
DOSSIER DE QUALIFICATION
AUX FONCTIONS DE MAÎTRE DE CONFÉRENCES

Section 27

Pascal Lafourcade

Ce dossier est destiné à la qualification aux candidatures de Maître de Conférence dans la section 27 (Informatique).

Table des matières

1	Résumé.	2
2	Curriculum Vitae.	3
	Identité.	3
	Fonctions occupées.	3
	Diplômes.	3
3	Activités d’enseignements.	5
	Actuellement à l’ETH Zürich	5
	Enseignements dans le cadre du monitorat.	5
	Autres activités d’enseignements.	5
	Projets d’ enseignements.	6
4	Activités administratives.	7
5	Activités de recherche.	8
	Participation aux projets.	10
	Participation à des écoles internationales.	11
	Compétences et activités.	11
	Exposés et séminaires.	11
6	Détails des enseignements dispensés par matière et par année :	13
	En informatique.	13
	En technique d’apprentissages.	16
	Documents pédagogiques réalisés.	18
7	Détails de mes activités de recherche.	20
	Travaux effectués lors du DEA RCFR.	20
	Travaux effectués pendant ma thèse.	20
	Travaux effectués après ma thèse.	24
	Projet de Recherche.	25
	Références.	25
8	Listes des pièces jointes.	28

1 Résumé.

Coordonnées.

Pascal LAFOURCADE, 29 ans né le 26 avril 1977 à Toulouse (31).

Information Security	Téléphone : +41 44 632 72 72
ETH Zürich IFW C 46.1	Fax : +41 44 632 11 72
Haldeneggsteig, 4	Email : pascal.lafourcade@inf.ethz.ch
CH-8092 Zürich, Suisse	Page Web : www.inf.ethz.ch/personal/pascall/

Enseignements.

- Assistant à l'ETH Zürich (2 × 24h de TD).
- Moniteur au C.I.E.S de Jussieu (3 × 64h de TD).
- Assistant en techniques d'apprentissages pour des universitaires (4 × 8h de TD).
- Vacataire à l'INSA Toulouse (20h de TD).

Thèmes de recherche.

Mon thème de recherche est la vérification formelle de protocoles cryptographiques. Je me suis jusqu'à présent intéressé à certaines propriétés algébriques des protocoles cryptographiques. J'ai développé des méthodes formelles de vérification pour la sécurité de la propriété de secret. J'étudie maintenant lors de mon séjour post-doctoral à l'ETH Zürich de nouvelles propriétés dans le cadre des communications wireless (sans fil).

Mots clefs : Méthodes formelles, vérification de protocoles cryptographiques, théories équationnelles, preuves automatiques, normalisation de preuves, système de déduction, unification, réécriture, résolution de systèmes d'équations.

Publications, communications & projets.

2 Revues Internationales, plus deux autres en cours de soumission.

2 Conférences Internationales

7 Autres publications : workshops, rapports techniques, projets

7 Présentations & Séminaires

Participations à 3 projets : VerSePro, ACI sécurité Rossignol et RNTL Prouvé.

2 Curriculum Vitae.

Identité.

Nom : LAFOURCADE
Prénom : Pascal
Né le : 26 avril 1977 à Toulouse (31)
Nationalité : Française
Émail : pascal.lafourcade@inf.ethz.ch
Page web : www.inf.ethz.ch/personal/pascall/

Adresse professionnelle :

Pascal LAFOURCADE
Information Security
ETH Zürich, IFW C 46.1
Haldeneggsteig 4
CH-8092 Zürich, Suisse
Téléphone : +41 44 632 72 72
Fax : +41 44 632 11 72

Fonctions occupées.

Oct 2006 - : Bourse DGA pour un stage post-doctoral d'un an dans l'équipe Information Security de David BASIN à l'ETH Zürich.

Oct 2003 - Oct 2006 : Moniteur à l'université Paris XII (C.I.E.S. de Jussieu) et allocataire de recherche au Laboratoire Spécification et Vérification (LSV) de Cachan (2 ans) et au Laboratoire d'Informatique Fondamentale (LIF) de Marseille (1 an), dans le cadre de l'ACI Sécurité Rossignol.

Diplômes.

Doctorat de l'École Normale Supérieure de Cachan : Débuté le 1er Octobre 2003, soutenu le 25 Septembre 2006 à Cachan et obtenu avec mention *Très Honorable*.

Sujet :

« *Vérification de protocoles cryptographiques en présence de théories équationnelles.* »

Président Claude KIRCHNER Directeur de recherche au LORIA (Nancy).

Rapporteurs Luca VIGANÒ Chercheur à l'ETH (Zürich, Suisse).

Yassine LAKHNECH Prof. à l'Université Joseph Fourier (Grenoble).

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

Directeurs Denis LUGIEZ Professeur à l'Université Aix-Marseille I.

Ralf TREINEN Maître de Conférence à l'ENS Cachan.

Jan 2006 - Sept 2006 : Diplôme Universitaire **NTCA** (Nouvelles Techniques Cognitives d'Apprentissages) de l'École Normale Supérieure de 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 : **Maîtrise** de mathématiques fondamentales.
Licence d'informatique, mention *Bien*.
- 2000 : **Licence** de mathématiques fondamentales.
- 1997 : **DEUG** MIAS, option informatique.
- 1995** : Baccalauréat Scientifique (spécialité mathématiques), mention *Assez-Bien*.

3 Activités d'enseignements.

J'ai effectué mes expériences d'enseignements en informatique en tant que moniteur et vacataire. La figure 1 donne un résumé des différents enseignements dispensés lors de mon monitorat à l'Université Paris XII en première année à l'université de Créteil et à l'Institut Universitaire de Technologie de Fontainebleau. J'ai également été assistant en techniques d'apprentissages dans le supérieur, vacataire en informatique à l'INSA Toulouse, et professeur particulier en mathématiques. Actuellement, je suis en stage post-doctoral à l'ETH Zürich (Suisse), dans le cadre de ce stage j'ai un poste d'assistant en informatique et en mathématiques. Ces enseignements sont réalisés en anglais. Je présente ici une vue synthétique de ces enseignements et détaille le contenu de chaque enseignement par matière et par année dans la suite du document (cf section 6).

Actuellement à l'ETH Zürich

Je suis assistant en anglais dans les cours :

- « Modelisation & Simulation » du professeur Gaston GONNET (24h de TD)
- « Information & Security » du professeur David BASIN (24h de TD)

Enseignements dans le cadre du monitorat.

Tutrice de monitorat : Danièle BEAUQUIER, LACL, Université Paris XII.

Période : Années universitaires 2003-2006.

Durée : $3 \times 64h = 192h$ équivalent TD.

Public	Intitulé	Nature	Eq TD
1ère Année DEUG	Initiation à la Programmation en C	TD/TD	64h
1ère Année IUT	Bases de données	TD	12h
	Php & Mysql	Projet	20h
	Base de la Programmation en C	TD	32h
	Bases de données	TD	32h
2ème Année IUT	Système & Réseaux	TP	32h
		Total	192h

FIG. 1 – Résumé des enseignements dispensés par niveaux dans le cadre du monitorat.

Autres activités d'enseignements.

Assistant en techniques d'apprentissages :

- 8h TD, 2ème Année à l'IUT d'Orsay 2006 : *Motivation et mémorisation.*

- 8h TD, moniteurs des C.I.E.S. Jussieu, Versailles et Sorbonne : *Émotions et motivation*, lors des Journées Apprentissages de Cachan 2006.
- 8h TD, moniteurs des C.I.E.S. de Marseille : *Représentations mentales et motivation*, lors des Journées Apprentissages de Marseille 2006.
- 8h TD, 1ère année de l'ESO : *Représentations mentales, mémorisation, émotions et motivations* 2006.

Vacations : vacataire en 1ère Année à l'INSA Toulouse 20h de TP : Programmation en ADA95 (2002-2003).

Soutien scolaire : professeur particulier de mathématiques pour tous les niveaux du collège au lycée, 2h à 4h par semaine (1995 - 2001).

Projets d'enseignements. ---

Les matières que j'aimerais enseigner se répartissent en trois catégories :

D'une part je suis attaché aux thèmes proches de l'informatique théorique, plus proches de ma formation et pour lesquels je peux enseigner à différents niveaux.

D'autre part j'ai particulièrement apprécié enseigner à un public de « non informaticiens » et leur apprendre les bases d'un langage de programmation. Cela m'a permis de me confronter aux problèmes qu'ils rencontrent et ce déficit pédagogique me passionne. Je suis prêt à enseigner l'informatique à des étudiants débutants en premières années d'université.

Finalement fort de mon expérience lors de mes différentes interventions en techniques d'apprentissages, j'aimerais participer à l'élaboration d'un projet permettant d'aider les étudiants à mieux réussir leurs études. Pour ce faire, j'envisage de construire un cours sur les techniques d'apprentissages (mémorisation, motivation, représentations mentales, ...) en me basant sur les progrès et découvertes scientifiques des neurosciences lors des ces vingt dernières années.

4 Activités administratives.

Organisation de colloques :

- Participation au comité d'organisation de la conférence internationale FORMATS 2006 à Paris du 25 au 28 Septembre 2006 (Webmaster du site d'inscription). <http://www.lsv.ens-cachan.fr/formats06/>
- Participation au comité d'organisation des Journées Apprentissages 2006 à Paris du 17 au 19 Mai 2006 (Webmaster du site d'inscription et assistant en TD). <http://www.lsv.ens-cachan.fr/~finkel/ja2006.html>
- Membre du comité organisateur des Rencontres Emplois pour les Doctorants (RED) de l'École Doctorale Sciences Pratiques (EDSP) à l'École Normale Supérieure de Cachan en mai 2005, manifestation de 3 jours organisée tous les 18 mois. Cette manifestation a pour but de donner aux doctorants des informations sur les possibilités de carrières à la fois publiques et privées qui leur sont offertes après leur doctorat. Nous avons réuni lors des ces rencontres une centaine de doctorants et une vingtaines d'intervenants extérieurs (industriels, universitaires, anciens doctorants, chasseur de têtes ...).

Charges Administratives :

- Membre de l'équipe SOS, mailing liste d'aide pour les utilisateurs de Linux.
- Membre de l'équipe INSTSOFT, groupe d'installation du Laboratoire Spécification et Vérification (LSV) pour des logiciels sous Linux.
- Responsable de la mise à jour de la page web interne de recherche bibliographique pour les membres du LSV. Cette page récapitule l'ensemble des moyens existants pour rechercher une référence bibliographique à l'ENS Cachan.
- Responsable des pages web internes d'aide pour l'utilisation du graveur et du scanner du LSV.

5 Activités de recherche.

Je donne une vue synthétique de mes travaux de recherche en présentant la liste de mes publications. Je récapitule ensuite mes différentes activités de recherche, de communications et de formations à travers les différents projets, écoles d'été, conférences et séminaires auxquels j'ai participé. Dans la section 7, je détaille l'ensemble de mes recherches passées et actuelles. Je présente également mon projet de recherche. L'ensemble de mes publications est disponible électroniquement :

<http://www.lsv.ens-cachan.fr/~lafourca/publis.php>

Revue internationale

— 2006 —

- [1] V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1) :1–43, 2006.
- [2] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of abelian groups with distributive encryption. *Information and Computation*, 2006. To appear. 51 pages.

Conférences internationales

— 2006 —

- [3] S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis in presence of a homomorphism operator and *exclusive or*. In M. Bugles, B. Preenel, V. Sassone, and I. 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 132–141, Venice, Italy, July 2006. Springer-Verlag.

— 2005 —

- [4] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for AC-like equational theories with homomorphisms. In J. 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, Apr. 2005. Springer-Verlag.

Mémoires

— 2006 —

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

— 2003 —

- [6] P. 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 Formalisation du Raisonnement, Toulouse, France, June 2003. 66 pages.

Autres publications

— 2006 —

- [7] P. Lafourcade, D. Lugiez, and R. Treinen. ACUNh : Unification and disunification using automata theory. In J. Levy, editor, *Proceedings of the 20th International Workshop on Unification (UNIF'06)*, pages 6–20, Seattle, Washington, USA, Aug. 2006.

— 2005 —

- [8] P. Lafourcade, D. Lugiez, and R. 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, Oct. 2005. 39 pages.

Soumissions à des revues internationales

— 2006 —

- [9] S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis for monoidal equational theories. Research Report LSV-06-17, Laboratoire Spécification et Vérification, ENS Cachan, France, Nov. 2006. 47 pages.
- [10] P. Lafourcade. Intruder deduction for the equational theory of *exclusive-or* with commutative and distributive encryption. In M. Fernández and C. Kirchner, editors, *Preliminary Proceedings of the 1st International Workshop on Security and Rewriting Techniques (SecReT'06)*, pages 20–24, Venice, Italy, July 2006.

Rapports de Contract

— 2004 —

- [11] V. Bernat, H. Comon-Lundh, V. Cortier, S. Delaune, F. Jacquemard, P. Lafourcade, Y. Lakhnech, and L. 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, Dec. 2004. 33 pages.
- [12] V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. Technical Report 2, projet RNTL PROUVÉ, June 2004. 19 pages.

Participation aux projets.

Membre de l'ACI Sécurité Rossignol (Action Concertée Incitative). Projet soutenu par le ministère français de la recherche 2003 - 2006, réunissant les équipes de recherche suivantes :

- LIF de Marseille
- INRIA Futurs, LIX
- LSV, ENS Cachan
- Verimag (Grenoble)

Sur le thème : *Sémantique de la vérification de protocoles cryptographiques : théorie et applications*. (www.cmi.univ-mrs.fr/~lugiez/aci-rossignol.html).

Membre de projet RNTL (Réseau National des Technologies Logicielles) PROUVÉ, projet soutenu par le ministère français de la recherche 2003 -2006, réunissant les partenaires suivantes :

- CRIL Technology Systèmes Avancés
- France Télécom R&D
- INRIA Lorraine (Nancy)
- LSV, ENS de Cachan
- Verimag (Grenoble)

Sur le thème : *Protocoles cryptographiques : Outils de Vérification*. (www.lsv.ens-cachan.fr/prouve/).

Membre du Projet VerSePro : Provably Secure Protocols for Wireless Networks, entre l'École Polytechnique Fédérale de Lausanne (EPFL) et l'Eidgenössische Technische Hochschule Zürich (ETHZ), projet faisant partie du projet décennal Mobile and Information Communication Systems (MISC : www.mics.org/).

Participation à des écoles internationales.

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 25-29 avril 2005 Marseille, France.

www.cmi.univ-mrs.fr/~secur05/

2004 École d'été ICCL : Théorie de la preuve et preuve automatique de théorème, 14-26 juin 2004, Technische Universität Dresden.

www.computational-logic.org/iccl/events/SA-2004/

Compétences et activités.

Évaluation d'articles : J'ai été relecteur pour les conférences suivantes : 20ème conférence internationale sur la déduction automatique (CADE 2005), et 17ème conférence internationale sur les techniques et applications de la réécriture (RTA 2006).

Langues étrangères : anglais (confirmé), espagnol (moyen), allemand (débutant).

Languages de programmation : C, Pascal, Java, Prolog, Scheme, SQL. Php, ADA95, Maple, outils de vérification de protocoles : Avispa, Proverif.

Exposés et séminaires.

- 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 68NQRT à Rennes à l'IRISA, France, 27 juin 2006. <http://www.irisa.fr/NQRT/>
- École de printemps internationale sur la sécurité à Marseille, France, 25-29 avril 2005.
- Séminaire de l'équipe Information Security de l'ETH Zürich, le 8 Septembre 2006.

- Plusieurs exposés à différents groupes de travail et rencontres de projet : groupe de travail de l'équipe SECurité des Systèmes d'Information (SECSI) au LSV, équipe MOdelisation VERification (LIF Marseille), ACI Sécurité Rossignol à Cachan, à Grenoble et à l'école polytechnique, projet RNTL PROUVé à Nancy.

6 Détails des enseignements dispensés par matière et par année :

En informatique.

J'ai effectué mes enseignements en informatique en tant que : vacataire à l'INSA Toulouse durant l'année scolaire 2002-2003 et moniteur à l'université Paris XII Créteil de 2003 à 2006. Ma tutrice de monitorat est Danièle BEAUQUIER, professeur à l'université Paris XII. Ma première année de monitorat s'est déroulée à l'université Paris XII avec un public de DEUG MIAS 1ère année. Les deux autres années de monitorat ont été effectuées à l'Institut Universitaire Technologique de Fontainebleau avec des étudiants de première et deuxième année. Actuellement j'enseigne en anglais dans le cadre d'un poste d'assistant à l'ETH Zürich pour les cours de « Modelisation et Simulation » et de « Information Security ».

Année 2002-2003 : Vacataire à l'INSA Toulouse. _____

Programmation en ADA95 :

- *Durée* : 20 heures de TP.
- *Public* : 2 groupes de 14 étudiants en première année à l'INSA Toulouse .
- *Responsable* : Gilles MOTET : motet@insa.univ-tlse.fr
- *Description* : Grâce au langage ADA95 les étudiants découvrent les bases de la programmation, à travers les tableaux, les conditions, les itérations, les fonctions et les procédures.
- *Réalisation* : Préparation des sujets d'examen sur machines et corrections des programmes rendus.

Année 2003-2004 : Moniteur à l'université Paris XII Créteil. _____

Initiation à la Programmation en C :

- *Durée* : 32 heures de TD et 32 heures (eq. TD) de TP.
- *Public* : 2 groupes de 40 étudiants en première année de DEUG MIAS.
- *Responsable* : Danièle BEAUQUIER : beauquier@univ-paris12
- *Description* : Ce module a pour but d'apprendre les bases de la programmation à travers le langage C à des étudiants qui n'avaient jamais programmé et étaient sans aucune connaissance en informatique. Les étudiants apprennent les principales notions de la programmation en informatique. En particulier, ils

manipulent les notions de tableaux, itérations (boucles), conditions, chaînes de caractères et pointeurs.

- *Réalisation* : Site Web pour les étudiants avec les sujets et corrigés des Travaux Dirigés et Travaux Pratiques. Aide à la préparation des sujets de Travaux Pratiques, Travaux Dirigés et du sujet d'examen, surveillance d'examen.

Année 2004-2005: Moniteur à l'IUT de Fontainebleau. _____

Bases de Données :

- *Durée* : 32 heures de TD.
- *Public* : 2 groupes de 22 étudiants en première année d'IUT informatique.
- *Responsable* : Régine LALEAU laleau@univ-paris12.fr
- *Description* : Ce module présente les bases de données grâce au langage SQL. Les étudiants abordent les concepts de clé primaire, clé étrangère, jointure naturelle, entité relation, requête, dépendance fonctionnelle, forme normale et normalisation.
- *Réalisation* : participation à l'élaboration des sujets de Travaux Pratiques, de Travaux Dirigés et du sujet d'examen.

Système et Réseaux :

- *Durée* : 32 heures (eq TD) de TP.
- *Public* : 2 groupes de 16 étudiants en seconde année d'IUT informatique.
- *Responsable* : Konstantin VERCHININE : verko@capet.iut-fbleau.fr
- *Description* : Nous introduisons les concepts de système de fichiers, tube de communication, fork, socket. Ces éléments seront ensuite utilisés pour mieux comprendre les notions qui sont liées aux réseaux.
- *Réalisation* : participation à la correction et l'évaluation des partiels sur machine.

Année 2005-2006: Moniteur à l'IUT de Fontainebleau. _____

Base de la programmation en C :

- *Durée* : 32 heures de TD.
- *Public* : 4 groupes de 20 étudiants en première année IUT informatique.

- *Responsables* : Patrick CIEGELSKI et Luc HERNANDEZ.
- *Description* : Comme son nom l'indique, il s'agit d'initier les étudiants à la programmation et à l'algorithmique via le langage C. Ils abordent ainsi les notions de tableaux, fonctions, boucles, conditions, chaînes de caractères et pointeurs.
- *Réalisation* : réalisation de l'ensemble de mes séances de Travaux Dirigés.

Base de données :

- *Durée* : 12 heures de TD.
- *Public* : 2 groupes de 20 étudiants en première année d'IUT informatique.
- *Responsable* : Régine LALEAU : laleau@univ-paris12.fr
- *Description* : Ce module s'adresse à des étudiants de l'IUT en première année ayant déjà abordé lors du premier semestre les systèmes de gestions de bases de données en SQL et Oracle. La dépendance fonctionnelle et la normalisation sont les deux notions que nous étudions avec ces étudiants.
- *Réalisation* : participation à l'élaboration des TDs.

Projet en Mysql & Php :

- *Durée* : 20 heures (eq TD) Projet Mysql & Php.
- *Public* : 2 groupes de 20 étudiants en première année d'IUT informatique.
- *Responsables* : Régine LALEAU et Farida SEMMAK : laleau@univ-paris12.fr
- *Description* : Après avoir appris les bases de la programmation en Php, les étudiants appliquent concrètement les notions de bases de données. Dans le cadre de ce projet, ils ont élaboré un site Web pour la gestion d'un site en ligne d'achat de livre. Cela va de l'analyse du problème jusqu'à la réalisation, sous forme de projet, du site Web.
- *Réalisation* : participation à l'élaboration du sujet, encadrement des projets en TD et TP, et évaluation finale des projets lors de présentations orales avec démonstration du produit fini.

Année 2006-2007: Assistant en anglais à l'ETH Zürich. _____

Modélisation et Simulation :

- *Durée* : 24 heures TD.
- *Public* : 1 groupe de 20 étudiants en troisième année d'université à l'ETH Zürich.
- *Responsable* : Gaston GONNET : gonnet@inf.ethz.ch
- *Description* : Ce module de mathématique propose d'abord une modélisation de différents problèmes concrets, comme la localisation par GPS, la structure de protéines, etc ... Ensuite nous introduisons les outils mathématiques nécessaires à la résolution de ces problèmes, tels la méthode des moindres carrés, les décompositions en vecteurs propres etc... Nous appliquons alors ces méthodes à la résolution pratique des problèmes introduits.
- *Réalisation* : participation à l'élaboration du sujet de TD.

Information Security :

- *Durée* : 24 heures TD.
- *Public* : 1 groupe de 20 étudiants en 4ème année d'université à l'ETH Zürich.
- *Responsable* : David BASIN : basin@inf.ethz.ch
- *Description* : Ce module donne une vue générale des principes et méthodes de sécurité de l'information à travers de nombreuses applications. Nous abordons les notions relatives aux fondements de la cryptographie, aux échanges de clés, à la sécurité des protocoles, aux méthodes de contrôles et de politiques d'accès ainsi qu'aux notions d'anonymat et de confidentialité.
- *Réalisation* : participation à l'élaboration du sujet de TD.

En technique d'apprentissages.

J'ai eu l'occasion d'assister Alain FINKEL lors de ses cours sur les techniques d'apprentissages destinées au public universitaire. J'ai obtenu le Diplôme Universitaire de l'École Normale Supérieure de Cachan : Nouvelles Techniques Cognitives d'Apprentissages (NTCA) en septembre 2006, pour parfaire mes compétences dans ce domaine.

Assistant aux journées apprentissages de Marseille 2005. _____

Représentations mentales et motivation :

- *Durée* : 8 heures de TD.
- *Public* : 2 groupes de 15 moniteurs en deuxième année au C.I.E.S. de Marseille.
- *Responsable* : Alain FINKEL & Yves MATHEY directeur du CIES Provence-Côte d'Azur-Corse. finkel@lsv.ens-cachan.fr
- *Description* : Tout d'abord les moniteurs découvrent et explorent leurs propres représentations mentales. On s'aperçoit ainsi que chacun possède sa propre représentation mentale de notion aussi simple que le point en géométrie. Ensuite les moniteurs apprennent à expliciter une prise de décision anodine. Finalement ils découvrent comment motiver leurs élèves en se servant des techniques de prise de décision, d'explicitation et des notions apprises sur les représentations mentales.
- *Réalisation* : participation à l'élaboration de ces séances.

Année 2005-2006: Assistant en TD à l'IUT d'Orsay. _____

Mémoires et motivation :

- *Durée* : 8 heures de TD.
- *Public* : 4 groupes de 20 étudiants en première année d'IUT informatique à Orsay.
- *Responsable* : Alain FINKEL : finkel@lsv.ens-cachan.fr
- <http://www.lsv.ens-cachan.fr/~finkel/ja2006>
- *Description* : Dans un premier temps les étudiants découvrent comment mémoriser et quelles stratégies mettre en place pour une meilleure mémorisation. Ensuite ils cherchent quel objectif envisager pour leur cursus futur. Nous vérifions avec eux que cet objectif est un "bon" objectif, car avoir un bon objectif aide à être motivé.
- *Réalisation* : participation à l'élaboration de ces séances.

Assistant au journées apprentissages de Cachan, Mai 2006. _____

Émotions et motivation :

- *Durée* : 8 heures de TD.
- *Public* : 2 groupes de 20 enseignants.
- *Responsable* : Alain FINKEL : finkel@lsv.ens-cachan.fr
- *Description* : Dans un premier temps les participants découvrent grâce à une technique d'explicitation quels besoins sont cachés derrière leurs émotions. Ensuite ils apprennent à expliciter une prise de décision anodine. Finalement ils découvrent comment motiver leurs élèves.
- *Réalisation* : participation à l'élaboration de ces séances.

Assistant au journées de formation de l'École Supérieure d'Ostéopathie (ESO), Novembre 2006. _____

Représentations mentales & mémorisation :

- *Durée* : 8 heures de TD.
- *Public* : 1 groupes de 20 ostéopathes en formation.
- *Responsable* : Alain FINKEL : finkel@lsv.ens-cachan.fr
- *Description* : Dans un premier temps les participants découvrent grâce à des exemples leurs propres modes de représentation mentales. Ensuite ils apprennent comment le travail sur ces représentations mentales leur permet de mieux comprendre certains mécanismes d'apprentissages. Lors de la seconde séance, nous proposons d'explorer les différentes facettes de la mémoire et d'acquérir des méthodes de mémorisation. Ensuite nous explorons les émotions et besoins des participants pour renforcer leurs motivations.
- *Réalisation* : participation à l'élaboration de ces séances.

Documents pédagogiques réalisés.

- Site Web sur l'initiation à la programmation.
- Surveillance d'examen en DEUG MIAS 1.

- Aide à la réalisation des contrôles continus, sujet de projet et élaboration des TD et TP en Base de données.
- Grille de correction de copies d'examen des partiels sur machine de système.
- Grille d'évaluation des projets de Php & Mysql
- Réalisation des sujets de TD en base de la programmation en C.
- Réalisation des séances de TD sur la motivation lors des journées apprentissages de Marseille.
- Réalisation des séances de TD sur les émotions lors des journées apprentissages de Cachan.
- Réalisation des séances de TD sur la mémorisation, la définition d'un bon objectif pour des étudiants de l'IUT d'Orsay.

Le site Web pour les étudiants de DEUG première année ainsi que quelques-uns des autres supports pédagogiques réalisés se trouvent à l'adresse suivante :

<http://www.lsv.ens-cachan.fr/~lafourca/enseignement.php>

7 Détails de mes activités de recherche.

Travaux effectués lors du DEA RCFR.

J'ai effectué mon stage de recherche de DEA Représentation de la Connaissance et Formalisation du Raisonnement (RCFR) à l'Institut de Recherche en Informatique de Toulouse (IRIT), dans l'équipe Raisonnements Plausibles, Décision, Méthodes de Preuve (RDPM) sur l'aide à la décision pour la résolution de conflits dans l'ordonnancement de tâches sous la direction de Claudette CAYROL, Hélène FARGIER et Marie-Christine LAGASQUIÉ-SCHIEX. Lorsqu'il n'existe pas de solution à un problème d'ordonnancement, le calcul des conflits, ensembles minimaux de contraintes « incohérents », donne les explications de cet échec. Cette notion de conflits existe aussi en logique propositionnelle (ensembles minimaux de formules inconsistantes). Dans ce travail [6], nous adaptons de nombreux critères de préférences locales issus de la résolution de conflits en logique propositionnelle, à la résolution de conflits dans un problème d'ordonnancement. Nous introduisons également de nouveaux critères « colorés » spécifiques aux problèmes d'ordonnancement. Ce cadre formel d'aide à la décision permet de transformer un problème d'ordonnancement sans solution en un problème d'ordonnancement avec solution, en respectant les préférences locales. Nous spécifions pour tous nos critères des algorithmes de type « Branch-and-Bound » pour la recherche de solutions optimales. L'implémentation de certains critères nous montre que l'ordre de résolution des conflits est crucial et confirme que la résolution de tels conflits est un problème exponentiel.

Travaux effectués pendant ma thèse.

Ces travaux portent sur un tout autre domaine que le travail réalisé en DEA. Dans le cadre de l'ACI Sécurité Rossignol, j'ai obtenu une bourse de thèse entre le Laboratoire Spécification et Vérification de Cachan (LSV) et le Laboratoire d'Informatique Fondamentale de Marseille (LIF), sous la direction de Ralf TREINEN (LSV) et Denis LUGIEZ (LIF). Mon travail de thèse porte sur les méthodes formelles, la sécurité informatique et plus particulièrement sur la vérification des protocoles cryptographiques en présence de propriétés algébriques.

Vérification de protocoles cryptographiques.

De nos jours l'informatique occupe une place importante dans notre quotidien. La démocratisation de l'ordinateur et l'essor d'internet impliquent un changement considérable de nos modes de consommation et de communication. Ainsi nous pouvons gérer nos comptes bancaires, acheter un billet d'avion, payer nos impôts depuis notre ordinateur relié à internet ou directement sur notre téléphone mobile. Ces transactions utilisent des protocoles de communications complexes qui transmettent des données confidentielles. Toutes ces applications nécessitent des garanties de sécurité élevées,

portant sur les propriétés de secret, d'authenticité des participants, mais aussi de nombreuses autres propriétés parmi lesquelles l'anonymat (des votants lors d'élections), l'équité (pour les signataires d'un contrat), la non-révocation (des commandes pour un commerçant) etc ... Les concepteurs de ces protocoles de communication utilisent des primitives cryptographiques pour sécuriser les échanges de messages entre les différents participants. Depuis les années 1980, les progrès en matière de cryptographie nous assurent l'existence d'algorithmes de chiffrement suffisamment sûrs. Mais même en supposant que les algorithmes utilisés, typiquement le chiffrement, les fonctions à sens unique ou les générateurs aléatoires sont parfaits i.e. inviolables, la plupart des protocoles publiés comportent des failles. Comme le montre le fameux protocole de Needham-Schroeder [NS78] considéré comme sûr jusqu'à ce qu'une attaque « logique » fut découverte 15 ans après sa publication par G. Lowe [Low95]. Une attaque logique consiste à jouer le protocole de différentes manières pour en extraire des informations supposées secrètes, par opposition à une attaque par cryptanalyse qui va chercher à déchiffrer les messages cryptés échangés par les participants. Depuis la découverte de cette faille, la vérification formelle de protocoles cryptographiques a pris une importance considérable dans le domaine de la sécurité informatique.

Formalisation des protocoles cryptographiques : le modèle de Dolev-Yao.

En 1983, Dolev et Yao [DY83] proposent une des premières formalisation des protocoles cryptographiques, utilisée par de nombreux auteurs comme base à de nombreuses méthodes de vérification de protocoles cryptographiques [Mea96, Pau97, Mon99, GK00, GL00, Bla01, AC02, CKR⁺03, BEL04, CRZ05]. Dolev et Yao supposent dans leur modèle « l'hypothèse de chiffrement parfait » : le seul moyen d'obtenir le contenu d'un message chiffré est de connaître la clef de déchiffrement. Ils abstraient également le réseau de communication entre deux participants en supposant que les messages sont échangés instantanément entre les différents participants via un réseaux idéalisé peu importe le type de connexion utilisée (câble, fibre optique, ondes radio, ...). Dans ce modèle, les messages envoyés et reçus ne sont pas des nombres, ni des suites de bits, ni des signaux électriques, mais des éléments d'une algèbre de termes, éventuellement modulo une théorie équationnelle. Cette approche considère aussi le cas le plus pessimiste et modélise un intrus omniprésent, i.e. l'intrus contrôle le réseau et peut donc intercepter, bloquer, modifier les messages échangés sur le réseau, et aussi jouer des sessions du protocole avec les autres participants. Les capacités de cet intrus de Dolev-Yao sont modélisées par une système de déduction ce qui lui permet par exemple de déchiffrer un message s'il en connaît la clef de déchiffrement.

En utilisant cette modélisation, dans laquelle il est facile de représenter une ou plusieurs exécutions du protocole, il a été prouvé [DLMS99, CKR⁺03] que si le nombre de sessions est non-borné alors le problème de secret i.e., savoir si une donnée d secrète entre deux participants peut être découverte par un intrus, est un problème indécidable.

Mes travaux.

En considérant le modèle de Dolev-Yao pour un nombre borné de sessions, je me suis intéressé à l'affaiblissement de l'hypothèse de chiffrement parfait pour la propriété de secret. L'hypothèse de chiffrement parfait signifie que les primitives de chiffrements sont considérées comme des « boîtes noires » et qu'il est impossible de retrouver le message original contenu dans le message crypté sans posséder la clef de déchiffrement. Remarquons d'abord que les algorithmes de chiffrements sont construits à partir de fonctions mathématiques qui possèdent certaines propriétés algébriques et que les protocoles eux-mêmes utilisent certaines propriétés algébriques. Pour analyser de manière plus réaliste les protocoles, il est important de prendre en compte les propriétés algébriques lors de la vérification, car il est possible qu'un intrus utilise ces propriétés algébriques pour obtenir une information secrète. J'ai donc cherché au cours de ma thèse à affaiblir l'hypothèse du chiffrement parfait en prenant en compte les propriétés algébriques de certaines théories équationnelles.

Les propriétés algébriques : J'ai dans un premier temps répertorié et classé les protocoles utilisant dans leurs spécifications une propriété algébrique soit dans les méthodes de chiffrement utilisées soit de part leur conception même. J'ai cherché à présenter, chaque fois que cela était possible, une attaque sur le protocole utilisant ces propriétés algébriques. Ce premier travail [12] en collaboration avec V. Cortier et S. Delaune dans le cadre du projet RNTL Prouvé a donné lieu à une première publication [2] dans la revue internationale « Journal of Computer Security ». Dans cette étude, nous présentons l'ensemble des propriétés algébriques utilisées par les protocoles cryptographiques actuels et l'ensemble des résultats de vérification existants pour ces propriétés algébriques.

Suite à cette étude, j'ai focalisé mon attention sur les propriétés algébriques dites « d'homomorphismes » ($h(a + b) = h(a) + h(b)$) non encore vérifiées formellement. Cette propriété d'homomorphisme permet, comme l'a montré G.J. Simmons [Sim94], à un intrus de découvrir de l'information confidentielle sur le protocole TMN [TMN89] d'échange de clef via un serveur.

J'ai d'abord étendu le modèle de l'intrus de Dolev-Yao pour prendre en compte lors de la vérification de protocoles cryptographiques des propriétés algébriques pertinentes. Dans le cadre du projet RNTL Prouvé [11] nous avons également dégagé à partir d'un modèle étendu de l'intrus des conditions suffisantes pour la vérification automatique. Je me suis alors fixé sur l'intrus « passif » pour cette propriété d'homomorphisme. L'intrus passif est la première étape de la vérification des protocoles cryptographiques, un tel intrus écoute juste les messages échangés sur le réseau. Il cherche ensuite à en déduire de l'information confidentielle grâce à ces capacités. Ensuite je me suis intéressé à l'intrus « actif » qui en plus d'écouter tous les messages du réseau comme son homologue passif, peut intercepter, modifier, bloquer des messages et jouer des sessions du protocole avec les autres participants.

L'intrus passif :

Dans le cadre d'un intrus passif en collaboration avec mes directeurs de thèse, j'ai élaboré un premier ensemble de résultats de décidabilité pour la propriété de secret en présence d'un opérateur homomorphique (h) sur un opérateur associatif et commutatif (ACH), ou sur l'opérateur du *ou-exclusif* ($ACUNh$) ou sur l'opérateur des groupes abéliens (AGh). Ces résultats sont basés sur une extension du résultat de localité de Mac Allester [McA93] et des techniques de normalisation d'arbres de preuves développées dans le système déductif de Dolev-Yao étendu par une théorie équationnelle. J'ai présenté ce travail [4] lors de la conférence internationale RTA 2005. Par la suite la complexité de ce résultat a été améliorée par S. Delaune [Del06a].

Nous avons ensuite résolu le cas d'un chiffrement distributif ($\{a + b\}_k = \{a\}_k + \{b\}_k$, où $\{m\}_k$ dénote le chiffrement du message m par la clef k). Dans ce cas, nous avons autant de symboles homomorphiques que de clefs possibles, ce qui nous empêche d'utiliser la technique proposée précédemment. Nous avons donc construit une nouvelle procédure dans un premier temps pour un chiffrement distributif sur l'opérateur sur *ou-exclusif* ($ACUN$) [8] et ensuite sur l'opérateur des groupes abéliens (AG). L'ensemble de ces résultats ont été accepté dans la revue internationale « Information and Computation » [1].

Enfin j'ai considéré le cas d'un chiffrement distributif et commutatif ($\{\{m\}_{k1}\}_{k2} = \{\{m\}_{k2}\}_{k1}$) pour l'opérateur du *ou-exclusif* ($ACUN$). Cette nouvelle théorie équationnelle, dénotée par $ACUN\{.\}$. Commutatif, demande une étude plus minutieuse des arbres de preuves et de nouvelles caractérisations pour obtenir une normalisation de preuves adéquates. J'ai présenté ce travail lors du Workshop International Secret 2006 [10], une version longue de ce résultat est en cours de soumission pour une revue internationale. Dans mon manuscrit de thèse [5], j'étends ce résultat au groupe abélien. J'ai également proposé, dans un chapitre de ma thèse, des exemples de théories équationnelles qui montrent que dans le cas d'un intrus passif la décidabilité du problème de secret et celle du problème d'unification ne sont pas liées, contrairement au cas de l'intrus actif, où l'indécidabilité du problème d'unification implique l'indécidabilité du problème de secret.

L'intrus actif : En collaboration avec mes directeurs de thèse et S. Delaune, nous avons résolu pour un nombre borné de sessions le problème du secret pour la théorie équationnelle $ACUNh$ constituée d'un opérateur homomorphique (h) qui distribue sur l'opérateur du *ou-exclusif* ($ACUN$). J'ai présenté ce travail à la conférence internationale ICALP 2006 [3]. Lors de cette étude nous avons suivi l'approche de J. Millen et V. Shmatikov [MS01, MS03], dans laquelle ils modélisent les protocoles par des systèmes de contraintes *bien définis*. Nous avons proposé une nouvelle caractérisation algébrique des systèmes de contraintes bien définis, et un algorithme d'unification complet pour cette théorie équationnelle [7]. Ceci nous a permis de transformer les systèmes de contraintes bien définis en systèmes d'équations diophantiennes quadra-

tiques. Grâce à cette nouvelle caractérisation, nous avons pu développer une méthode de résolution de ces systèmes d'équations quadratiques particuliers, ce qui est dans le cas général un problème indécidable.

Bilan : Je résume dans la figure 2 les principaux résultats obtenus lors de mon doctorat sur la vérification de protocoles cryptographiques en présence de théories équationnelles.

	Complexité	
	Intrus passif	Intrus actif
ACUN_h	<i>P-TIME</i> [4],[Del06a]	<i>Décidable</i> [3]
AG_h	<i>P-TIME</i> [4],[Del06a]	<i>Indécidable</i> [Del06b]
ACUN{.}. & AG{.}.	<i>EXP-TIME</i> [1]	?
ACUN{.}. & AG{.}. Commutatif	<i>2EXP-TIME</i> [10, 5]	?

Figure 2: Récapitulatif des résultats obtenus durant ma thèse.

Travaux effectués après ma thèse.

La Direction Générale de l'Armement (DGA) a retenu mon dossier pour une bourse post-doctorale d'un an à l'ETH Zürich dans l'équipe de David Basin. Mon séjour en Suisse va me permettre d'élargir mes connaissances en vérification formelle de protocoles cryptographiques et de commencer de nouvelles collaborations sur de nouveaux sujets. Je présente maintenant les travaux commencés à Zürich.

Généralisation : Suite à notre publication à la conférence ICALP 2006, nous avons dégagé les critères nécessaires à notre procédure pour la théorie de l'homomorphisme et du *ou-exclusif* et avons étendu notre résultat de décidabilité pour un nombre borné

de sessions à l'ensemble des théories monoïdales. Ce travail [9] est soumis à une revue internationale.

Réseaux sans fil : Dans le cadre du projet VerSePro (Provably Secure Protocols for Wireless Networks) entre l'EPFL et l'ETHZ, je m'intéresse à une modélisation des réseaux sans fil afin de pouvoir vérifier formellement les protocoles développés dans ce domaine en plein essor, depuis les dernières années.

Projet de Recherche.

Si j'ai la possibilité de poursuivre ma carrière dans la recherche, je prévois de continuer mes travaux comme suit :

Prolongement de la thèse : J'envisage de résoudre les problèmes laissés ouverts à la suite de mes travaux de thèse comme le montre la figure 2. Je souhaite regarder le cas d'un intrus actif en présence d'une méthode de chiffrement commutative et distributive sur l'opérateur du *ou-exclusif* dans un premier temps et ensuite le cas de l'opérateur des groupes abéliens.

Les Webs Services : Je pense aussi m'intéresser aux nouvelles propriétés algébriques ou non qui se dégagent des interactions des différents acteurs des applications sécurisées sur internet (Webs Services). Les Webs Services ajoutent un côté dynamique et compositionnel par rapport aux protocoles cryptographiques classiques. Essayer de formaliser et vérifier ces nouvelles technologies me semble être un challenge intéressant et important de la sécurité informatique.

Autres types de protocoles cryptographiques : J'aimerais aussi commencer à vérifier formellement des propriétés comme l'anonymat, l'équité et également aux protocoles de groupes et de vote électronique. Ceci en m'appuyant sur mes travaux passés, car ces protocoles utilisent souvent des propriétés algébriques pour garantir certaines propriétés.

Références.

- [AC02] R. Amadio and W. Charatonik. On name generation and set-based analysis in the Dolev-Yao model. In *Proc. International Conference on Concurrency Theory (CONCUR'02)*, volume 2421 of *Lecture Notes in Computer Science*, pages 499–514, Brno, Czech Republic, 2002. Springer-Verlag.
- [BEL04] L. Bozga, C. Ene, and Y. Lakhnech. A symbolic decision procedure for cryptographic protocols with time stamps. In *Proc. 15th Interna-*

- tional Conference on Concurrency Theory (CONCUR'04)*, Lecture Notes in Computer Science, London, England, 2004. Springer-Verlag. To appear.
- [Bla01] B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *Proc. 14th Computer Security Foundations Workshop (CSFW'01)*, pages 82–96, Cape Breton, Canada, 2001. IEEE Computer Society Press.
- [CKR⁺03] Y. Chevalier, R. Küsters, M. Rusinowitch, M. Turuani, and L. Vigneron. Extending the Dolev-Yao intruder for analyzing an unbounded number of sessions. In *Proc. 17th International Workshop in Computer Science Logic (CSL'03)*, volume 2803 of *Lecture Notes in Computer Science*, pages 128–141, Vienna, Austria, 2003. Springer-Verlag.
- [CRZ05] V. Cortier, M. Rusinowitch, and E. Zalinescu. A resolution strategy for verifying cryptographic protocols with cbc encryption and blind signatures. In *PPDP*, pages 12–22, 2005.
- [Del06a] S. Delaune. Easy intruder deduction problems with homomorphisms. *Information Processing Letters*, 97(6):213–218, 2006.
- [Del06b] S. Delaune. An undecidability result for AGh. Research Report LSV-06-02, Laboratoire Spécification et Vérification, ENS Cachan, France, February 2006. 9 pages.
- [DLLT06] S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis in presence of a homomorphism operator and *exclusive or*. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06)*, Lecture Notes in Computer Science, pages 132–143, Venice, Italy, jul 2006. Springer-Verlag.
- [DLMS99] N. Durgin, P. Lincoln, J. Mitchell, and A. Scedrov. Undecidability of bounded security protocols. In *Proc. Workshop on Formal Methods and Security Protocols (FMSP'99)*, Trento, Italy, 1999.
- [DY83] D. Dolev and A. Yao. On the security of public-key protocols. In *Transactions on Information Theory*, volume 29, pages 198–208. IEEE Computer Society Press, March 1983.
- [GK00] T. Genet and F. Klay. Rewriting for cryptographic protocol verification (extended version). In *Proc. of the 17th International Conference on Automated Deduction (CAD'00)*, volume 1831 of *Lecture Notes in Artificial Intelligence*. Springer Verlag, January 2000.
- [GL00] J. Goubault-Larrecq. A method for automatic cryptographic protocol verification. In *Proc. of the 15th International Parallel and Distributed Processing Symposium, IPDPS 2000*, volume 1800 of *Lecture Notes in Computer Science*, pages 977–984, Cancun, Mexico, May 2000. Springer Verlag.

- [Low95] G. Lowe. An attack on the Needham-Schroeder public key authentication protocol. *Information Processing Letters*, 56(3):131–133, November 1995.
- [McA93] D. A. McAllester. Automatic recognition of tractability in inference relations. *Journal of the ACM*, 40(2):284–303, April 1993.
- [Mea96] C. Meadows. Language generation and verification in the NRL protocol analyzer. In *Proc. 9th Computer Security Foundation Workshop (CSFW'96)*, pages 48–62, Kenmare, Ireland, 1996. IEEE Computer Society Press.
- [Mon99] D. Monniaux. Abstracting cryptographic protocols with tree automata. In *Sixth International Static Analysis Symposium (SAS'99)*, number 1694 in Lecture Notes in Computer Science, pages 149–163. Springer Verlag, 1999.
- [MS01] J. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In *Proc. 8th ACM Conference on Computer and Communications Security (CCS'01)*. ACM Press, 2001.
- [MS03] J. Millen and V. Shmatikov. Symbolic protocol analysis with products and Diffie-Hellman exponentiation. In *Proc. 16th Computer Security Foundation Workshop (CSFW'03)*, pages 47–62, Pacific Grove, California, USA, 2003. IEEE Computer Society Press.
- [NS78] R. Needham and M. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.
- [Pau97] L. Paulson. Mechanized proofs for a recursive authentication protocol. In *Proc. 10th Computer Security Foundations Workshop (CSFW'97)*, pages 84–95, Rockport, Massachusetts, USA, 1997. IEEE Computer Society Press.
- [Sim94] G. Simmons. Cryptoanalysis and protocol failures. *Communications of the ACM*, 37(11):56–65, 1994.
- [TMN89] M. Tatebayashi, N. Matsuzaki, and D. B. Newman. Key distribution protocol for digital mobile communication systems. In *Proc. 9th Annual International Cryptology Conference (CRYPTO'89)*, volume 435 of *Lecture Notes in Computer Science*, pages 324–333, Santa Barbara, California, USA, 1989. Springer-Verlag.

8 Listes des pièces jointes.

Photocopie de la carte d'identité.

Thèse de doctorat :

- Copie de l'attestation de délivrance de doctorat.
- Copies des deux rapports de pré-soutenance (Lucas VIGANÒ et Yassine LAKHNECH).
- Copie du rapport de soutenance.
- Manuscrit de thèse.

Enseignements :

- Copie de l'attestation de monitorat du C.I.E.S. de Jussieu.
- Lettre de recommandation de ma tutrice de monitorat (Danièle BEAUQUIER).
- Lettre de recommandation de ma responsable d'enseignement à l'IUT (Régine LALEAU).

Recherche :

- Lettre de recommandation de mes directeurs de thèse (Denis LUGIEZ et Ralf TREINEN).
- Attestation de post-doc (David BASIN).

Publications jointes :

- [1] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of abelian groups with distributive encryption. *Information and Computation*, 2006. To appear. 51 pages.
- [2] V. Cortier, S. Delaune, and P. Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.
- [3] S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis in presence of a homomorphism operator and *exclusive or*. In M. Buglesi, B. Preneel, V. Sassone, and I. 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 132–141, Venice, Italy, July 2006. Springer.