

Curriculum Vitae

Personal Informations

Surname: Lafourcade
First name: Pascal
Date of birth: April 26th, 1977 at Toulouse
Nationality: French
Email: pascal.lafourcade@imag.fr
Home page: www-verimag.imag.fr/~plafourc/

Professional Address:

Laboratoire Verimag centre Equation
2, avenue de Vignate
38610 Gières FRANCE
Phone: +33 (0) 4 56 52 04 14
Mobile: +33 (0) 6 83 54 90 70
Fax: +33 (0) 4 56 52 03 44

Educations & Positions

2007 – Maître de conférence at University Joseph Fourier, laboratory Verimag team DCS.
2006 – 2007 Post-Doc at ETH Zurich in the Information Security team led by David Basin.
2003 – 2006 Ph.D Student in Computer Science : *Verification of cryptographic protocols*
Laboratoire Spécification et Vérification (LSV), ENS de Cachan,
Laboratoire d'Informatique Fondamentale (LIF), Université Aix-Marseille1.
Thesis advisors: Prof. Dr. Denis Lugiez and Dr. Ralf Treinen
2005 – 2006 University Diploma of ENS Cachan :
Nouvelles Techniques Cognitives d'Apprentissages.
1995 – 2003 Student at Paul Sabatier University, Toulouse France.
2003 : DEA (Postgraduate Degree) in Artificial Intelligence at IRIT.
2002 : Maîtrise (Master's Degree) in Computer Science.
2001 : Maîtrise (Master's Degree) in Fundamental Mathematics.
Licence (Bachelor) in Computer Science.
1999 : Licence (Bachelor) in Fundamental Mathematics.
1995 : Baccalauréat Option Mathematics.

Research Interests

My research is centered around *formal methods* for the symbolic verification of cryptographic protocols. In contrast to many existing works in the field which assume the *perfect cryptography assumption*, that is that cryptographic primitives are unbreakable and can be considered as black boxes, my research aims at verifying protocols by taking into account algebraic properties of cryptographic primitives. More specifically, I have investigated both the *intruder deduction problem* (security against passive attacks) and the *symbolic trace reachability problem* (security against active attacks) for an extension of the Dolev-Yao attacker model by equational axioms.

Participation in Research Projects

Responsible Verimag of ANR Sesur AVOTé: sponsored by the French ministry of Research 2007 - 2010. *Formal verification electronic vote protocols*. (<http://www.lsv.ens-cachan.fr/anr-avote/>).

Responsible Verimag of ANR Sesur SFINCS: sponsored by the French ministry of Research 2007 - 2010. *Securing Flow of INformation for Computing pervasive Systems*. (<http://www.lifl.fr/>).

Member of ANR Sesur SCALP: sponsored by the French ministry of Research 2007 - 2010. *Security of Cryptographic ALgorithms with Probabilities*. (<http://scalp.gforge.inria.fr/>).

Member of the Rossignol project: sponsored by the French ministry of Research (Action Concertée Incitative “security”) 2003 - 2006.
Semantic of the verification of cryptographic protocols : theory and applications.
(www.cmi.univ-mrs.fr/~lugiez/aci-rossignol.html)

Member of the PROUVÉ project: sponsored by the French ministry of Research (Réseaux National des Technologies Logicielles) 2003 - 2006 (www.lsv.ens-cachan.fr/prouve/)
Protocoles cryptographiques : Outils de VÉrification.

Teaching

I am a teaching assistant (three-year contract) at Créteil University (Paris XII) and Fontainebleau IUT (technical institute). I teach an amount of 192 hours in Computer Science:

2008 – 2009

Computer assistant in lecture called INF121: Introduction to programming, fonctionnal approach. (18h)

Assistant in lecture called INF242 Introduction to logic. (36h)

Professor in 3rd year of ENSIMAG for the lecture: Models for security. (18h)

Professor in Master Pro 2 Security, Cryptography and information coding in the unit: Security models: proofs, protocols and politics. (56h)

2007 – 2008

- Computer assistant in lecture called INF121: Introduction to programming, fonctionnal approach. (18h)
- Assistant in lecture called INF242 Introduction to logic. (36h)
- Professor in Master Recherche 2 of UFR IMA for the lecture: Models and analysis of security protocols. (18h)
- Professor in Master Pro 2 Security, Cryptography and information coding in the unit: Security models: proofs, protocols and politics. (56h)
- 2006 – 2007
- Assistant at ETH Zurich, in Modelisation et Simulation. (36 h)
- Assistant at ETH Zurich, in Information Security. (36 h)
- 2005 – 2006
- 1st-year students, project supervisor *MySQL & PhP* (20 h)
 - 1st-year students, exercise sessions *Data Bases SQL* (12 h)
 - 1st-year students, exercise sessions *Fundamentals of Programming in C* (32 h)
 - TD 2nd-year student Orsay IUT , Motivation & Memorisation (8h)
 - TD for assistants :
 - Mental Representations & Motivation, Journées Apprentissages de Marseille (8h)
 - Emotions & Motivation, Journées Apprentissages (8h)<http://www.lsv.ens-cachan.fr/~finkel/ja2006.html>
- 2004 – 2005
- 1st-year students, lecture *Data Bases SQL* (32 h)
 - 2nd-year students, exercise sessions *System and Networks* (32 h)
- 2003 – 2004
- 1st-year students, exercise sessions *Introduction to Programming in C* (64 h)
- 2002 – 2003
- 1st-year students, at INSA Toulouse, exercise sessions *Programmation ADA95* (32h)

Participation to International Schools

- 2009 Spring School Computational and Symbolic Proofs of Security CoSyProof 2009, 4-9 Avril 2009, Itzu-Atawa Japan <http://www.rcis.aist.go.jp/events/csps2009/index-en.html>
- 2006 Summer School Marktoberdorf on Software System Reliability and Security, Marktoberdorf Germany August 1-13, 2006 <http://asimod.in.tum.de/>
- 2005 Spring School on Security at Marseille, France April 25-29, 2005 www.cmi.univ-mrs.fr/~secur05/
- 2004 ICCL Summer School 2004 Proof Theory and Automated Theorem Proving, Technische Universitaat Dresden, June 14-26, 2004 www.computational-logic.org/iccl/events/SA-2004/

Talks

- Exposé au iCIS Seminaire de l'Université de Calgary Février 2009.
- Exposé au 3rd International Workshop on Security and Rewriting Techniques (SecReT'08), Pittsburgh, PA USA, June , 2008. "Relation between Unification Problem and Intruder Deduction Problem"
- Exposé au Workshop on Foundations of Computer Security, Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security, (FCS-ARSPA-WITS'08), June 2008, Pittsburgh PA, USA. "Automated Proofs for Asymmetric Encryption"
- Exposé au Workshop on Formal and Computational Cryptography, (FCC'08), June 2008, Pittsburgh PA, USA. "Automated Proofs for Asymmetric Encryption."
- Exposé invité au seminaire
- Exposé invité au Third Franco-Japanese Computer Security Workshop Nancy, France, 13 et 14 Mars 2008. "Comparing State Spaces in Automatic Security Protocol Verification".
- Exposé au Workshop AVOCS'07 (Seventh International Workshop on Automated Verification of Critical Systems) Oxford, 10-12 September 2007. "Comparing State Spaces in Automatic Security Protocol Verification".
- Exposé invité à la Conférence IBIZA'07 "Automatic Verification of Cryptographic Protocols (Explain by Examples)", 9 fevrier 2007, Kazimierz Dolny Pologne.
- The 33rd International Colloquium on Automata, Languages and Programming (ICALP 2006), Venice, Italy.
- 1st International Workshop on Security and Rewriting Techniques (SecRet 2006), Venice, Italy.
- 16th International Conference on Rewriting Techniques and Applications (RTA 2005), Nara Japan.
- Seminar NQRT at Rennes, France, June 27 2006, <http://www.irisa.fr/NQRT/>
- Spring School on Security at Marseille, France, April 25-29, 2005.
- Several talks in working groups and meetings: Working group SECSI (LSV), MOdelisation VERification team (LIF Marseille), ACI (Action Concertée Incitative) Rossignol à Cachan (LSV) et à l'École polytechnique (LIX), project RNTL (Réseau National des Technologies Logicielles) PROUVÉ à Grenoble (Vérimag) et à Nancy.

Skills, Activities

Reviewing: I have reviewed articles submitted at the international conferences 20th International Conference on Automated Deduction (CADE 2005), 17th International Conference on Rewriting Techniques and Applications (RTA 2006), 34th International Colloquium on Automata, Languages and Programming (ICALP 2007), 12th European Symposium Research Computer Security (ESORICS 2007), 13th European Symposium Research Computer Security (ESORICS 2008), 6th ACM Workshop on Formal Methods in Security Engineering (FMSE 2008), 10th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2009), 21st International Conference on Computer Aided Verification (CAV 2009).

Activities for Verimag

- Co-responsible of the option: “Foundations of Computer Science: Design and Validation” in the Master of Grenoble.
- Co-organisator of the seminar cryptography of Grenoble.
- Responsible of the working group on security in the DCS team at Verimag.
- Co-responsible of the Communication team of Verimag: design of the new VRIMAG flyer.

2008-2009:

- Organiser and PC member of the 2nd Canada-France MITACS Workshop on Foundations & Practice of Security, Grenoble, France 26 - 27 Juin, 2009.
- Organisateur et membre du comité de programme du 3ème Workshop VETO: Security and Electronic Vote, Grenoble, France 28 Juin, 2009. Organiser and PC member of the 3rd Workshop VETO: Security and Electronic Vote, Grenoble, France, 28 Juin, 2009.
- Supervising of 2 TERs in Master 1 Université Joseph Fourier (Vanessa Terrade, Guillaume Meffray).
- Supervising of one TER in 2nd year of ENIMAG (Alitcha Anzala-Yamajako).
- Member of the selection committee of the University of Lille 1.
- Organizer of 2 days of DCS tema seminar (40 persons) at Autrans.
- Organizer of DCS team Diner (40 persons) Château de Sassenage.

2007-2008:

- Supervising of a one-month “stage d’excellence” in L1 (Abdoulaye Maiga).
- Supervising of 2 six-month Master thesis about implementation of a zero-knowledge protocol on a contactless card (Dalal Altenaiji & Aisha Almarashda).
- Supervising of six-month Master thesis on electronic voting (Roukaya KEINJ).
- Supervising of two-month intership on homomorphic encryption and non-interference (Varun Chawla).
- Co-advisor of 4 Magister internships in L3 (Laure Fourad, Mathide Duclos, Endri Vangjel et Pierre-Louis Aublin).
- PC member of the 1st Canada-France MITACS Workshop on Foundations & Practice of Security Montreal, Quebec May 31 - June 2, 2008.
- PC member of the conference IBIZA’08.
- Organizer of 2 days of DCS tema seminar (40 persons) at Cal de Porte.

Activities for the LSV at ENS de Cachan

- Webmaster for the registration website for the conference FORMATS’06 (Paris)
- Member of the organizing Committee of the RED 2005 (meeting for PhD students)
- Member of the SOS team (help for linux users) and INSTSOFT Team (installation of linux softwares) au sein du LSV.

Languages: french, english, spanish, german.

Programming Languages: C, Pascal, Java, Prolog, Scheme, Ocaml, SQL, Php, ADA95.

Publications

International Journals

— 2009 —

- [CLN09] Cas J.F. Cremers, Pascal Lafourcade, and Philippe Nadeau. Comparing state spaces in automatic protocol analysis. 5458/2009:70–94, 2009.

— 2008 —

- [DLLT08] Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis for monoidal equational theories. *Information and Computation*, 206:312–351, February-April 2008.
- [Pap08] M. Schaller P. Lafourcade P. Basin D. Capkun S. Hubaux J.-P. Papadimitratos, P. P. Poturalski. Secure neighborhood discovery: a fundamental element for mobile ad hoc networking. *Communications Magazine, IEEE Publication*, 46(2):132–139, Feb 2008.

— 2007 —

- [LLT07] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Intruder deduction for the equational theory of Abelian groups with distributive encryption. *Information and Computation*, 205(4):581–623, April 2007.

— 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.

International Conferences

— 2009 —

- [GLLS09a] Martin Gagne, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi-Naini. Automated proofs for encryption modes. In *13th Annual Asian Computing Science Conference Focusing on Information Security and Privacy: Theory and Practice (ASIAN0'9)*, Urumqi, China, oct 2009.

— 2008 —

- [CDE⁺08a] Judicael Courant, Marion Daubignard, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. Automated proofs for asymmetric encryption. In *15th ACM Computer and Communications Security Conference (CCS'08)*, 2008.

— 2006 —

- [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 —

- [LLT05a] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Intruder deduction for AC-like equational theories with homomorphisms. 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 308–322, Nara, Japan, April 2005. Springer.

Thesis

— 2006 —

- [Laf06] Pascal Lafourcade. *Vérification des protocoles cryptographiques en présence de théories équationnelles*. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2006. 209 pages.

Other Publications

— 2009 —

- [GL09] Florent Garnier and Pascal Lafourcade. Modularity of termination of trs under fair strategies. Technical report, CNRS, Laboratoire Verimag, University Joseph Fourier, Grenoble I, 2009.
- [GLLS09b] Martin Gagne, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi-Naini. Automated proofs for encryption modes. In Ralf Kuesters, editor, *Workshop on Formal and Computational Cryptography, (FCC'09)*, Port Jefferson NY, USA, jul 2009.
- [ML09] Sreekanth Malladi and Pascal Lafourcade. Prudent engineering practices to prevent type-flaw attacks under algebraic properties. In Hubert Comon-Lundh and Catherine Meadows, editors, *Workshop on Security and Rewriting Techniques, (SecReT'09)*, Port Jefferson NY, USA, jul 2009.

— 2008 —

- [CDE⁺08b] Judicael Courant, Marion Daubignard, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. Automated proofs for asymmetric encryption. In *Proceedings of the LICS-Affiliated Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis*, 2008.
- [Laf08] Pascal Lafourcade. Relation between intruder deduction problem and unification. In *Proceedings of the LICS-Affiliated 3rd International Workshop on Security and Rewriting Techniques (SecReT'08)*, 2008.

— 2007 —

- [CL07] Cas Cremers and Pascal Lafourcade. Comparing state spaces in automatic security protocol verification. Technical Report 558, Department of Computer Science, ETH Zurich, Switzerland, April 2007. 25 pages.
- [KL07] Bogdan Księżopolski and Pascal Lafourcade. Attack and revision of an electronic auction protocol using OFMC. Technical Report 549, Department of Computer Science, ETH Zurich, Switzerland, February 2007. 13 pages.

— 2006 —

- [Laf07] Pascal Lafourcade. Intruder deduction for the equational theory of *exclusive-or* with commutative and distributive encryption. In Maribel Fernández and Claude Kirchner, editors, *Proceedings of the 1st International Workshop on Security and Rewriting Techniques (SecReT'06)*, volume 171 of *Electronic Notes in Theoretical Computer Science*, pages 37–57, Venice, Italy, July 2007. Elsevier Science Publishers.
- [LLT06] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. ACUNh: Unification and disunification using automata theory. In Jordi Levy, editor, *Proceedings of the 20th International Workshop on Unification (UNIF'06)*, pages 6–20, Seattle, Washington, USA, August 2006.

— 2005 —

- [LLT05b] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Intruder deduction for the equational theory of *exclusive-or* with distributive encryption. Research Report LSV-05-19, Laboratoire Spécification et Vérification, ENS Cachan, France, October 2005. 39 pages.

— 2004 —

- [LLT04] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Intruder deduction for AC-like equational theories with homomorphisms. Research Report LSV-04-16, Laboratoire Spécification et Vérification, ENS Cachan, France, November 2004. 69 pages.

— 2003 —

- [Laf03] Pascal Lafourcade. Application de la résolution de conflits « logiques », à l'aide à la décision pour la résolution de aux conflits des problèmes d'ordonnancement. Rapport de DEA, DEA Représentation de la Connaissance et Fomalisation du Raisonnement, Toulouse, France, June 2003. 66 pages.

Contract Reports

— 2004 —

- [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.
- [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.

Interests

Basket-ball player and coach - junior / senior.

Hot air balloon pilot - Air Aventure Association.

Maths tuition - Grammar school / High school.

Summer camp coordinator - teenagers.

Dance : rock, salsa, ballroom dancing.