Pascal Lafourcade, Maître de conférences

Identité

LAFOURCADE

Pascal

Né le 26 avril 1977 à Toulouse

pascal.lafourcade@imag.fr

http ://sancy.univ-bpclermont.fr/∼lafourcade/index.html

Adresse professionnelle :

Laboratoire LIMOS
Équipe Réseaux et Protocoles
Campus Universitaire des Cézeaux
BP 86, 63172 Aubière Cedex, France
Téléphone : +33 (0) 4 73 17 70 48
Mobile : +33 (0) 6 83 54 90 70

Formations & postes

2013- : Maître de conférence, mise à disposition de l'Université D'Auvergne (UDA), titulaire de la chaire informatique sur la Confiance Numérique à Clermont Université, Laboratoire LIMOS UMR 6158.

2007- : Maître de conférence à l'Université Joseph Fourier (UJF), laboratoire Verimag UMR 5104.

2012 : Habilitation à Diriger des Recherches, soutenue le 6 Novembre 2012.
Titre : Computer-Aided Security for Encryption Schemes, Voting protocols and Wireless Sensor Networks.
Composition du Jury :

Président	David POINTCHEVAL	Directeur de recherche au CNRS (LIENS, Paris)
Rapporteurs	Gilles BARTHE	Directeur de Recherche à IMDEA (Mardid, Espagne)
	Hubert COMON-LUNDH	Professeur à l'ENS Cachan
	Ralf KÜESTERS	Professeur à l'Université de Kiel (Allemagne)
Examinateurs	David BASIN	Professeur à l'ETH (Zurich, Suisse)
	Yassine LAKHNECH	Professeur à l'Université Joseph Fourier (Grenoble)
	Peter RYAN	Professeur à l'Université de Luxembourg (Luxembourg)

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
Examinateur	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 conflits des problèmes d'ordonnancement*. 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 formaliser les propriétés de sécurité des protocoles de communication et développer des techniques de vérification automatiquement pour ces protocoles. Je développe des méthodes de preuves assistées par ordinateur pour prouver la sécurité des primitives cryptographiques. Mes recherches s'articulent donc autour des thématiques suivantes :

- Réseaux de capteurs :
  - Analyse de sécurité des réseaux sans fil, modèle d'adversaire plus réaliste.
  - Analyse du respect de la vie privée (*privacy*) des communications sans fils.
- Modélisation et analyse de protocoles cryptographiques :
  - Modélisation et vérification des protocoles de e-examen et de réputation.
  - Analyse de sécutité des protocoles de e-cash.
  - Surveillance (monitoring) de protocoles de vente aux enchères.
  - Détection d'intrus par surveillance d'exécution de protocoles.
- Analyse de sécurité de primitives cryptographiques :
  - Preuve de sécurité de schémas basés sur des couplages.

Mots clefs : Vérification formelle, sécurité, réseaux de capteurs, protocoles cryptographiques, modélisation.

Projets

En Cours :

Participation à la soumission du projet ANR 2015 : TECAP

Passés

Membre de l'ANR Verso ProSe : Projet soutenu par le ministère français de la recherche 2010 - 2014. (Protocoles de sécurité : modèle formel, modèle calculatoire, and implémentations) https://crypto.di.ens.fr/projects:prose:main

Membre de l'ANR Verso ARESA 2 : Projet soutenu par le ministère français de la recherche 2009 - 2012, *Avancées en Réseaux de capteurs Efficaces, Sécurisés et Auto-Adaptatifs.* (http://www-verimag.imag.fr/ARESA2.html).

Responsable du projet MSTIC UJF 2011-2012 Terra : Theoretical Evaluation of Randomized Routing Algorithms. (http://www-verimag.imag.fr/Terra.html?lang=fr)

Responsable Verimag de l'ANR Sesur AVOTé : Projet soutenu par le ministère français de la recherche 2007 - 2011. *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://sfincs.gforge.inria.fr).

Membre de l'ANR Sesur SCALP : Projet soutenu par le ministère français de la recherche 2007 - 2011. *Security of Cryptographic ALgorithms with Probabilities.* (http://scalp.gforge.inria.fr/).

Membre du projet Minalogic SHIVA 2009 - 2012. *Secured Hardware Immune Versatile Architecture.* (http://www-verinew.imag.fr/SHIVA.html).

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 mise à disposition de l'Université d'Auvergne, avant je fus successivement :

- 2007-2013 : maître de conférence à l'Université Joseph Fourier, depuis la rentrée 2007.
- 2006 - 2007 : Assitant du professeur Gaston GONNET et David BASIN à l'ETH Zurich (Switzerland). (48H = 2 * 24H TD)
- 2003 - 2006 : 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.
- 2005 - : Assistant du professeur Alain FINKEL en techniques d'apprentissages dans le supérieur.
- 2002 - 2003 : Vacataire à l'INSA (Toulouse) avec Gilles MOTET.

2014 – 2015

Professeur en anglais du module “Security Models” à la filière internationnale à l’ISIMA. (32h)

Professeur du cours Introduction à la sécurité à l’IUT RT.(15h)

Professeur d’un cours sur les méthodes d’apprentissage à l’IUT RT.(12h)

Professeur d’un cours sur les méthodes d’apprentissage à l’IUT INFO.(5h)

2013 – 2014

Professeur d’une semaine de cours de Master intensif à l’Université de Monastir (Tunise), “Modèles pour la sécurité”.

Professeur en anglais du module “Security Models” à la filière internationnale à l’ISIMA. (32h)

Professeur du cours Introduction à la sécurité à l’IUT RT.(18h)

Professeur d’un cours sur les méthodes d’apprentissage à l’IUT RT.(14h)

2012 – 2013

Professeur et responsable du cours APF à PolyTech Grenoble

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. (30h)

Professeur dans le Master en alternance SAFE. (30h)

Correspondant ASUR

Membre de l’IREM groupe algorithmique (48h)

2011 – 2012

Professeur et responsable du cours APF à PolyTech Grenoble en RICM3 : Algorithmique : Programmation Fonctionnelle. (22h)

Professeur et responsable de l’UE INF242 : Introduction à la logique (base de la démonstration automatique). (27h)

Professeur et co-responsable de l’UE INF121 : Introduction à la programmation fonctionnelle. (27h)

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. (30h)

Professeur dans le Master en alternance SAFE. (30h)

Correspondant ASUR

Membre de l’IREM groupe algorithmique (48h)

2010 – 2011

Professeur du cours LP2 à PolyTech Grenoble en RICM3 : Langage de programmation fonctionnelle. (22h)+(20hTD + 15HTP)

Professeur du cours INF242 d'Introduction à la logique (base de la démonstration automatique). (27h)

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. (65h)

Correspondant ASUR

2009 – 2010

Professeur du cours LP2 à PolyTech Grenoble en RICM3 : Langage de programmation fonctionnelle. (22h)

Professeur du cours INF242 d'Introduction à la logique (base de la démonstration automatique). (27h)

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. (65h)

Correspondant ASUR

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$^{\text{ème}}$ année d'université à l'ETH Zurich, Modelisation et Simulation. (36 h)

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

2005 – 2006

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

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

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

TD 2ème 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 1ère Année d'IUT, Bases de données SQL (32 h).

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

2003 – 2004

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

2002 – 2003

TP en 1ère 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 invité à la conférence CSS'2014, Pologne Lublin, Septembre, 2014.
- Exposé invité à la conférence JNCT'2014, Toulouse, Juin, 2014.
- Exposé d'ouverture de la chaire Confiance Numérique, Octobre 2013.
  http://confiance-numerique.clermont-universite.fr/
- Exposé au séminaire du LIMOS, "Formal analysis of security properties for e-voting and e-auction protocols", mai 2013.
  http://limos.isima.fr/spip.php?article745
- Exposé au séminaire méthodes formelles et sécurité de Rennes, "Automatic security proof of cryptographic primitives : public encryption, symmetric encryption modes, MAC", mars 2013
  http://seminaire-dga.gforge.inria.fr/index_fr.html

- Exposé au Citi (Lyon), “Formal analysis of security properties for e-voting and e-auction protocols”, avril 2013.
- Exposé au Groupe de Travail Modélisation et Vérification du LaBri (Bordeaux), “Automatic security proof of cryptographic primitives : public encryption, symmetric encryption modes, MAC”, avril 20113.
  http://mvtsi.labri.fr/
- Exposé invité à la conférence CSS’2012, Pologne, Septembre, 2012.
- Exposé au 3rd Canada-France MITACS Workshop on Foundations & Practice of Security, Toronto, France June, 2010.
- 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/
- Plusieurs exposés : Projet PROSE, Projet ARESA2, 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

Membre de comité : FPS 2009, FPS 2010, SIS 2010, SETOP 2011, AFRICACRYPT 2012, FPS 2012, FPS 2013, GreHack 2012, GreHack2013, Maroc 2013, Hotspot2014, CSS 1014, FPS'14, SDTA'14, DISC'14.

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), Journal IET Information Security 2009, 7th International Symposium on Frontiers of Combining Systems (FROCOS 2009), Journal on Formal Methods in System Design (FMSD 2010), 4th International Workshop on Verification and Evaluation of Computer and Communication Systems (VECOS 2010), 4th Canada-France Workshop on Foundations & Practice of Security (FPS 2011), 38th International Colloquium on Automata, Languages and Programming (ICALP 2011), 22nd International Conference on Rewriting Techniques and Applications (RTA 2011), 12th International Conference on Distributed Computing and Networking (ICDNS2011), 4th SETOP International Workshop on Autonomous and Spontaneous Security (SETOP 2011), 18th ACM Conference on Computer and Communications Securit (CCS 2011), Annual International Conference on the Theory and Applications of Cryptology (AFRICACRYPT 2012), 15èmes Rencontres Francophones pour les Aspects Algorithmiques des Télécommunications (Algotel 2013), The 11th International Conference on Applied Cryptography and Network Security (ACNS 2013), (CSR 2013), Selected Areas in Cryptography 2013 (SAC 2013), (ICNAS 2013), (CADE 2013), 12th Smart Card Research and Advanced Application Conference (CARDIS 2103), Journal Information and Computation (IC 2013), Journal of Automated reasonning (JAR 2013), ACM Transactions on Computational Logic (TOCL 2013), 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2014), 2nd Workshop on Hot Issues in Security Principles and Trust (HotSpot 2014), The 7th International Symposium on Foundations & Practice of Security (FPS'2014),3rd Conference on Cryptography and Security Systems (CCS 2014), 21st ACM Conference on Computer and Communications Security (CSS 2014), 9th DPM International Workshop on Data Privacy Management (DPM 2014).

Activités au LIMOS

- (2013-)Responsbale du séminaire Confiance Numérqiue(2013-)
- Membre de l'IREM de Clermont-Ferrand dans les groupes ISN, informatique sans ordinateur et algorithmique.
  http://confiance-numerique.clermont-universite.fr/

2014-2015 :

- Encadrement d'un stage de 1ère année d'ISIMA sur le chiffrement ADFGVX (anne-Lise Michel et Victor Salard)
- Encadrement d'un stage de 3ème année d'ISIMA sur la cryptograhie visuelle en 3D (Jean-Paul Roussel et Quentin Desmestre).
- Évaluateur pour l'ANR.
- Co-organisation du 1st symposium on Digital Trust in Auvergne (SDTA'14) les 4 et 5 Décembre 2014.
  http://confiance-numerique.clermont-universite.fr/SDTA-2014/

- Directeur de thèse de Xavier Bultel (1/10/2014-), sur la sécurité des données dématérialisées, financée par une bourse de la chaire de confiance numérique.

2013-2014 :

- Co-Directeur de thèse d'Amrit Kumar (1/11/2013-), avec Cédric Lauradoux (Équipe INRIA Privatics).
- Encadrement d'un stage de L3 de l'ENS Lyon, Carine Séraphim.
- Encadrement d'un stage de M2 de l'Université de Monastir (Firas Ben Njima)
- Co-organisation des journées C2 mars 1014
- Membre de 2 comités de sélection à l'Université de Limoges.
- Obtention d'un bourse Erasmus Mundus pour collaborer avec l'université de Manastir (Tunisie).

Activités à Verimag

- Co-responsable du magister L2 au DLST (2010-2013).
- Co-responsable du magister informatique de l'UFR IMA (2009-2013).
- Co-responsable de l'option "Fondements de l'informatique : Conception et Validation" du M2R de Grenoble (2007-2013).
- Co-organisateur du séminaire cryptographie de Grenoble (2008-2013).
- Responsable du groupe de travail sécurité de l'équipe DCS Verimag (2007-2013).
- Co-responsable de l'équipe Comunication de Verimag (2008-2013) : réalisation de la plaquette du laboratoire, site web, 20 ans de Verimag.

2012-2013 :

- Directeur de thèse d'Ali Kassem (3 ans).
- Membre du comité d'organisation des 20 ans de Verimag
- Membre du jury de la thèse d'Abdourhamane IDRISSA, soutenu à l'université de Saint-Étienne le 20 septembre 2012

2011-2012 :

- Directeur d'un stage de M2R sur la vérification de protocoles de routage (Ali Kassem).
- Encadrant d'un post-doc Martin Gagné : vérification formelle de MAC
- Encadrant d'un post-doc Antoine Gerbaud : Analyse théorique d'algoritmes de routage dans les WSN
- Directeur de thèse (3 ans) de Raphaël Jamet intitulé « Protocols and Models for the Security of Wireless Ad-Hoc Networks » (soutenue le 3/10/2014).
- Membre du jury de thèse de Jean Lancrenon : Authentification d'objets à distance soutenue le 22-06-2011 à Grenoble
- Membre du jury de thèse de Marion Daubignard, Formal Methods for Concrete Security Proofs soutenue le 12/01/2012

2010-2011 :

- Encadrant d'un post-doc Martin Gagné : vérification formelle de MAC
- Encadrant d'un post-doc Antoine Gerbaud : Analyse théorique d'algoritmes de routage dans les WSN

- Directeur de thèse (3 ans) de Jannik Dreire sur la vérification de protocoles cryptographiques.
- Directeur d'un stage d'excellence de 2 mois sur la détection d'intrus par anlayse de log (Alexia Madelon).
- Directeur d'un stage d'excellence de 1 mois sur la vérification de protocole de e-auction (Michael Lafrasse).
- Directeur de deux stages de M2P (6 mois) sur le vote électronique (Jean-Pierre Cyndia et Bashar Saleh)
- Co-organisateur du 12th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2011).

2009-2010 :

- Directeur d'un stage d'excellence de 2 mois sur le typage et la non-interference (Sylvain Vigier et Diego Divario).
- Co-directeur d'un stage de M2R de 6 mois sur les chiffrements homomorphiques (Mohamed Alnuaimi).
- Co-directeur d'un stage de M1 de 6 mois sur les protocoles distribués (Clément Ponsonnet).

2008-2009 :

- Membre du PC du 4th Canada-France MITACS Workshop on Foundations & Practice of Security.
- Membre du PC du 4th SETOP International Workshop on Autonomous and Spontaneous Security
- 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 séminaire 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 Altenaiji & Aisha Almarashda).
- Directeur d'un stage de M2R de 6 mois sur le vote electronique (Roukaya KEINJ).
- Directeur d'un stage de 2 mois sur le chiffrement homomorphique et la non-intrference (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 séminaire 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 courant, espagnol scolaire, allemand notion.

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

Publications

*

Bibliographie

En soumission

— 2015 —

[ADJL15] Karine Altisen, Stéphane Devismes, Raphaël Jamet, and Pascal Lafourcade. SR3 : Secure resilient reputation-based routing. *ACM transaction on sensor networks*, 2015.

[AGLM15] Affoua Thérèse Aby, Alexandre Guitton, Pascal Lafourcade, and Michel Misson. SLACK-MAC : Adaptive mac protocol for low duty-cycle wireless sensor networks. *The 20th IEEE Symposium on Computers and Communications (ISCC 2015)*, IEEE, 2015.

[BLM+15] Béatrice Bérard, Pascal Lafourcade, Laure Millet, Maria Potop-Butucaru, Yann Thierry-Mieg, and Sébastien Tixeuil. Formal verification of mobile robot protocols. *Theoretical Computer Science (TCS)*, Elsevier, 2015.

[DDL15] Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. Brandt's fully private auction protocol revisited. *Journal of Computer Security Special Issue on Security and High Performance Computing Systems*, 2015.

[DELL15] Jannik Dreier, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. On the existence and decidability of unique decompositions of processes in the pi-calculus. *Theoretical Computer Science (TCS)*, Elsevier, 2015.

[GLLSN15] Martin Gagné, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi-Naini. Automated proofs of block cipher modes of operation. *Journal of Automatic Reasoning*, 2015.

Livres

— 2015 —

[LL15] Pascal Lafourcade and Isabelle Lebrun. *S'exercer à apprendre*. De Boeck, 2015.

— 2014 —

[CLM14] Fabienne Carrier, Pascal Lafourcade, and Laurent Mounier. *Exercices de programmation fonctionnelle en Ocaml une approche pédagogique par l'algorithmique, la preuve et la complexité*. Ellipses, 2014.

— 2012 —

[DLL12a] Stéphane Devismes, Pascal Lafourcade, and Michel Lévy. *Informatique théorique : Logique et démonstration automatique, Introduction à la logique propositionnelle et à la logique du premier ordre*. Ellipses, 2012.

Édition de proceedings

— 2012 —

[GAL12] Joaquín García-Alfaro and Pascal Lafourcade, editors. *Foundations and Practice of Security - 4th Canada-France MITACS Workshop, FPS 2011, Paris, France, May 12-13, 2011, Revised Selected Papers*, volume 6888 of *Lecture Notes in Computer Science*. Springer, 2012.

Chapitre de livre

— 2012 —

[JL12] Raphaël Jamet and Pascal Lafourcade. *Formal Model for (k)-Neighborhood Discovery Protocols*, chapter in Advances in Network Analysis and its Applications. Springer, 2012.

Magazine

— 2008 —

[PPS+08] Panos Papadimitratos, Marcin Poturalski, Patrick Schaller, Pascal Lafourcade, David Basin, Srdjan Čapkun, and Jean-Pierre Hubaux. Secure Neighborhood Discovery : A Fundamental Element for Mobile Ad Hoc Networking. *IEEE Communications Magazine*, 46(2) :132–139, February 2008.

Revues internationales

— 2014 —

[ADGL14] Karine Altisen, Stéphane Devismes, Antoine Gerbaud, and Pascal Lafourcade. Comparison of mean hitting times for a degree-biased random walk. *Discrete Applied Mathematics*, 170 :104–109, 2014.

[MCL14b] Ismail Mansour, Gérard Chalhoub, and Pascal Lafourcade. Evaluation of secure multihop node authentication and key establishment mechanisms for wireless sensor networks. *Journal of Sensor Actuator Networks*, 3(3) :224–244, 2014.

— 2011 —

[CDE+10] Judicaël Courant, Marion Daubignard, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. Automated proofs for asymmetric encryption. *Journal of Automated Reasoning*, 46(3-4) :261–291, 2010.

— 2008 —

[DLLT08] Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis for monoidal equational theories. *Information and Computation*, 205 :581–623, 2008.

— 2007 —

[KL07] Bogdan Ksiezopolski and Pascal Lafourcade. Attack and revison of an electronic auction protocol using ofmc. *Annales UMCS, Informatica*, 6(1) :171–183, 2007.

[Laf07a] Pascal Lafourcade. Intruder deduction for the equational theory of exclusive-or with commutative and distributive encryption. *Electr. Notes Theor. Comput. Sci.*, 171(4) :37–57, 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

— 2015 —

[DGK+15] Jannik Dreier, Rosario Giustolisi, Ali Kassem, Pascal Lafourcade, Gabriele Lenzin, and Peter Y.A. Ryan. A framework for testing verifiability in traditional and electronic exams. In *ISPEC 2015*, 2015.

— 2014 —

[DGK+14] Jannik Dreier, Rosario Giustolisi, Ali Kassem, Pascal Lafourcade, Gabriele Lenzini, and Peter Y. A. Ryan. Formal analysis of electronic exams. In Mohammad S. Obaidat, Andreas Holzinger, and Pierangela Samarati, editors, *SECRYPT 2014 - Proceedings of the 11th International Conference on Security and Cryptography, Vienna, Austria, 28-30 August, 2014*, pages 101–112. SciTePress, 2014. Best Paper Award.

[DJL14] Jannik Dreier, Hugo Jonker, and Pascal Lafourcade. Secure auctions without cryptography. In Alfredo Ferro, Fabrizio Luccio, and Peter Widmayer, editors, *Fun with Algorithms - 7th International Conference, FUN 2014, Lipari Island, Sicily, Italy, July 1-3, 2014. Proceedings*, volume 8496 of *Lecture Notes in Computer Science*, pages 158–170. Springer, 2014.

[JL14b] Raphaël Jamet and Pascal Lafourcade. (in)corruptibility of routing protocols. In *Foundations and Practice of Security - 7th International Symposium, FPS 2014, Montréal, Canada, 2014*, Lecture Notes in Computer Science. Springer, 2014. Best Paper Award.

[KLL14a] Ali Kassem, Pascal Lafourcade, and Yassine Lakhnech. Formal verification of e-reputation protocols. In *Foundations and Practice of Security - 7th International Symposium, FPS 2014, Montréal, Canada*, Lecture Notes in Computer Science. Springer, 2014.

[KLL14c] Amrit Kumar, Pascal Lafourcade, and Cédric Lauradoux. Performances of cryptographic accumulators. In *IEEE 39th Conference on Local Computer Networks, LCN 2014, Edmonton, AB, Canada, 8-11 September, 2014*, pages 366–369. IEEE Computer Society, 2014.

[MCL+14a] Ismail Mansour, Gérard Chalhoub, Pascal Lafourcade, , and François Delobel. Secure key renewal and revocation for wireless sensor networks. In *IEEE 39th Conference on Local Computer Networks, LCN 2014, Edmonton, AB, Canada, 8-11 September, 2014*, pages 382–385. IEEE Computer Society, 2014.

[MCL14c] Ismail Mansour, Gérard Chalhoub, and Pascal Lafourcade. Secure multihop key establishment protocols for wireless sensor networks. In Zbigniew Kotulski, Bogdan Ksiezopolski, and Katarzyna Mazur, editors, *Cryptography and Security Systems - Third International Conference, CSS 2014, Lublin, Poland, September 22-24, 2014. Proceedings*, volume 448 of *Communications in Computer and Information Science*, pages 166–177. Springer, 2014.

[MRC+14] Ismail Mansour, Damian Rusinek, Gérard Chalhoub, Pascal Lafourcade, and Bogdan Ksiezopolski. Multihop node authentication mechanisms for wireless sensor networks. In Song Guo, Jaime Lloret, Pietro Manzoni, and Stefan Ruehrup, editors, *Ad-hoc, Mobile, and Wireless Networks - 13th International Conference, ADHOC-NOW 2014, Benidorm, Spain, June 22-27, 2014 Proceedings*, volume 8487 of *Lecture Notes in Computer Science*, pages 402–418. Springer, 2014.

— 2013 —

[ADJL13b] Karine Altisen, Stéphane Devismes, Raphael Jamet, and Pascal Lafourcade. SR3 : Secure resilient reputation-based routing. In *IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS 2013, Cambridge, MA, USA, May 20-23, 2013*, pages 258–265. IEEE, 2013.

[DDL13] Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. Brandt's fully private auction protocol revisited. In Amr Youssef, Abderrahmane Nitaj, and Aboul Ella Hassanien, editors, *Progress in Cryptology - AFRICACRYPT 2013, 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings*, volume 7918 of *Lecture Notes in Computer Science*, pages 88–106. Springer, 2013.

[DELL13] Jannik Dreier, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. On unique decomposition of processes in the applied -calculus. In Frank Pfenning, editor, *Foundations of Software Science and Computation Structures - 16th International Conference, FOSSACS 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*, volume 7794 of *Lecture Notes in Computer Science*, pages 50–64. Springer, 2013.

[DJL13] Jannik Dreier, Hugo Jonker, and Pascal Lafourcade. Defining verifiability in e-auction protocols. In Kefei Chen, Qi Xie, Weidong Qiu, Ninghui Li, and Wen-Guey Tzeng, editors, *8th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '13, Hangzhou, China - May 08 - 10, 2013*, pages 547–552. ACM, 2013.

[DLL13] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. Formal verification of e-auction protocols. In David A. Basin and John C. Mitchell, editors, *Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*, volume 7796 of *Lecture Notes in Computer Science*, pages 247–266. Springer, 2013.

[GLL13] Martin Gagné, Pascal Lafourcade, and Yassine Lakhnech. Automated security proofs for almost-universal hash for mac verification. In Jason Crampton, Sushil Jajodia, and Keith Mayes, editors, *Computer Security - ESORICS 2013 - 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013. Proceedings*, volume 8134 of *Lecture Notes in Computer Science*, pages 291–308. Springer, 2013.

[JL14a] Raphael Jamet and Pascal Lafourcade. Discovering flaws in ids through analysis of their inputs. In Jean Luc Danger, Mourad Debbabi, Jean-Yves Marion, Joaquín García-Alfaro, and A. Nur Zincir-Heywood, editors, *Foundations and Practice of Security - 6th International Symposium, FPS 2013, La Rochelle, France, October 21-22, 2013, Revised Selected Papers*, volume 8352 of *Lecture Notes in Computer Science*. Springer, 2014.

[KLL14b] Ali Kassem, Pascal Lafourcade, and Yassine Lakhnech. A more realistic model for verifying route validity in ad-hoc networks. In Jean Luc Danger, Mourad Debbabi, Jean-Yves Marion, Joaquín García-Alfaro, and A. Nur Zincir-Heywood, editors, *Foundations and Practice of Security - 6th International Symposium, FPS 2013, La Rochelle, France, October 21-22, 2013, Revised Selected Papers*, volume 8352 of *Lecture Notes in Computer Science*. Springer, 2014.

— 2012 —

[ADGL12] Karine Altisen, Stéphane Devismes, Antoine Gerbaud, and Pascal Lafourcade. Analysis of random walks using tabu lists. In Guy Even and Magnús M. Halldórsson, editors, *Structural Information and Communication Complexity - 19th International Colloquium, SIROCCO 2012, Reykjavik, Iceland, June 30-July 2, 2012, Revised Selected Papers*, volume 7355 of *Lecture Notes in Computer Science*, pages 254–266. Springer, 2012.

[DLL12b] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. Defining privacy for weighted votes, single and multi-voter coercion. In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*, volume 7459 of *Lecture Notes in Computer Science*, pages 451–468. Springer, 2012.

[DLL12c] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. A formal taxonomy of privacy in voting protocols. In *Proceedings of IEEE International Conference on Communications, ICC 2012, Ottawa, ON, Canada, June 10-15, 2012*, pages 6710–6715. IEEE, 2012.

[GKL12] Nacira Ghoualmi, Noudjoud Kahya, and Pascal Lafourcade. Key management protocol in wimax revisited. In *The Third International Conference on Communications Security and Information Assurance (CSIA 2012)*, Delhi, India, May 2012. Springer.

— 2011 —

[DLL12d] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. Vote-independence : A powerful privacy notion for voting protocols. In Joaquín García-Alfaro and Pascal Lafourcade, editors, *Foundations and Practice of Security - 4th Canada-France MITACS Workshop, FPS 2011, Paris, France, May 12-13, 2011, Revised Selected Papers*, volume 6888 of *Lecture Notes in Computer Science*, pages 164–180. Springer, 2012.

[FLA11] Laurent Fousse, Pascal Lafourcade, and Mohamed Alnuaimi. Benaloh's dense probabilistic encryption revisited. In *Progress in Cryptology - AFRICACRYPT 2011 - 4th International Conference on Cryptology in Africa, Dakar, Senegal, July 5-7, 2011. Proceedings*, volume 6737 of *Lecture Notes in Computer Science*, pages 348–362. Springer, 2011.

[GLLSN12] Martin Gagné, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi-Naini. Automated verification of block cipher modes of operation, an improved method. In Joaquín García-Alfaro and Pascal Lafourcade, editors, *Foundations and Practice of Security - 4th Canada-France MITACS Workshop, FPS 2011, Paris, France, May 12-13, 2011, Revised Selected Papers*, volume 6888 of *Lecture Notes in Computer Science*, pages 23–31. Springer, 2012.

— 2010 —

[CDE+11] Judicaël Courant, Marion Daubignard, Cristian Ene, Pascal Lafourcade, and Yassine Lakhnech. Automated proofs for asymmetric encryption. In Dennis Dams, Ulrich Hannemann, and Martin Steffen, editors, *Concurrency, Compositionality, and Correctness, Essays in Honor of Willem-Paul de Roever*, volume 5930 of *Lecture Notes in Computer Science*, pages 300–321. Springer, 2011.

[TWE+10] Jérémie Tharaud, Sven Wohlgemuth, Isao Echizen, Noboru Sonehara, Günter Müller, and Pascal Lafourcade. Privacy by data provenance with digital watermarking - a proof-of-concept implementation for medical services with electronic health records. In *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2010), Darmstadt, Germany, 15-17 October, 2010, Proceedings*, pages 510–513. IEEE Computer Society, 2010.

— 2009 —

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

[LTV09] Pascal Lafourcade, Vanessa Terrade, and Sylvain Vigier. Comparison of cryptographic verification tools dealing with algebraic properties. In Pierpaolo Degano Joshua Guttman, editor, *sixth International Workshop on Formal Aspects in Security and Trust, (FAST'09)*, Eindhoven, Netherlands, nov 2009.

— 2008 —

[CDE+08a] Judicaël 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 Buglesi, 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 et Habilitation à diriger des recherches

— 2012 —

[Laf12] Pascal Lafourcade. *Computer-Aider Security for : Cryptographic Primitives, Voting Protocols and Wireless Sensor Networks*. Habilitation à diriger des recherches, Verimag, Grenoble, France, 11 2012. 192 pages.

— 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.

— 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.

Workshops

— 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] Judicaël 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*, Pittsburg, USA, 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.

— 2006 —

[Laf07b] 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.

Conférences Françaises

— 2014 —

[MLC14a] Ismail Mansour, Pascal Lafourcade, and Gérard Chalhoub. Mécanismes d'authentification pour des réseaux de capteurs sans fil multi-sauts. In *16èmes Rencontres Francophones pour les Aspects Algorithmiques des Télécommunications, Algotel'2014, Le-Bois-Plage-en-Ré, France*, 2014.

[MLC14b] Ismail Mansour, Pascal Lafourcade, and Gérard Chalhoub. Révocation et renouvellement sécurisés de clés pour les rcsf. In *Journées Nationales de Communications Terrestres, JNCT'14, Blagnac France*, 2014.

— 2013 —

[ADJL13a] Karine Altisen, Stéphane Devismes, Raphael Jamet, and Pascal Lafourcade. Routage sécurisé et résilient pour réseaux de capteurs sans fils. In *15èmes Rencontres Francophones pour les Aspects Algorithmiques des Télécommunications Algotel 2013*, 2013.

— 2011 —

[ADLP11] Karine Altisen, Stéphane Devismes, Pascal Lafourcade, and Clément Ponsonnet. Routage par marche aléatoire à listes tabous. In *In Proceedings of 13èmes Rencontres Francophones pour les Aspects Algorithmiques des Télécommunications, Algotel'2011. Pages 87-90, May 23-26, 2011. Cap Estérel.*, page 5, 2011.

Autres publications

— 2011 —

[ADGL11] Karine Altisen, Stéphane Devismes, Antoine Gerbaud, and Pascal Lafourcade. Technical report for simple and biased random walks with tabu list. Technical report, Laboratory VERIMAG, 2011.

— 2010 —

[ADLP10] K. Altisen, S. Devismes, P. Lafourcade, and C. Ponsonnet. Probabilistic methods for routing in wireless sensor networks. Technical report, Laboratory VERIMAG, 2010.

— 2007 —

[CL07] Cas Cremers and Pascal Lafourcade. Comparing state spaces in automatic security protocol verification. Technical Report 558, Department of Computer Science, ETH Zurich, 2007. 25 pages.

— 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.

Pédagogie

[DGL07] Dariusz Dobrowolski, Anna Grabowska, and Pascal Lafourcade. The concept of developing e-learnung repository - metadata and group work. In *ICETA 2007, 5 th International Conference on Emerging e-Learning Technologies and Applications*, pages 217–220, The High Tatra, Slovakia, sept 2007.

[HDB+12] Christian Hoffmann, Julien Douady, Martial Billon, Marceline Bonvalot, Florence Courtois, Pascal Lafourcade, Isabelle Le Brun, Estelle Moraux, Claire Rist, and Marie-Françoise Soulage. Deux approches pour une formation opérante des étudiants de l'université joseph fourier (grenoble, france) aux méthodes de travail universitaire. In *27e Congrès International de Pédagogie Universitaire (Association Internationale de Pédagogie Univeersitaire AIPU)*, Trois-Rivières, Québec, may 2012.

[Laf11a] Pascal Lafourcade. La génération Y. Colloque Pédagogique National GEII, june 2011. Angoulême, publié dans le journal des IUTs GEII.

[Laf11b] Pascal Lafourcade. Techniques d'apprentissage en liaison avec l'analyse cognitive. Colloque Pédagogique National GEII, june 2011. Angoulême, publié dans le journal des IUTs GEII.

Vulgarisation

[DP10] Marion Daubignard and Lafourcade Pascal. Je veux te dire un secret mais tout le monde m'écoute. Visions Croisées, magazine de vulgarisation scientifique édité par les moniteurs du CIES de l'Académie de Grenoble, march 2010.

[Laf10] Pascal Lafourcade. Sécurité et cryptographie par l'image, may 2010. Conférence dans le cadre du programme « Invitez les sciences et la technologie dans votre classe »organisé par la DAAC de Grenoble (Délégation Académique aux arts et à la culture de l'Académie).

Divers

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

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

Danse de société : rock, salsa ...