adjunkt professor (Chargé d'Enseignement)* 2003 – 2004

### **Université Libre de Bruxelles**

*Assistant Researcher* 1999 – 2004

*Student Assistant* 1998 – 1999

## Education

---

### **ENS Cachan**

*Habilitation thesis* 2011

### **Université Libre de Bruxelles**

*PhD in Computer Science* 2003

### **Université Libre de Bruxelles**

*Licence (M.Sc.) in Computer Science, La Plus Grande Distinction (summa cum laude)* 1999

### **Université Libre de Bruxelles**

*Candidature in Computer Science, Distinction (cum laude)* 1997

### **Lycée Hubert Clement Esch-sur-Alzette (Luxembourg)**

*Diplôme de fin d'études secondaires, section D (economy-mathematics), mention Bien* 1995

## Language skills

---

Luxembourgish (mother tongue), French (fluent), Dutch (fluent), German (fluent), English (fluent), Italian (good notions)

## Awards

---

- Distinguished paper award for our paper *DEEPSEC: Deciding Equivalence Properties in Security Protocols — Theory and Practice* at the 39th IEEE Symposium on Security and Privacy (S&P'18).
- ETAPS 2017 best paper nominee for our paper *On communication models when verifying equivalence properties*.
- Our paper *Automated verification of equivalence properties of cryptographic protocol* is listed in ACM Computing Reviews' 21st Annual Best of Computing list of notable books and articles for 2016.
- Recipient of an ERC Consolidator Grant in 2014.
- Winner of the “*concours bourse de voyage 2003*” by the Wallonia-Brussels Federation in Belgium (sponsoring a two month research stay at the University of Pennsylvania, Philadelphia, USA).
- *Solvay Award* in 2000 for my Master thesis *A study of several non-repudiation protocols*.

## Research stays

---

- 26/10/2008–08/11/2008: two week research stay at the AIST, Tokyo, Japan.
- 01/10/2005–31/10/2005: one-month research stay at the University of Birmingham, in the group of Dr Mark D. Ryan and Prof. Marta Kwiatkowska.
- 01/02/2004–31/07/2004: six-month research stay at the University of Birmingham, in the group of Dr Mark D. Ryan and Prof. Marta Kwiatkowska.
- 01/06/2003–31/07/2003: two-month stay at the University of Pennsylvania, in the group of Prof. Andre Scedrov.
- 08/07/2002–13/07/2002: one week stay at the *Laboratoire Spécification et Vérification* of the CNRS and the Ecole Normale Supérieure de Cachan, in order to work with Alexandre Boisseau.
- 01/01/2001–01/02/2001: international fellow at the *Stanford Research Institute*, in the group of Dr Victoria Stavridou and Dr Bruno Dutertre.

## Theses

---

- *Modelling and analyzing security protocols in cryptographic process calculi*, Habilitation thesis, ENS Cachan, March 2011.  
Jury: Martín Abadi (reviewer), Ran Canetti (reviewer), Hubert Comon-Lundh, Jean-Pierre Jouannaud, Catuscia Palamidessi (reviewer), David Pointcheval, Michael Rusinowitch, Andre Scedrov.
- *Formal Analysis of Optimistic Fair Exchange Protocols*, Ph.D. thesis, Université Libre de Bruxelles, December 2003.  
Jury: Hubert Comon-Lundh, Raymond Devillers, Jean-François Raskin (co-supervisor), Yves Roggeman (supervisor), Andre Scedrov.
- *A Study of Several Non-repudiation protocols*, Master Thesis. Université Libre de Bruxelles, June 1999, *La Plus Grande Distinction*.  
Jury: Y. Roggeman (supervisor), G. Latouche, T. Massart, O. Markowitch.  
This thesis was awarded the *Solvay award* in May 2000.

## Program Committees

---

- PLAS'17 (*ACM SIGSAC Workshop on Programming Languages and Analysis for Security*)

- ESORICS'17 (22nd European Symposium on Research in Computer Security)
- Voting'17 (2nd Workshop on Advances in Secure Electronic Voting)
- Euro SP'17 (2nd IEEE European Symposium on Security and Privacy)
- FSTTCS'16 (36th Conference on Foundations of Software Technology and Theoretical Computer Science)
- ESORICS'16 (21st European Symposium on Research in Computer Security)
- CSF'16 (29th IEEE Computer Security Foundations Symposium)
- Voting'16 (1st Workshop on Advances in Secure Electronic Voting)
- AsiaCCS'16 (11th ACM Symposium on Information, Computer and Communications Security)
- ACISP'16 (21st Australasian Conference on Information Security and Privacy)
- CryptoForma'15 (4th International CryptoForma Workshop)
- TGC'15 (10th International Symposium on Trustworthy Global Computing)
- FCS'15 (Workshop on Foundations of Computer Security)
- ESORICS'15 (20th European Symposium on Research in Computer Security)
- AsiaCCS'15 (10th ACM Symposium on Information, Computer and Communications Security)
- ICFEM'14 (16th International Conference on Formal Engineering Methods)
- ACNS'14 (12th International Conference on Applied Cryptography and Network Security)
- SEC@SAC'14 (3th edition of the Computer Security track at the 29th ACM Symposium on Applied Computing): **co-chair** with Giampaolo Bella and Manuel Barbosa
- POST'14 (3rd Conference on Principles of Security and Trust): **co-chair** with Martín Abadi
- ESORICS'13 (18th European Symposium on Research in Computer Security)
- RV'13 (4th International Conference on Runtime Verification)
- ISPEC'13 (9th International Conference on Information Security Practice and Experience)
- PoST'13 (2nd Conference on Principles of Security and Trust)
- TGC'12 (7th International Symposium on Trustworthy Global Computing)
- FSTTCS'12 (32nd Conference on Foundations of Software Technology and Theoretical Computer Science)
- CSF'12 (25th IEEE Computer Security Foundations Symposium)
- ACNS'12 (10th International Conference on Applied Cryptography and Network Security)
- ISPEC'12 (8th International Conference on Information Security Practice and Experience)
- PoST'12 (1st Conference on Principles of Security and Trust)
- FAST'11 (8th International Workshop on Formal Aspects of Security and Trust)
- PST'11 (9th Annual Conference on Privacy, Security and Trust)
- SecReT'10 (5th International Workshop on Security and Rewriting Techniques): **co-chair** with Paliath Narendran
- MoVeP'10 (Modelling and Verifying Parallel Processes)
- WISSEC'09 (4th Benelux Workshop on Information and System Security)
- SecCo'09 (7th International Workshop on Security Issues in Concurrency): **co-chair** with Michele Boreale
- ASIAN'09 (13th Annual Asian Computing Science Conference)
- VOTE-ID'09 (Second international conference on E-voting and Identity)
- SecCo'08 (6th International Workshop on Security Issues in Concurrency): **co-chair** with Prakash Panangaden
- FMSE'08 (6th ACM Workshop on Formal Methods in Security Engineering)
- ICICS'08 (10th International Conference on Information and Communications Security)
- WOTE'08 (IAVoSS Workshop On Trustworthy Elections)

- ISC'08 (*11th Information Security Conference*)
- ISPEC'08 (*4th Information Security Practice and Experience Conference*)
- WOTE'07 (*IAVoSS Workshop On Trustworthy Elections*)
- IMIS'07 (*Interactive Multimedia & Intelligent Services in Mobile and Ubiquitous Computing*)
- ISC'07 (*10th Information Security Conference*)
- FCC'06 (*2nd workshop on Formal and Computational Cryptography*): **co-chair** with Véronique Cortier
- WOTE'06 (*IAVoSS Workshop On Trustworthy Elections*)
- ICS'06 (*Workshop on Information and Computer Security*)
- SecUbiq'06 (*2nd international workshop on Security in Ubiquitous Computing Systems*)
- IWAP'05 (*4th International Workshop for Applied PKI*)

## Steering Committees

---

- European Joint Conferences on Theory and Practice of Software (ETAPS) (2012-2014)
- Conference on Principles of Security and Trust (POST) (2011-2015)
- IEEE Computer Security Foundations Symposium (CSF) (since 2010)

## Organizing Committees

---

- co-organizer of the INRIA Alumni Jam session, Nancy, 2012
- **general chair** of the 24th IEEE Computer Security Foundations Symposium (CSF 2011)
- co-organizer of the Dagstuhl seminar *Formal Protocol Verification Applied*, October 2007
- member of the organizing committee of the 4th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'06)
- co-organizer of the ARTIST2 security workshop, (Pisa, 2006 and Trento, 2007)
- member of the organizing committee of *Perspectives in Verification* (workshop in honour of Prof. Dr. Wolfgang Thomas), Cachan, 2005
- co-organizer of the *Workshop on the link between formal and computational models*, Paris, 2005

## Invited talks and tutorials

---

- Keynote talk at 29th the IEEE Computer Security Foundations Symposium (CSF'16), Lisboa, Portugal, June 2016.
- 14th International School on Foundations of Security Analysis and Design (FOSAD'14), Bertinoro, Italy, Sep. 2014.
- 3rd International CryptoForma workshop at ESORICS, Royal Holloway, UK, Sep. 2013.
- École Jeunes Chercheurs en Programmation (EJCP'13), Rennes, France, Mai 2013.
- Colloquium in honour of Raymond DEVILLERS' 65th birthday, Brussels, Belgium, Oct. 2010.
- Computational and Symbolic Proofs of Security (CosyProofs) 2010, 37th Spring School on theoretical computer science and French-Japanese collaboration workshop, Barbizon, France.
- SecVote'10, Summer school on secure electronic voting, Bertinoro, Italy.
- Workshop at UCL, Louvain-La-Neuve, Feb. 2008.
- TFIT'08, Fourth Taiwanese-French Conference on Information Technology, Taipei, Taiwan.
- SecCo'07, 5th International Workshop on Security Issues in Concurrency, invited panelist at the panel discussion "Information hiding: state-of-the-art and emerging trends".
- Workshop on the Interplay of Programming Languages and Cryptography 2007, Sophia Antipolis, France.

- MOVEP'06, Summer school on MODelling and VERifying parallel Processes, Bordeaux, France.

## PhD committees

---

- External examiner for R. Stanley (Bristol University, UK), 2017.
- Examiner for R. David (Université de Lorraine, France), 2017
- Examiner for M. Duclos (Université de Grenoble, France), 2016.
- External examiner for A. Bruni (DTU, Denmark), 2015.
- External reviewer for E. Cuvelier (Université de Louvain-la-Neuve, Belgium), 2015
- Jury member for A. Kassem (Université Joseph Fourier, Grenoble, France), 2015
- Jury member for M. Melissen (University of Luxembourg, Luxembourg), 2013
- Reviewer for J. Dreier (Université Joseph Fourier, Grenoble, France), 2013.
- External reviewer for S. Meier (ETH Zurich, Switzerland), 2013.
- Reviewer for M. Daubignard (Université Joseph Fourier, Grenoble, France), 2012.
- Reviewer for A. Baskar (CMI, India), 2011.
- Jury member (*examineur*) for C. Braun (École Polytechnique, France), 2010.
- External reviewer for D. Kaehler (Christian-Albrechts-Universität zu Kiel, Germany), 2008.

## Supervision

---

- PhD students:
  - Charlie Jacomme (2017 –). Co-supervised with Hubert Comon.
  - Itsaka Rakotonirina (2017 – ). Co-supervised with Vincent Cheval.
  - Ludovic Robin (2014 – 2018). Co-supervised with Stéphanie Delaune.
  - Robert Künnemann (2010 – 2014). Co-supervised with Graham Steel.
  - Ștefan Ciobâcă (2008 – 2011). Co-supervised with Véronique Cortier.
  - Antoine Mercier (2006 – 2009). Co-supervised with Ralf Treinen.
- Post-docs: Laurent Mazaré (10/2006–03/2007), Graham Steel (10/2007–08/2008), Joe-Kai Tsay (since 10/2009), Céline Chevalier (10/2010 – 08/2011), Peter Rønne (since 04/2015 – 03/2016), Ivan Gazeau (09/2016–), Sergiu Bursuc (02/2017–)
- Master students: Itsaka Rakotonirina, (2016, co-supervised with Vincent Cheval) Ludovic Robin (2014, co-supervised with Stéphanie Delaune), Apoorva Desphande (2012, co-supervised with Stéphanie Delaune), Daniel Pasaila (2011, co-supervised with Stéphanie Delaune), Ștefan Ciobâcă (2008, co-supervised with Stéphanie Delaune), Nicolas Tanghe (2003), Jamal Saghir (2003), Sébastien Vandamme (2002, co-supervised with Olivier Markowitch).

## Projects

---

I am/was involved in the following projects

- ERC grant SPOOC (PI)
- ANR Sequoia (PI)
- ERC ProSecure (associate member, funded by the European Research Council)
- ANR VERSO ProSe (local PI, funded by the French national research agency ANR)
- JST-CNRS project *Cryptography and logic: Computer-checked security proofs* (French PI, French-Japanese project)
- ARA SESUR AVOTÉ (local PI, funded by the French national research agency ANR),
- ARA SSIA FormaCrypt (funded by the French national research agency ANR),
- ARTIST2 European network of excellence

- RNTL PROUVÉ (funded by the French ministry of Research)
- ACI Rossignol (funded by the French ministry of Research)

## Teaching

---

- 2013– *Theory of Computer Security* in the Master of Université de Lorraine.
- 2009–2011 Part of *Cryptographic protocols: formal and computational proofs* in the “Master Parisien de Recherche en Informatique” .
- 2007–2008 Part of *Cryptographic protocols: formal and computational proofs* in the “Master Parisien de Recherche en Informatique” .
- 2006–2007 Course on *Cryptographic Protocols* (part of the course “ Vérification de systèmes dynamiques et paramétrés”) in the “Master Parisien de Recherche en Informatique”.
- 2005–2010 Course on *Verification of Cryptographic Protocols* (part of the course “Méthodes de vérification de sécurité”) in the “Master Sécurité des Systèmes Informatiques” at Paris 12.
- 2005–2006 Exercise sessions of *Complexity* in the “Magistère” at ENS Cachan.
- 2003–2004 *Bases de Données* (Data Bases) (introduction, entity-relation model, relational model, formal query languages, SQL, integrity and security, normalization theory, specialized data structures).
- 1999–2004 Exercise sessions of *Algorithmique Générale 1* (General Algorithmics part 1) (search and sorting algorithms, recursion, basic data structures such as trees and heaps, backtracking algorithms).
- 1999–2004 Exercise sessions of *Algorithmique Générale 2* (General Algorithmics part 2) (de-recursification techniques, abstract data types, graph algorithms).
- 1999–2004 Exercise sessions of *Réseaux* (Computer Networks) (introduction to networks, network layers, TCP/IP and OSI models).
- 2001–2002 Exercise sessions of *Modèles stochastiques des systèmes informatiques* (stochastic models in computer science) (probability theory, markov chains and markovian processes applied to the modeling of computer systems).
- 2001–2002 Exercise sessions of *Modélisation informatique* (Modeling in Computer Science). (introduction to programming in C and basic algorithms, generation of stochastic variables, introduction to simulations).
- 1999–2001 Exercise sessions of *Informatique et Mathématiques de la gestion* (Computer science and mathematics applied to management) (introduction to programming in Pascal and basic algorithms, introduction to simulations).

## Responsibilities

---

- 2018 member of the hiring committee for a professor position at Université de Lorraine.
- 2014 – member of the INRIA evaluation committee (this involves 2-3 Inria hiring committees each year).
- 2014 member of the hiring committees (*Jury CR*) of INRIA Rennes and INRIA Grenoble
- 2010 member of the hiring committee (*Jury CR*) of INRIA Saclay—Île-de-France
- 2008 - 2011 member of the *Commission Scientifique* of INRIA Saclay—Île-de-France
- 2007 - 2011 vice-head (*responsable permanent*) of the INRIA SECSI team
- 2009 member of the hiring committee (“comité de sélection”) for a Verimag/CEA chair of Ensimag, Grenoble
- 2007–2008 member of the hiring committee (“commission de spécialistes”) in computer science of ENS Cachan
- 2004–2008 organizer of LSV’s weekly seminar
- 2000–2004 member of the *Conseil du Département* of the computer science department, Brussels Free University

## Publications

---

### Book chapters

- [1] 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.

### Edited books

- [2] Martín Abadi and Steve Kremer, editors. *Proceedings of 3rd International Conference on Principles of Security and Trust (POST'14)*, volume 8414 of *Lecture Notes in Computer Science*. Springer.
- [3] Véronique Cortier and Steve Kremer, editors. *Formal Models and Techniques for Analyzing Security Protocols*, volume 5 of *Cryptology and Information Security Series*. IOS Press, 2011.
- [4] Michele Boreale and Steve Kremer, editors. *Proceedings of the 7th International Workshop on Security Issues in Concurrency (SecCo'09)*, volume 7 of *Electronic Proceedings in Theoretical Computer Science*.
- [5] Steve Kremer and Prakash Panangaden, editors. *Proceedings of the 6th International Workshop on Security Issues in Concurrency (SecCo'08)*, volume 242(3) of *Electronic Notes in Theoretical Computer Science*. Elsevier Science Publishers, August 2009.
- [6] Liqun Chen, Steve Kremer, and Mark D. Ryan, editors. *Formal Protocol Verification Applied*, volume 07421 of *Dagstuhl Seminar Proceedings*.
- [7] Véronique Cortier and Steve Kremer, editors. *Proceedings of the 2nd Workshop on Formal and Computational Cryptography (FCC'06)*.

### Journals

- [8] Steve Kremer and Robert Künnemann. [Automated analysis of security protocols with global state](#). *Journal of Computer Security*, 24(5):583–616, 2016.
- [9] Rohit Chadha, Vincent Cheval, Ștefan Ciobâcă, and Steve Kremer. [Automated verification of equivalence properties of cryptographic protocol](#). *ACM Transactions on Computational Logic*, 17(4), November 2016. **Listed in ACM Computing Reviews' 21st Annual Best of Computing list of notable books and articles for 2016.**
- [10] Myrto Arapinis, Stéphanie Delaune, and Steve Kremer. [Dynamic tags for security protocols](#). *Logical Methods in Computer Science*, 10(2), 2014.
- [11] Véronique Cortier and Steve Kremer. [Formal models and techniques for analyzing security protocols: A tutorial](#). *Foundations and Trends in Programming Languages*, 1(3):151–267, 2014.
- [12] Céline Chevalier, Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. [Composition of password-based protocols](#). *Formal Methods in System Design*, 43(3):369–413, 2013.

- [13] Ștefan Ciobâcă, Stéphanie Delaune, and Steve Kremer. [Computing knowledge in security protocols under convergent equational theories](#). *Journal of Automated Reasoning*, 48(2):219–262, 2012.
- [14] Steve Kremer, Antoine Mercier, and Ralf Treinen. [Reducing equational theories for the decision of static equivalence](#). *Journal of Automated Reasoning*, 48(2):197–217, 2012.
- [15] 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.
- [16] Steve Kremer and Laurent Mazaré. [Computationally sound analysis of protocols using bilinear pairings](#). *Journal of Computer Security*, 18(6):999–1033, November 2010.
- [17] Véronique Cortier, Steve Kremer, and Bogdan Warinschi. [A survey of symbolic methods in computational analysis of cryptographic systems](#). *Journal of Automated Reasoning*, 46(3-4):225–259, April 2010.
- [18] 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.
- [19] 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.
- [20] Mathieu Baudet, Véronique Cortier, and Steve Kremer. [Computationally sound implementations of equational theories against passive adversaries](#). *Information and Computation*, 207(4):496–520, April 2009.
- [21] Jean Cardinal, Steve Kremer, and Stefan Langerman. [Juggling with pattern matching](#). *Theory of Computing Systems*, 39(3):425–437, June 2006.
- [22] Rohit Chadha, Steve Kremer, and Andre Scedrov. [Formal analysis of multi-party contract signing](#). *Journal of Automated Reasoning*, 36(1-2):39–83, January 2006.
- [23] Steve Kremer and Jean-François Raskin. [A game-based verification of non-repudiation and fair exchange protocols](#). *Journal of Computer Security*, 11(3):399–429, 2003.
- [24] Steve Kremer and Olivier Markowitch. [Fair multi-party non-repudiation protocols](#). *International Journal on Information Security*, 1(4):223–235, July 2003.
- [25] Steve Kremer, Olivier Markowitch, and Jianying Zhou. [An intensive survey of fair non-repudiation protocols](#). *Computer Communications*, 25(17):1606–1621, November 2002.



## Conferences

- [26] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. [The deepsec prover](#). In *Proceedings of the 30th International Conference on Computer Aided Verification, Part II (CAV'18)*, Oxford, UK, July 2018. Springer.
- [27] Charlie Jacomme and Steve Kremer. [An extensive formal analysis of multi-factor authentication protocols](#). In *Proceedings of the 31st IEEE Computer Security Foundations Symposium (CSF'18)*, Oxford, UK, July 2018, pages 1–15. IEEE Computer Society Press.
- [28] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. [Deepsec: Deciding equivalence properties in security protocols - theory and practice](#). In *Proceedings of the 39th IEEE Symposium on Security and Privacy (S&P'18)*, San Francisco, CA, USA, May 2018, pages 525–542. IEEE Computer Society Press. **Distinguished paper award**.
- [29] Ivan Gazeau and Steve Kremer. [Automated analysis of equivalence properties for security protocols using else branches](#). In *Proceedings of the 22nd European Symposium on Research in Computer Security (ESORICS'17)*, Oslo, Norway, September 2017, volume 10493 of *Lecture Notes in Computer Science*, pages 1–20. Springer.
- [30] David Baelde, Stéphanie Delaune, Ivan Gazeau, and Steve 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, USA, August 2017, pages 234–248. IEEE Computer Society Press.
- [31] Stéphanie Delaune, Steve Kremer, and Ludovic Robin. [Formal verification of protocols based on short authenticated strings](#). In *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF'17)*, Santa Barbara, USA, August 2017, pages 130–143. IEEE Computer Society Press.
- [32] Kushal Babel, Vincent Cheval, and Steve Kremer. [On communication models when verifying equivalence properties](#). In *Proceedings of the 6th International Conference on Principles of Security and Trust (POST'17)*, Uppsala, Sweden, April 2017, volume 10204 of *Lecture Notes in Computer Science*, pages 141–163. Springer. **Best paper nominee**.
- [33] Michael Backes, Jannik Dreier, Steve Kremer, and Robert Künnemann. [A novel approach for reasoning about liveness in cryptographic protocols and its application to fair exchange](#). In *Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)*, Paris, France, April 2017, pages 76–91. IEEE Computer Society.
- [34] Jannik Dreier, Charles Duménil, Steve Kremer, and Ralf Sasse. [Beyond subterm-convergent equational theories in automated verification of stateful protocols](#). In *Proceedings of the 6th International Conference on Principles of Security and Trust (POST'17)*, Uppsala, Sweden, April 2017, volume 10204 of *Lecture Notes in Computer Science*, pages 117–140. Springer.
- [35] Charlie Jacomme, Steve Kremer, and Guillaume Scerri. [Symbolic models for isolated execution environments](#). In *Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)*, Paris, France, April 2017, pages 530–545. IEEE Computer Society.
- [36] Myrto Arapinis, Véronique Cortier, and Steve Kremer. [When are three voters enough for privacy properties?](#) In Ioannis Askoxylakis, Sotiris Ioannidis, Sokratis Katsikas, and Catherine

- Meadows, editors, *Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS'16)*, Heraklion, Crete, September 2016, volume 9879 of *Lecture Notes in Computer Science*, pages 241–260. Springer.
- [37] Steve Kremer and Peter Rønne. [To du or not to du: A security analysis of du-vote](#). In *Proceedings of the 1st IEEE European Symposium on Security and Privacy (EuroS&P'16)*, Saarbrücken, Germany, March 2016, pages 303–323. IEEE Computer Society.
- [38] Véronique Cortier, Fabienne Eigner, Steve Kremer, Matteo Maffei, and Cyrille Wiedling. [Type-based verification of electronic voting protocols](#). In *Proceedings of the 4th Conference on Principles of Security and Trust (POST'15)*, London, UK, April 2015, volume 9036 of *Lecture Notes in Computer Science*, pages 303–323. Springer.
- [39] Steve Kremer and Robert Künnemann. [Automated analysis of security protocols with global state](#). In *Proceedings of the 35th IEEE Symposium on Security and Privacy (S&P'14)*, San Jose, CA, USA, May 2014, pages 163–178. IEEE Computer Society Press.
- [40] Steve Kremer, Robert Künnemann, and Graham Steel. [Universally composable key-management](#). In Jason Crampton and Sushil Jajodia, editors, *Proceedings of the 18th European Symposium on Research in Computer Security (ESORICS'13)*, Egham, UK, September 2013, volume 8134 of *Lecture Notes in Computer Science*, pages 327–344. Springer.
- [41] Myrto Arapinis, Véronique Cortier, Steve Kremer, and Mark D. Ryan. [Practical Everlasting Privacy](#). In David Basin and John Mitchell, editors, *Proceedings of the 2nd Conference on Principles of Security and Trust (POST'13)*, Rome, Italy, March 2013, volume 7796 of *Lecture Notes in Computer Science*, pages 21–40. Springer.
- [42] Stéphanie Delaune, Steve Kremer, and Daniel Pasaila. [Security protocols, constraint systems, and group theories](#). In Bernhard Gramlich, Dale Miller, and Uli Sattler, editors, *Proceedings of the 6th International Joint Conference on Automated Reasoning (IJCAR'12)*, Manchester, UK, June 2012, volume 7364 of *Lecture Notes in Artificial Intelligence*, pages 164–178. Springer.
- [43] Rohit Chadha, Ștefan Ciobâcă, and Steve Kremer. Automated verification of equivalence properties of cryptographic protocols. In Helmut Seidl, editor, *Programming Languages and Systems — Proceedings of the 21th European Symposium on Programming (ESOP'12)*, Tallinn, Estonia, March 2012, volume 7211 of *Lecture Notes in Computer Science*, pages 108–127. Springer.
- [44] Céline Chevalier, Stéphanie Delaune, and Steve Kremer. [Transforming password protocols to compose](#). In Supratik Chakraborty and Amit Kumar, editors, *Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11)*, Mumbai, India, December 2011, Leibniz International Proceedings in Informatics, pages 204–216. Leibniz-Zentrum für Informatik.
- [45] 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, pages 66–82. IEEE Computer Society Press.

- [46] Steve Kremer, Graham Steel, and Bogdan Warinschi. [Security for key management interfaces](#). In *Proceedings of the 24th IEEE Computer Security Foundations Symposium (CSF'11)*, Cernay-la-Ville, France, June 2011, pages 266–280. IEEE Computer Society Press.
- [47] Ben Smyth, Mark D. Ryan, Steve Kremer, and Mounira Kourjeh. [Towards automatic analysis of election verifiability properties](#). In Alessandro Armando and Gavin Lowe, editors, *Proceedings of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'10)*, Paphos, Cyprus, March 2010, volume 6186 of *Lecture Notes in Computer Science*, pages 146–163. Springer, October 2010.
- [48] 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)*, Pisa, Italy, September 2010, volume 6561 of *Lecture Notes in Computer Science*, pages 111–125. Springer.
- [49] Steve Kremer, Mark D. Ryan, and Ben Smyth. [Election verifiability in electronic voting protocols](#). In Dimitris Gritzalis and Bart Preneel, editors, *Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10)*, Athens, Greece, September 2010, volume 6345 of *Lecture Notes in Computer Science*, pages 389–404. Springer.
- [50] 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)*, Kanpur, India, December 2009, volume 4 of *Leibniz International Proceedings in Informatics*, pages 169–180. Leibniz-Zentrum für Informatik.
- [51] Steve Kremer, Antoine Mercier, and Ralf Treinen. [Reducing equational theories for the decision of static equivalence](#). In Anupam Datta, editor, *Proceedings of the 13th Asian Computing Science Conference (ASIAN'09)*, Seoul, Korea, December 2009, volume 5913 of *Lecture Notes in Computer Science*, pages 94–108. Springer.
- [52] Ștefan Ciobâcă, 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)*, Montreal, Canada, August 2009, *Lecture Notes in Artificial Intelligence*, pages 355–370. Springer.
- [53] Rohit Chadha, Stéphanie Delaune, and Steve Kremer. [Epistemic logic for the applied pi calculus](#). In David Lee, Antónia Lopes, and Arnd Poetsch-Heffter, editors, *Proceedings of IFIP International Conference on Formal Techniques for Distributed Systems (FMOODS/FORTE'09)*, Lisbon, Portugal, June 2009, volume 5522 of *Lecture Notes in Computer Science*, pages 182–197. Springer.
- [54] Steve Kremer. [Computational soundness of equational theories \(tutorial\)](#). In Gilles Barthe and Cédric Fournet, editors, *Revised Selected Papers from the 3rd Symposium on Trustworthy Global Computing (TGC'07)*, Sophia-Antipolis, France, November 2007, volume 4912 of *Lecture Notes in Computer Science*, pages 363–382. Springer, 2008. Invited tutorial.
- [55] 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), Doha, Qatar, November 2008*, volume 5330 of *Lecture Notes in Artificial Intelligence*, pages 128–142. Springer.

- [56] Steve Kremer, Antoine Mercier, and Ralf Treinen. [Proving group protocols secure against eavesdroppers](#). In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *Proceedings of the 4th International Joint Conference on Automated Reasoning (IJCAR'08), Sydney, Australia, August 2008*, volume 5195 of *Lecture Notes in Artificial Intelligence*, pages 116–131. Springer-Verlag.
- [57] 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), Pittsburgh, PA, USA, June 2008*, pages 239–251. IEEE Computer Society Press.
- [58] Stéphanie Delaune, Steve Kremer, and Graham Steel. [Formal analysis of PKCS#11](#). In *Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF'08), Pittsburgh, PA, USA, June 2008*, pages 331–344. IEEE Computer Society Press.
- [59] 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), New Delhi, India, December 2007*, volume 4855 of *Lecture Notes in Computer Science*, pages 133–145. Springer.
- [60] Steve Kremer and Laurent Mazaré. [Adaptive soundness of static equivalence](#). In Joachim Biskup and Javier Lopez, editors, *Proceedings of the 12th European Symposium on Research in Computer Security (ESORICS'07), Dresden, Germany, September 2007*, volume 4734 of *Lecture Notes in Computer Science*, pages 610–625. Springer.
- [61] Véronique Cortier, Steve Kremer, Ralf Küsters, and Bogdan Warinschi. [Computationally sound symbolic secrecy in the presence of hash functions](#). In Naveen Garg and S. Arun-Kumar, editors, *Proceedings of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'06), Kolkata, India, December 2006*, volume 4337 of *Lecture Notes in Computer Science*, pages 176–187. Springer.
- [62] 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), Venice, Italy, July 2006*, pages 28–39. IEEE Computer Society Press.
- [63] Aybek Mukhamedov, Steve Kremer, and Eike Ritter. [Analysis of a multi-party fair exchange protocol and formal proof of correctness in the strand space model](#). In Andrew S. Patrick and Moti Yung, editors, *Revised Papers from the 9th International Conference on Financial Cryptography and Data Security (FC'05), Roseau, The Commonwealth Of Dominica, August 2005*, volume 3570 of *Lecture Notes in Computer Science*, pages 255–269. Springer.
- [64] Mathieu Baudet, Véronique Cortier, and Steve Kremer. [Computationally sound implementations of equational theories against passive adversaries](#). In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05), Lisboa, Portugal, July 2005*, volume 3580 of *Lecture Notes in Computer Science*, pages 652–663. Springer.

- [65] Steve Kremer and Mark D. Ryan. [Analysing the vulnerability of protocols to produce known-pair and chosen-text attacks](#). In Riccardo Focardi and Gianluigi Zavattaro, editors, *Proceedings of the 2nd International Workshop on Security Issues in Coordination Models, Languages and Systems (SecCo'04)*, London, UK, August 2004, volume 128(5) of *Electronic Notes in Theoretical Computer Science*, pages 84–107. Elsevier Science Publishers, May 2005.
- [66] Steve Kremer and Mark D. Ryan. [Analysis of an electronic voting protocol in the applied pi-calculus](#). In Mooly Sagiv, editor, *Programming Languages and Systems — Proceedings of the 14th European Symposium on Programming (ESOP'05)*, Edinburgh, Scotland, UK, April 2005, volume 3444 of *Lecture Notes in Computer Science*, pages 186–200. Springer.
- [67] Shahrokh Saeednia, Steve Kremer, and Olivier Markowitch. [An efficient strong designated verifier signature scheme](#). In Jong In Lim and Dong Hoon Lee, editors, *Revised Papers of the 6th International Conference on Information Security and Cryptology (ICISC'03)*, Seoul, Korea, November 2003, volume 2971 of *Lecture Notes in Computer Science*, pages 40–54. Springer, 2004.
- [68] Rohit Chadha, Steve Kremer, and Andre Scedrov. [Formal analysis of multi-party contract signing](#). In *Proceedings of the 17th IEEE Computer Security Foundations Workshop (CSFW'04)*, Asilomar, Pacific Grove, California, USA, June 2004, pages 266–279. IEEE Computer Society Press.
- [69] Jean Cardinal, Steve Kremer, and Stefan Langerman. [Juggling with pattern matching](#). In Paolo Ferragina and Roberto Grossi, editors, *Proceedings of the 3rd International Conference on Fun with Algorithms (FUN'04)*, Isola d'Elba, Italy, May 2004, pages 147–158. Edizioni Plus, Università di Pisa.
- [70] Olivier Markowitch, Dieter Gollmann, and Steve Kremer. [On fairness in exchange protocols](#). In Pil Joong Lee and Chae Hoon Lim, editors, *Revised Papers of the 5th International Conference on Information Security and Cryptology (ICISC'02)*, Seoul, Korea, November 2002, volume 2587 of *Lecture Notes in Computer Science*, pages 451–464. Springer, 2003.
- [71] Steve Kremer and Jean-François Raskin. [Game analysis of abuse-free contract signing](#). In *Proceedings of the 15th IEEE Computer Security Foundations Workshop (CSFW'02)*, Cape Breton, Nova Scotia, Canada, June 2002, pages 206–220. IEEE Computer Society Press.
- [72] Olivier Markowitch and Steve Kremer. [A multi-party optimistic non-repudiation protocol](#). In Dongho Won, editor, *Proceedings of the 3rd International Conference on Information Security and Cryptology (ICISC 2000)*, Seoul, Korea, December 2000, volume 2015 of *Lecture Notes in Computer Science*, pages 109–122. Springer, 2001.
- [73] Steve Kremer and Olivier Markowitch. [Selective receipt in certified e-mail](#). In C. Pandu Rangan and Cunsheng Ding, editors, *Proceedings of the 2nd International Conference on Cryptology in India (INDOCRYPT'01)*, Chennai, India, December 2001, volume 2247 of *Lecture Notes in Computer Science*, pages 136–148. Springer.
- [74] Olivier Markowitch and Steve Kremer. [An optimistic non-repudiation protocol with transparent trusted third party](#). In George I. Davida and Yair Frankel, editors, *Proceedings of the 4th International Conference on Information Security (ISC'01)*, Malaga, Spain, October 2001, volume 2200 of *Lecture Notes in Computer Science*, pages 363–378. Springer.

- [75] Steve Kremer and Jean-François Raskin. [A game-based verification of non-repudiation and fair exchange protocols](#). In Kim G. Larsen and Modens Nielsen, editors, *Proceedings of the 12th International Conference on Concurrency Theory (CONCUR'01), Aalborg, Denmark, August 2001*, volume 2154 of *Lecture Notes in Computer Science*, pages 551–565. Springer.

### Workshops

- [76] Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel. [A formal analysis of authentication in the TPM \(short paper\)](#). In Véronique Cortier and Kostas Chatzikokolakis, editors, *Preliminary Proceedings of the 8th International Workshop on Security Issues in Coordination Models, Languages and Systems (SecCo'10), Paris, France, August 2010*.
- [77] Ben Smyth, Mark D. Ryan, Steve Kremer, and Mounira Kourjeh. [Election verifiability in electronic voting protocols \(preliminary version\)](#). In Olivier Pereira, Jean-Jacques Quisquater, and François-Xavier Standaert, editors, *Proceedings of the 4th Benelux Workshop on Information and System Security (WISSEC'09), Louvain-la-Neuve, Belgium, November 2009*.
- [78] Ștefan Ciobâcă, Stéphanie Delaune, and Steve Kremer. [Computing knowledge in security protocols under convergent equational theories](#). In Hubert Comon-Lundh and Catherine Meadows, editors, *Preliminary Proceedings of the 4th International Workshop on Security and Rewriting Techniques (SecReT'09), Port Jefferson, NY, USA, July 2009*, pages 47–58.
- [79] Steve Kremer, Antoine Mercier, and Ralf Treinen. [Reducing equational theories for the decision of static equivalence \(preliminary version\)](#). In Hubert Comon-Lundh and Catherine Meadows, editors, *Preliminary Proceedings of the 4th International Workshop on Security and Rewriting Techniques (SecReT'09), Port Jefferson, NY, USA, July 2009*.
- [80] Stéphanie Delaune, Steve Kremer, and Graham Steel. [Formal analysis of PKCS#11](#). In Tei-Wei Kuo and Samuel Cruz-Lara, editors, *Proceedings of the 4th Taiwanese-French Conference on Information Technology (TFIT'08), Taipei, Taiwan, March 2008*, pages 267–278. Invited talk.
- [81] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. [Symbolic bisimulation for the applied pi calculus](#). In Daniele Goria and Catuscia Palamidessi, editors, *Preliminary Proceedings of the 5th International Workshop on Security Issues in Concurrency (SecCo'07), Lisbon, Portugal, September 2007*.
- [82] Steve Kremer and Laurent Mazaré. [Adaptive soundness of static equivalence](#). In Michael Backes and Yassine Lakhnech, editors, *Proceedings of the 3rd Workshop on Formal and Computational Cryptography (FCC'07), Venice, Italy, July 2007*.
- [83] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. [Verifying properties of electronic voting protocols](#). In *Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE'06), Cambridge, UK, June 2006*, pages 45–52.
- [84] Steve Kremer. [Formal verification of cryptographic protocols](#). Invited tutorial, 7th School on Modelling and Verifying Parallel Processes (MOVEP'06), Bordeaux, France, June 2006. 5 pages.

- [85] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. [Receipt-freeness: Formal definition and fault attacks \(extended abstract\)](#). In *Proceedings of the Workshop Frontiers in Electronic Elections (FEE 2005), Milan, Italy, September 2005*.
- [86] Rohit Chadha, Steve Kremer, and Andre Scedrov. [Formal analysis of multi-party contract signing](#). In Peter Ryan, editor, *Preliminary Proceedings of the 4th IFIP WG1.7 Workshop on Issues in the Theory of Security (WITS'04), Barcelona, Spain, April 2004*, pages 153–163.
- [87] Shahrokh Saeednia, Steve Kremer, and Olivier Markowitch. [Efficient designated verifier signatures](#). In *Proceedings of the 24th Symposium on Information Theory in the Benelux, Veldhoven, The Netherlands, May 2003*, pages 187–194.
- [88] Steve Kremer and Olivier Markowitch. [A multi-party non-repudiation protocol](#). In Sihan Qing and Jan H. P. Eloff, editors, *Proceedings of the IFIP TC11 15th Annual Working Conference on Information Security (SEC 2000), Beijing, China, August 2000*, volume 175 of *IFIP Conference Proceedings*, pages 271–280. Kluwer Academic Publishers.
- [89] Steve Kremer and Jean-François Raskin. [Formal verification of non-repudiation protocols — A game approach](#). In Edmund M. Clarke, Mevin Heintze, and Helmut Veith, editors, *Proceedings of the Workshop on Formal Methods and Computer Security (FMCS 2000), Chicago, USA, July 2000*.
- [90] Steve Kremer and Jean-François Raskin. [A game approach to the verification of exchange protocols — Application to non-repudiation protocols](#). In Pierpaolo Degano, editor, *Preliminary Proceedings of the 1st IFIP WG1.7 Workshop on Issues in the Theory of Security (WITS 2000), Geneva, Switzerland, July 2000*.
- [91] Steve Kremer and Olivier Markowitch. [Optimistic non-repudiable information exchange](#). In *Proceedings of the 21st Symposium on Information Theory in the Benelux, Wassenaar, The Netherlands, May 2000*, pages 139–146.

### Theses

- [92] Steve Kremer. [Modelling and analyzing security protocols in cryptographic process calculi](#). Mémoire d'habilitation, École Normale Supérieure de Cachan, France, March 2011.
- [93] Steve Kremer. [Formal analysis of optimistic fair exchange protocols](#). Thèse de doctorat, Université Libre de Bruxelles, Belgium, December 2003.

### Project reports

- [94] Véronique Cortier and Steve Kremer. [Results on a real life case study - helios 2.0](#). Deliverable AVOTE 4.3, (ANR-07-SESU-002), January 2012. 116 pages.
- [95] Steve Kremer. [Implementation of prototypes for equivalence properties](#). Deliverable AVOTE 2.3, (ANR-07-SESU-002), January 2012. 96 pages.
- [96] Steve Kremer. [Results on case studies from literature](#). Deliverable AVOTE 4.2, (ANR-07-SESU-002), January 2011. 96 pages.
- [97] Stéphanie Delaune and Steve Kremer. [Formalising security properties in electronic voting protocols](#). Deliverable AVOTE 1.2, (ANR-07-SESU-002), April 2010. 17 pages.

- [98] Véronique Cortier, Steve Kremer, and Pascal Lafourcade. [Computational soundness of static equivalence](#). Deliverable AVOTE 3.1, (ANR-07-SESU-002), March 2010. 106 pages.
- [99] Stéphanie Delaune and Steve Kremer. [Spécificités des protocoles de vote électronique](#). Deliverable AVOTE 1.1 (ANR-07-SESU-002), January 2009. 8 pages.
- [100] 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.
- [101] Steve Kremer, Yassine Lakhnech, and Ralf Treinen. [The PROUVÉ manual: Specifications, semantics, and logics](#). Technical Report 7, projet RNTL PROUVÉ, December 2005. 49 pages.
- [102] Stéphanie Delaune, Francis Klay, and Steve Kremer. [Spécification du protocole de vote électronique](#). Technical Report 6, projet RNTL PROUVÉ, November 2005. 19 pages.