

Curriculum Vitae

Identité

Nom : LAFOURCADE

Prénom : Pascal

Né le : 26 avril 1977 à Toulouse

Nationalité : Française

Email : pascal.lafourcade@imag.fr

Page web : <http://www-verimag.imag.fr/~plafourc/>

Adresse professionnelle :

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

Formations & postes

2007- : Maître de conférence à l'université Joseph Fourier, laboratoire Verimag équipe DCS.

2006-2007 : Post-Doctorant à l'ETH Zurich dans l'équipe Information Security de David Basin.

2003-2006 : Doctorat de l'ENS Cachan, mention *très honorable* soutenu le 25 Septembre 2006.

Titre : Vérification de protocoles cryptographiques en présence de théories équationnelles.

Composition du Jury :

Président Claude KIRCHNER Directeur de recherche au LORIA (Nancy)

Rapporteurs Yassine LAKHNECH Professeur à l'Université Joseph Fourier (Grenoble)
Luca VIGANÓ Chercheur à l'ETH (Zurich, Suisse)

Directeurs Denis LUGIEZ Professeur à l'Université Aix-Marseille I
Ralf TREINEN Maître de Conférences à l'ENS Cachan

Examineur Yannick CHEVALIER Maître de conférence à l'UPS (Toulouse III)

2005-2006 : Diplôme Universitaire NTCA (Nouvelles Techniques Cognitives d'Apprentissages) de l'ENS Cachan soutenu le 29 Septembre 2006, mention *assez-bien*.

1998-2003 : Étudiant à l'Université Paul Sabatier (Toulouse III).

2003 : **D.E.A.** Représentation de la Connaissance et Formalisation du Raisonnement, mention *assez bien*. Stage de recherche effectué à l'IRIT, sur l'*application de la résolution de conflits "logiques", à l'aide à la décision pour la résolution de aux conflits des problèmes d'ordonnement*. Co-encadré par Claudette CAYROL, Hélène FARGIER et Marie-Christine LAGASQUIÉ-SCHIEX.

2002 : **Maîtrise** d'informatique, mention *bien*.

2001 : **Licence** d'informatique, mention *bien*.

Maîtrise de mathématiques fondamentales.

2000 : **Licence** de mathématiques fondamentales.

1997 : **DEUG** MIAS, option informatique.

1995 : Baccalauréat Scientifique (spécialité mathématiques), mention *assez-bien*.

Interêts de recherche

Je m'intéresse à la vérification symbolique et calculatoire de propriétés de sécurité.

- Je cherche à modéliser et vérifier certaines propriétés de sécurité des protocoles de votes électronique (anonymat, vérifiabilité, équité ...). Pour cela nous nous proposons de regarder ce problème d'un point de vue symbolique mais aussi calculatoire.
- J'étudie également les protocoles de communication sans fils. Mon but est de comprendre comment cette nouvelle technologie modifie les modèles existants en vérification de protocoles cryptographiques, e.g., le modèle de Dolev-Yao.
- Enfin de nombreux travaux considèrent l'hypothèse de chiffrement parfait signifiant qu'il n'est pas possible de déchiffrer un message si on n'en connaît pas la clé de déchiffrement. En augmentant le pouvoir de l'intrus, je cherche à affaiblir cette hypothèse grâce à des propriétés algébriques des systèmes de chiffrement ou du protocole lui-même, ce afin de prouver que le protocole est sûr ou pour découvrir de nouvelles attaques.

Projets

En Cours :

Responsable Verimag de l'ANR Sesur AVOTé : Projet soutenu par le ministère français de la recherche 2007 - 2010. *Vérification formelle de protocoles de vote*. (<http://www.lsv.ens-cachan.fr/anr-avote/>).

Responsable Verimag de l'ANR Sesur SFINCS : Projet soutenu par le ministère français de la recherche 2007 - 2010. *Securing Flow of Information for Computing pervasive Systems*. (<http://www.lifl.fr/>).

Membre de l'ANR Sesur SCALP : Projet soutenu par le ministère français de la recherche 2007 - 2010. *Security of Cryptographic Algorithms with Probabilities*. (<http://scalp.gforge.inria.fr/>).

Passés

Membre de l'ACI Sécurité Rossignol (Action Concertée Incitative). Projet soutenu par le ministère français de la recherche 2003 - 2006. *Sémantique de la vérification de protocoles cryptographiques : théorie et applications*. (www.cmi.univ-mrs.fr/~lugiez/aci-rossignol.html).

Membre de PROUVÉ : projet RNTL (Réseau National des Technologies Logicielles) Projet soutenu par le ministère français de la recherche 2003 -2006. *Protocoles cryptographiques : Outils de Vérification*. (www.lsv.ens-cachan.fr/prouve/).

Enseignement

Actuellement, je suis maître de conférence à l'université Joseph Fourier, depuis la rentrée 2007. Avant je fus successivement :

- Assitant du professeur Gaston GONNET et David BASIN à l'ETH Zurich (Switzerland). (1 an)
- Moniteur (192h en 3 ans) au CIES de Jussieu, à l'université PARIS XII. Enseignement effectué à l'Université de Créteil avec Danièle BEAUQUIER et à l'IUT de Fontainebleau avec Régine LALEAU, Patrick CEGIELSKI et Konstantin VERCHINI.
- Assistant du professeur Alain FINKEL en techniques d'apprentissages dans le supérieur.
- Vacataire à l'INSA (Toulouse) avec Gilles MOTET.

2008 – 2009

Chargé de TP dans le cours INF121 : Introduction à la programmation, approche fonctionnelle. (18h)

Chargé de TD dans le cours INF242 d'Introduction à la logique (base de la démonstration automatique). (36h)

Professeur en 3ème année à l'ENSIMAG dans le module : Modèles pour la sécurité . (18h)

Professeur dans le Master Pro 2 Sécurité, Cryptographie et codage de l'information dans le module : Security models : proofs, protocols and politics. (56h)

2007 – 2008

Chargé de TP dans le cours INF121 : Introduction à la programmation, approche fonctionnelle. (18h)

Chargé de TD dans le cours INF242 d'Introduction à la logique (base de la démonstration automatique). (36h)

Professeur dans le Master Recherche 2 de l'UFR IMA dans le module : Models and analysis of security protocols. (18h)

Professeur dans le Master Pro 2 Sécurité, Cryptographie et codage de l'information dans le module : Security models : proofs, protocols and politics. (56h)

2006 – 2007

TD /TP en 2^{ème} année d'université à l'ETH Zurich, Modelisation et Simulation. (36 h)

TD en 2^{ème} année d'université à l'ETH Zurich, Information Security. (36 h)

2005 – 2006

Projet de fin d'année en 1^{ère} Année d'IUT, Bases de données MySQL et PHP (20 h)

TD en 1^{ère} Année d'IUT, Bases de la programmation en C (32 h)

TD en 1^{ère} Année d'IUT, Bases de données SQL (12 h)

TD 2^{ème} Année IUT d'Orsay, Motivation & Mémorisation (8h)

TD pour moniteurs :

– Représentations mentales & Motivation, Journées Apprentissages de Marseille (8h)

– Émotions & Motivation, Journées Apprentissages (8h)

<http://www.lsv.ens-cachan.fr/~finkel/ja2006.html>

2004 – 2005

TD en 1^{ère} Année d'IUT, Bases de données SQL (32 h).

TD en 2^{ème} Année d'IUT, Système et Réseau (32 h)

2003 – 2004

TD et TP en DEUG 1^{ère} année à l'Université de Créteil, Initiation à la programmation en C (64 h).

2002 – 2003

TP en 1^{ère} Année INSA Toulouse, Programmation en ADA95 (32 h).

Participation à des écoles internationales

- 2009 École de printemps 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 École d'été de Marktoberdorf sur la sûreté et la sécurité des systèmes logiciels, 1-13 août 2006, Marktoberdorf, Allemagne <http://asimod.in.tum.de/>
- 2005 École de printemps sur la sécurité, à 25-29 avril 2005, Marseille, France www.cmi.univ-mrs.fr/~secur05/
- 2004 École d'été ICCL 2004 Théorie de la preuve et preuve automatique de théorème, Technische Universitaat Dresden, 14-26 juin 2004 www.computational-logic.org/iccl/events/SA-2004/

Exposés et séminaires

- 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), Venise Italie.
- 1st International Workshop on Security and Rewriting Techniques (SecRet 2006), Venise Italie.
- 16th International Conference on Rewriting Techniques and Applications (RTA 2005), Nara Japon.
- Séminaire NQRT à Rennes, France, 27 juin 2006, <http://www.irisa.fr/NQRT/>
- École de printemps sur la sécurité à Marseille, France, 25-29 avril 2005.
- Plusieurs exposés : Projet SFINCS, projet AVOTE, groupe de travail SECSI (LSV), équipe MOdelisation VERification (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.

Compétences et activités

Evaluation d'articles : Relecteur pour les conférences et revues : Information and Communication, 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).

Activités à Verimag

- Co-responsable de l'option "Fondements de l'informatique : Conception et Validation" du M2R de Grenoble (2007-).
- Co-organisateur du séminaire cryptographie de Grenoble (2008-).
- Responsable du groupe de travail sécurité de l'équipe DCS Verimag (2007-).
- Co-responsable de l'équipe Communication de Verimag (2008-) : réalisation de la plaquette du laboratoire.

2008-2009 :

- Organisateur et membre du comité de programme du 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.
- Directeur de 2 TERS en Master 1 Université Joseph Fourier (Vanessa Terrade, Guillaume Meffray).
- Directeur d'un TER en 2ème année d'ENSIMAG (Alitcha Anzala-Yamajako).
- Membre du comité de sélection de l'Université de Lille 1.
- Organisateur de 2 jours de séminaires de l'équipe DCS de Verimag (40 personnes) à Autrans.
- Organisateur DCS team Diner (40 personnes) au Château de Sassenage.

2007-2008 :

- Encadrement d'un stage d'excellence d'un mois niveau L1 (Abdoulaye Maiga).
- Tuteur de 2 stages de M2P sur l'implantation de protocoles de preuves à divulgation nulle sur des cartes à puces (Dalal Altenajji & Aisha Almarashda).
- Directeur d'un stage de M2R de 6 mois sur le vote électronique (Roukaya KEINJ).
- Directeur d'un stage de 2 mois sur le chiffrement homomorphique et la non-intrférence (Varun Chawla).
- co-Directeur de 4 stages de Magister L3 (Laure Fourad, Mathide Duclos, Endri Vangjel et Pierre-Louis Aublin).
- Membre du comité de programme du 1er Canada-France MITACS Workshop on Foundations & Practice of Security Montréal, Québec 31 Mai - 2 Juin, 2008.
- Membre du comité de programme de IBIZA'08.
- Organisateur de 2 jours de séminaires de l'équipe DCS de Verimag (40 personnes) au Col de Porte.

Activités au LSV

- Webmaster du site d'inscription à la conférence FORMATS'06 (Paris)
- Membre du comité organisateur des RED 2005 (Rencontres Emplois pour les doctorants, manifestation de 3 jours avec 100 participants)
- Membre de l'équipe SOS (aide pour les utilisateurs de linux) et de l'équipe INSTSOFT (installation de software pour linux)

Langues étrangères : anglais, espagnol, allemand.

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

Publications

Revue Internationale

— 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. 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.

Conférences Internationales

— 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.

Thèse

— 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.

Autres 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'ordonnement. Rapport de DEA, DEA Représentation de la Connaissance et Fomalisation du Raisonnement, Toulouse, France, June 2003. 66 pages.

Rapports de Contract

— 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.

Divers

Entraîneur et joueur de basket-ball de jeunes et adultes.

Pilote de montgolfières dans l'association Air Aventure en Tarn-et-Garonne.

Professeur particulier de mathématiques - niveau : collège et lycée.

Animateur de colonie pour pré-adolescents.

Danse de société : rock, salsa ...