DOSSIER DE CANDIDATURE

AUX FONCTIONS DE MAÎTRE DE CONFÉRENCES

SECTION : 27

NUMÉRO : 0595

ETABLISSEMENT : UNIVERSITÉ GRENOBLE I

Pascal Lafourcade

Table des matières

1 Curriculum Vitae. 2
Identité. . . . 2
Fonctions occupées. . . . 2
Diplômes. . . . 2
Compétences. . . . 2

2 Activités d'enseignement. 3
Assistant à l'ETH Zürich. . . . 3
Moniteur au CIES de Jussieu, Université Paris XII. . . . 3
Autres activités d'enseignement. . . . 3
Projet d'enseignement. . . . 3
En informatique. . . . 4
En technique d'apprentissage. . . . 6
Documents pédagogiques réalisés. . . . 7

3 Activités administratives. 8

4 Activités de recherche. 9

5 Programme de recherche détaillé. 16

6 Listes des pièces jointes. 22

1 Curriculum Vitae.

Identité.

Nom : LAFOURCADE

Prénom : Pascal

Né le : 26 Avril 1977 à Toulouse (31)

Nationalité : Française

État civil : Célibataire

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
Portable : +41 78 878 83 54
Fax : +41 44 632 11 72

Fonctions occupées.

Oct 2006 - : Boursier DGA/CNRS, post-doctorant à l'ETH Zürich, dans l'équipe Information Security de D. BASIN.

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 de Cachan (LSV, 2 ans) et au Laboratoire d'Informatique Fondamentale de Marseille (LIF, 1 an), dans le cadre de l'ACI Sécurité Rossignol.

Sept 2001 - Août 2003 : Emploi jeune au sein du Basket Labège Auzeville Club (temps plein en parallèle du cursus universitaire).

Diplômes.

Doctorat de l'École Normale Supérieure de Cachan : Débuté le 1er Octobre 2003, soutenu le 25 Septembre 2006 à Cachan, 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, Professeur à l'Université Joseph Fourier (Grenoble).

Examinateur 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'Apprentissage) 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. 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 LAGASQUIE-SCHIEX, mention *Assez-Bien*.

2002 : **Maîtrise** d'informatique, mention *Bien* (option : analyse d'images et intelligence artificielle).

2001 : **Maîtrise** de mathématiques fondamentales (mémoire sur la théorie des nœuds).
Licence d'informatique, mention *Bien*.

1999 : **Licence** de mathématiques fondamentales.

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

1995 : Baccalauréat Scientifique, spécialité mathématiques, mention *Assez-Bien*.

Compétences.

Langues : Français langue maternelle, anglais courant, espagnol scolaire et allemand débutant.

Langages de programmation : C, Pascal, Java, Prolog, Scheme, SQL, PHP, HTML, ADA95, Maple.

Outils de vérification de protocoles : Cl-Atse, OFMC, TA4SP, SATMC, Proverif, Scyther, Hermes, Coprove.

Divers : Joueur et entraîneur de basket-ball, pilote de montgolfière, danseur (salsa, rock,...).

2 Activités d'enseignement.

Je présente ici une vue synthétique des enseignements effectués et mon projet d'enseignement. Dans la suite de cette section,je détaille le contenu de chaque enseignement par matière et par année.

Assistant à l'ETH Zürich.

J'enseigne dans les cours suivants en anglais :
– « Information & Security » du professeur David BASIN (24h de TD)
– « Modeling & Simulation » du professeur Gaston GONNET (24h de TD)

Moniteur au CIES de Jussieu, Université Paris XII.

Tutrice de monitorat : Danièle BEAUQUIER, LACL, Université Paris XII.
Période : Années universitaires 2003-2006.
Durée : 3×64h = 192h équivalent TD.

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

Public	Intitulé	Nature	Eq TD
1ère Année DEUG	Initiation à la Programmation en C	TD/TP	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 & Réseau	TP	32h
		Total	192h

Autres activités d'enseignement.

Assistant en techniques d'apprentissage :
– 8h TD, en 2ème Année à l'IUT d'Orsay 2006 : *Motivation et mémorisation*.
– 8h TD, pour les moniteurs des C.I.E.S. Jussieu, Versailles et Sorbonne : *Émotions et motivation*, lors des Journées Apprentissage de Cachan 2006.
– 8h TD, pour les moniteurs des C.I.E.S. de Marseille : *Représentations mentales et motivation*, lors des Journées Apprentissage de Marseille 2006.
– 8h TD, en 1ère année de l'ESO : *Représentations mentales, mémorisation, émotions et motivations* 2006.

Vacations : 20h de TP, en 1ère Année à l'INSA Toulouse : 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).

Projet d'enseignement.

Mes expériences d'enseignement m'ont permis d'aborder de nombreux sujets : sécurité informatique, modélisation et simulation, initiation à la programmation, système et réseau, bases de données. Lors de ces expériences, je me suis intégré dans plusieurs équipes pédagogiques, et j'ai pu découvrir différents fonctionnements et méthodes d'enseignement. Fort de ces expériences, j'aimerais enseigner les matières suivantes, réparties en trois catégories :

- D'une part, je suis attaché aux domaines proches de mes thèmes de recherche que sont la sécurité informatique et la vérification formelle. Actuellement, à l'ETH Zürich, j'enseigne avec grand plaisir dans le module "Information Security" à des étudiants de troisième année. Je suis prêt à m'investir dans l'élaboration d'enseignements sur des sujets connexes à mon domaine de recherche pour des étudiants de L3 ou de Master.

- D'autre part, j'ai particulièrement apprécié enseigner à un public de « non informaticiens » et leur apprendre les bases d'un langage de programmation, le fonctionnement du système et du réseau, ou encore les bases de données. Cela m'a permis de me confronter aux problèmes qu'ils rencontrent et ce défi pédagogique me passionne. Je suis donc prêt à enseigner l'ensemble des bases de l'informatique à des étudiants débutants en première année.
- Finalement, fort de mes expériences d'enseignement et de mes différentes interventions en techniques d'apprentissage, j'aimerais à plus long terme élaborer 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'apprentissage (mémorisation, motivation...) en me basant sur les progrès scientifiques des neuro-sciences de ces dernières années.

Néanmoins, je suis ouvert à toutes autres propositions d'enseignement, car fort de mes diverses expériences à différents niveaux : vacations, monitorat, assistanat, j'ai appris à enseigner de nombreuses matières. Je reste donc prêt à m'adapter aux besoins d'enseignement de mon futur établissement.

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 était Danièle BEAUQUIER, professeur à l'université Paris XII. Comme le spécifiè mon contrat de moniteur, ma première année s'est déroulée à l'université de Créteil Paris XII avec un public de DEUG MIAS 1ère année et les deux autres années 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 « Modeling & 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 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 TD et TP. Aide à la préparation des sujets de TP, TD 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 TP, de TD 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 sont ensuite utilisés pour mieux comprendre les notions de réseau.
- *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 des séances de TD.

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 et en base de données, les étudiants appliquent concrètement ces notions en réalisant un projet. Dans le cadre de ce projet, ils ont conçu et développé un site pour la gestion d'achat de livres en ligne. Cela va de l'analyse du problème jusqu'à la réalisation, sous forme de projet, du site.
- *Réalisation* : participation à l'élaboration du sujet du projet, 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.

Modeling & 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 d'informatique et mathématiques 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 efficace de ces problèmes, telles les méthodes des moindres carrés, de décomposition en vecteurs propres etc... Nous appliquons alors ces méthodes à la résolution aux problèmes introduits.
- *Réalisation* : participation à l'élaboration des sujet de TD et TP, surveillance d'examen et correction des copies.

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 clefs, 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 des sujets de TD, TP, et coordination des assistants.

En technique d'apprentissage.

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

Assistant aux journées apprentissage 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 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 des séances de TD.

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 des séances de TD.

Assistant aux journées apprentissage 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 des séances de TD.

Assistant aux journées de formation de l'École Supérieure d'Ostéopathie, Novembre 2006.

Représentations mentales & mémorisation :

- *Durée* : 8 heures de TD.
- *Public* : 1 groupe 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 représentations mentales. Ensuite ils apprennent comment le travail sur ces représentations mentales leur permet de mieux comprendre certains mécanismes d'apprentissage. 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 des séances de TD.

Documents pédagogiques réalisés.

- Réalisation des sujets de TD et TP du module "Information & Security" à l'ETH Zürich.
- Réalisation des TD, élaboration de l'examen du module "Modeling & Simulation" à l'ETH Zürich.
- 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 apprentissage de Marseille.
- Réalisation des séances de TD sur les émotions lors des journées apprentissage 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`

3 Activités administratives.

Organisation de colloques.

- Participation au comité d'organisation de la conférence internationale FORMATS 2006 à Paris du 25 au 28 Septembre 2006, 80 participants (Webmaster du site d'inscription).
  `http://www.lsv.ens-cachan.fr/formats06/`
- Participation au comité d'organisation des Journées Apprentissage 2006 à Paris du 17 au 19 Mai 2006. Journées destinées aux moniteurs et enseignants, avec une centaine de participants (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 vingtaine d'intervenants extérieurs (industriels, universitaires, anciens doctorants, chasseurs de têtes ...).

Charges administratives.

- Membre de l'équipe SOS, mailing liste d'aide pour les utilisateurs de Linux au Laboratoire Spécification et Vérification (LSV).
- Membre de l'équipe INSTSOFT, groupe d'installation du 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. Et responsable des pages web internes d'aide pour l'utilisation du graveur et du scanner.

Évaluation d'articles.

- *Information and Computation*, revue internationale.
- 34th International Colloquium on Automata, Languages and Programming (*ICALP 2007*).
- 16th International Conference on Rewriting Techniques and Applications (*RTA 2006*).
- 20th International Conference on Automated Deduction (*CADE 2005*).

4 Activités de recherche.

Je présente une vue synthétique de mes travaux de recherche et 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. Je présente enfin mon projet de recherche dans la section 5.

Travaux effectués lors du DEA RCFR, à l'IRIT Toulouse.

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, Décisions, Méthodes de Preuve (RPDMP). Mon travail portait 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 LAGASQUIE-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 [10], 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 qui a une complexité en temps exponentielle.

Travaux effectués pendant ma thèse, à l'ENS de Cachan.

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 de protocoles cryptographiques en présence de propriétés algébriques.

Vérification de protocoles cryptographiques.

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 communication complexes qui transmettent des données confidentielles. Toutes ces applications nécessitent des garanties de sécurité élevées, portant à la fois sur les propriétés de secret et 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 soient parfaits, i.e. inviolables, la plupart des protocoles publiés comportent des failles, comme le montre le fameux protocole de Needham-Schroeder [NS78] considéré sûr jusqu'à ce qu'une attaque « logique » fut découverte par G. Lowe [Low95] 15 ans après la publication du protocole. 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 formalisations des protocoles cryptographiques, utilisée depuis 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 réseau idéalisé quel que soit le type de connexion utilisé. 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 en modélisant un intrus omniprésent, i.e. un intrus qui 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 sont modélisées par un système de déduction, lui permettant par exemple de déchiffrer un message s'il en connaît la clef de déchiffrement.

Cette modélisation permet de représenter facilement une ou plusieurs exécutions du protocole. Grâce à ce modèle, 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 secrète entre deux participants peut être découverte par un intrus, est un problème indécidable. Se restreindre à un nombre borné de sessions rend le problème décidable [RT01].

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. Remarquons d'abord que les algorithmes de chiffrement sont construits à partir de fonctions mathématiques qui possèdent certaines propriétés algébriques. Notons également que les protocoles eux-mêmes sont souvent construits à partir de certaines propriétés algébriques. Pour analyser de manière plus réaliste les protocoles, il est donc important de prendre en compte les propriétés algébriques lors de la vérification. En effet, il est possible qu'un intrus utilise ces propriétés 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 certains opérateurs cryptographiques.

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 leurs conceptions même. J'ai cherché à présenter, chaque fois que possible, une attaque sur le protocole utilisant ces propriétés algébriques. Ce premier travail [15] dans le cadre du projet RNTL Prouvé a donné lieu à une 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.

Suite à cette étude, j'ai porté mon attention sur les propriétés algébriques dites « d'homomorphismes » jusqu'alors vérifiées formellement. Ces propriétés sont représentées par la théorie équationnelle suivante $h(a+b) = h(a) + h(b)$. 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 d'échange de clef TMN [TMN89].

J'ai d'abord étendu le modèle de l'intrus de Dolev-Yao pour prendre en compte des propriétés algébriques pertinentes lors de la vérification de protocoles cryptographiques. Dans le cadre du projet RNTL Prouvé [14], nous avons également dégagé à partir d'un modèle étendu de l'intrus des conditions suffisantes pour la vérification automatique. Je me suis d'abord concentré 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 uniquement les messages échangés sur le réseau et cherche 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 d'autres participants.

L'intrus passif : Dans le cadre d'un intrus passif, 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), 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 lors de la conférence internationale RTA 2005 [5].

Nous avons ensuite résolu le cas d'un chiffrement distributif, représenté par la théorie équationnelle $\{a+b\}_k = \{a\}_k + \{b\}_k$, 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 rend la tâche plus complexe. 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) [6]. L'ensemble de ces résultats a été accepté pour publication dans la revue internationale « Information and Computation » [1].

Enfin j'ai considéré le cas d'un chiffrement distributif et commutatif pour l'opérateur du *ou-exclusif* ($ACUN$) ce qui consiste à enrichir le modèle de l'équation $\{\{m\}_{k1}\}_{k2} = \{\{m\}_{k2}\}_{k1}$. 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 adéquate. J'ai présenté ce travail lors du workshop international SecRet 2006. Une version longue de ce résultat a été accepté pour publication dans la revue électronique ENTCS [3]. Dans mon manuscrit de thèse [6], j'étends ce résultat au groupe abélien. J'ai également proposé, dans un chapitre de ma thèse, des exemples de théories équationnelles montrant que dans le cas d'un intrus passif la décidabilité du problème de secret et celle du problème d'unification sont indépendants, contrairement au cas de l'intrus actif, où l'indécidabilité du problème d'unification implique l'indécidabilité du problème de secret.

L'intrus actif : J'ai résolu pour un nombre borné de sessions le problème du secret pour la théorie équationnelle $ACUNh$ constituée d'un opérateur homomorphique (h) distributif par rapport à l'opérateur du *ou-exclusif* ($ACUN$). J'ai présenté ce travail à la conférence internationale ICALP 2006 [4]. Lors de cette étude nous avons suivi l'approche de J. Millen et V. Shmatikov [MS01, MS03] qui modélisent les protocoles par des systèmes de contraintes *bien définis*. Nous avons proposé une nouvelle caractérisation algébrique des systèmes de contraintes bien définis. Cela nous a permis de transformer les systèmes de contraintes bien définis en systèmes d'équations diophantiennes quadratiques. Grâce à cette nouvelle caractérisation, nous avons pu développer une méthode de résolution de ces systèmes d'équations quadratiques particuliers, problème indécidable en général. Par la suite nous avons étendu ce travail difficile et complexe à d'autres théories équationnelles [11] .Ce travail nous a aussi amené à développer un algorithme d'unification complet pour cette théorie équationnelle [7].

Bilan : Dans le tableau suivant, je résume les principaux résultats obtenus lors de mon doctorat sur la vérification de protocoles cryptographiques en présence de théories équationnelles.

	Complexité	
	Intrus passif	**Intrus actif**
ACUNh	*P-TIME* [5],[Del06a]	*Décidable* [4]
AGh	*P*-TIME [5],[Del06a]	*Indécidable* [Del06b]
ACUN$\{.\}_.$ **& AG**$\{.\}_.$	*E*XP-TIME [1]	*?*
ACUN$\{.\}_.$ **& AG**$\{.\}_.$ **Commutatif**	*2*EXP-TIME [3, 6]	*?*

Travaux effectués aprés ma thèse, à l'ETH Zürich.

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 « Information and Security » de David Basin. Mon post-doctorat en Suisse me permet d'élargir mes connaissances en vérification formelle de protocoles cryptographiques et de commencer de nouvelles collaborations sur d'autres sujets. Je présente ici les travaux que j'ai commencés à Zürich depuis le 1^{er} Octobre 2006.

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 est en cours de soumission à une revue internationale [11].

J'ai commencé une collaboration avec Yannick Chevalier (IRIT, Toulouse) pour résoudre les problèmes laissés ouverts à la suite de mes travaux de thèse présentés dans le tableau récapitulatif ci-dessus. Cette collaboration porte plus précisement sur 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.

De plus, dans le cadre du projet VerSePro (Provably Secure Protocols for Wireless Networks) entre l'EPFL et l'ETH Zürich, je m'intéresse à une modélisation des réseaux sans fil afin de pouvoir vérifier formellement les protocoles développés dans ce domaine en plein essor, ces dernières années. J'ai également commencé une collaboration avec Ralf Kuesters dans l'équipe « Foundations of Computer and Network Security » sur la vérificaion formelle des protocoles de groupe.

Enfin, j'ai commencé une collaboration avec Bogdan Księżopolski, Université de Lublin Pologne, sur la vérification de protocoles de vente aux enchères électroniques. Ce travail [12], nous a permis, grâce à la modélisation dans l'outil OFMC [BMV05], de trouver une faille sur un protocole de vente aux enchères. Nous proposons aussi une nouvelle version corrigée et vérifiée par cet outil de ce protocole.

Liste de publications.

L'ensemble de mes publications est disponible électroniquement à l'adresse suivante :

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

Revues internationales

— 2007 —

[1] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of abelian groups with distributive encryption. *Information and Computation*, 205(4) :581–623, Apr. 2007.

— 2006 —

[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.

Revue internationale électronique

— 2007 —

[3] P. Lafourcade. Intruder deduction for the equational theory of *exclusive-or* with commutative and distributive encryption. In M. Fernández and C. Kirchner, editors, *Selected Papers from the 1st International Workshop on Security and Rewriting Techniques (SecReT'06)*, Electronic Notes in Theoretical Computer Science, Venice, Italy, 2007. Elsevier Science Publishers. To appear.

Conférences internationales

— 2006 —

[4] 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 132–143, Venice, Italy, July 2006. Springer.

— 2005 —

[5] 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.

Thèse

— 2006 —

[6] 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.

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.

— 2004 —

[9] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for AC-like equational theories with homomorphisms. Research Report LSV-04-16, Laboratoire Spécification et Vérification, ENS Cachan, France, Nov. 2004. 69 pages.

— 2003 —

[10] 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 Fomalisation du Raisonnement, Toulouse, France, June 2003. 66 pages.

Soumissions à des revues internationales

— 2007 —

[11] 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. Soumis à Information and Computation.

[12] B. Księżopolski and P. Lafourcade. Attack and revison of an electronic auction protocol using OFMC. Technical Report 549, Department of Computer Science, ETH Zurich, Switzerland, Feb. 2007. 13 pages. Soumis à Annales UMCS, Informatica.

Rapports de Contrats

— 2007 —

[13] P. Lafourcade. Rapport d'activités à 3 mois, contrat CNRS/DGA référence : 06 60 019 00 470 75 01 « Utilisation et exploitation des théories équationnelles dans l'analyse des protocoles cryptographiques. ». Technical report, ETH Zürich, Jan. 2007. 3 pages.

— 2004 —

[14] 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.

[15] 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.

Projets.

ACI Sécurité Rossignol (Action Concertée Incitative 2003 - 2006). Projet soutenu par le ministère français de la recherche, 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`).

Ma thèse fut financé par l'ACI Rossignol pour renforcer la collaboration entre les différents laboratoires et plus particulièrement entre le LSV et le LIF. L'ensemble de mes travaux s'inscrit donc dans cette ACI.

Projet RNTL PROUVÉ (Réseau National des Technologies Logicielles 2003-2006). Projet soutenu par le ministère français de la recherche, réunissant les partenaires suivants :
- 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/`).

Mes travaux sur les propriétés algébriques constituent une partie importante des avancées effectuées dans ce projet. Ce projet a permis de nombreuses collaborations entre les différents partenaires et l'élaboration d'un langage commun de spécification pour la vérification de protocoles.

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

Dans ce projet, nous cherchons à modéliser les propriétés induites par les réseaux sans fil et à prendre en compte la mobilité des entités dues à ce nouveau mode de communication afin de vérifier de nouveaux protocoles.

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/`

Communications.

Exposé invité :

- Conférence internationale IBIZA 2007, 9 Février 2007, Pologne.

Présentations d'articles à des conférences internationales :

- 33rd International Colloquium on Automata, Languages and Programming (*ICALP 2006*), 10 Juillet 2007, Venise Italie.
- 16th International Conference on Rewriting Techniques and Applications (*RTA 2005*), 20 Avril 2005, Nara Japon.

Présentations d'article à un workshop international :

- 1st International Workshop on Security and Rewriting Techniques (*SecReT 2006*), 15 Juillet 2006, Venise Italie.

Séminaires et exposés :

- Séminaire du groupe "Information Security" à l'ETH Zürich, Suisse, 9 Septembre 2006.
- 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 poytechnique, projet RNTL PROUVé à Nancy.

Participations aux conférences et workshops internationaux :

- 2nd Workshop on Formal and Computational Cryptography (*FCC 2006*), Venise Italie.
- 6th International Workshop on Issues in the Theory of Security (*WITS 2006*), Vienne Autriche.
- 18th IEEE Computer Security Foundations Workshop (*CSFW 2005*), Aix-en-Provence France.
- 19th International Workshop on Unification (*UNIF 2005*), Nara Japon.
- European Joint Conferences on Theory and Practice of Software (*ETAPS 2004*), Barcelone Espagne.

Collaborations.

Actuellement, j'ai commencé des travaux sur les thèmes suivants :

Les réseaux sans fil, avec :

- David Basin, ETH Zürich Suisse.
- Srdjan Capkun, ETH Zürich Suisse.
- Patrick Schaller, ETH Zürich Suisse.

Les protocoles de groupes, avec :

- Ralf Kuesters, ETH Zürich Suisse.

Les propriétés algébriques, avec :

- Yannick Chevalier, IRIT Toulouse.

La vérification de protocoles de vote et de vente aux enchères, avec :

- Cas Cremers, ETH Zürich Suisse.
- Luca Viganò, Université de Verone Italie.
- Sebatian Mödersheim, IBM Zürich Suisse.
- Bogdan Księżopolski, Université de Lublin Pologne.

5 Programme de recherche détaillé.

Analyse automatique et formelle des propriétés des protocoles de nouvelle génération.

Assurer la confidentialité des données est un enjeu majeur des systèmes informatiques actuels, compte tenu de la prolifération des échanges sécurisés d'information sur internet. La plupart des appareils électroniques sont désormais connectés entre eux et interagissent pour proposer de nouveaux services aux utilisateurs. Dans ce nouvel environnement, les concepteurs de tels systèmes créent des protocoles cryptographiques de plus en plus complexes ayant pour but d'assurer la confidentialité des informations échangées ainsi que de nouvelles propriétés, comme l'anonymat, l'équité... En raison de la complexité croissante de ces protocoles, il apparaît clairement qu'une analyse manuelle n'est pas suffisante. Une telle approche avait par exemple vérifié le célèbre protocole de Needham-Schroeder [NS78] avant qu'une analyse automatique et formelle quinze ans plus tard ne révèle l'existence d'une faille [Low95]. En conséquence, il est indispensable aujourd'hui de développer des méthodes formelles et automatiques de vérification pour les propriétés des protocoles cryptographiques de nouvelle génération : en particulier les protocoles régissant les Web Services, les communications sans fil, le commerce électronique... L'analyse de ces protocoles spécialisés est difficile car elle met en œuvre les quatre aspects suivants :

- l'*environnement* dans lequel le protocole est exécuté.
- l'*implantation* même des protocoles.
- les *opérateurs algébriques* utilisés dans la spécification même du protocole.
- les *propriétés globales* que doivent garantir les protocoles.

Mon projet de recherche consiste donc à analyser de la manière la plus réaliste possible les protocoles suivant ces quatre axes. Pour faciliter cette analyse, je compte étudier pour chacun de ces aspects une classe de protocoles particulièrement représentative. Mon projet de recherche concerne l'analyse automatique et formelle des propriétés des protocoles de nouvelle génération et s'articule autour des thèmes suivants :

- *Étude de nouvelles propriétés des réseaux sans fil.*
- *Modélisation et vérification des Web Services.*
- *Analyse formelle des protocoles de groupe.*
- *Vérification des protocoles de vote et de vente aux enchères.*

Étude de nouvelles propriétés des réseaux sans fil.

Objectif : Le premier aspect de mon programme de recherche vise à étudier les protocoles cryptographiques en prenant en compte l'environnement dans lequel ils sont exécutés.

Problématique : Compte tenu de l'émergence de l'intelligence ambiante (objets intelligents, sensibles à leur environnement et capables d'interagir) il est important de modéliser, d'analyser et de vérifier les protocoles cryptographiques dans un réseau sans fil. Ces dernières années, les connexions sans fil (*wireless*) entre les différents composants d'un réseau se sont développées grâce à la multiplication des systèmes embarqués. Ces avancées technologiques modifient considérablement les hypothèses faites habituellement dans la vérification de protocoles cryptographiques. Nous ne pouvons plus considérer que les messages sont échangés instantanément entre deux agents et les connexions sans fil permettent aux agents de se déplacer tout en restant connectés. Par exemple, le système de navigation embarqué dans un véhicule s'informe de l'état du réseau routier (accident, embouteillages...) en communiquant avec les autres véhicules. Tout cela donne naissance à de nouveaux protocoles et à de nouvelles propriétés qu'il faut alors vérifier : propriété de voisinage, de borne sur la distance entre les participants, de localisation des agents... Ces propriétés sont cruciales pour établir une connexion sans fil sécurisée entre deux agents. Récemment plusieurs protocoles ont été développés pour découvrir si deux agents ont la possibilité de communiquer directement : dans ce cas, les deux agents sont voisins, ils possèdent la propriété de « voisinage ». Je souhaite proposer un modèle permettant l'analyse la plus réaliste possible de ces nouvelles propriétés spatiales et temporelles pour les protocoles de nouvelle génération pour un réseau sans fil.

État de l'art : Les concepteurs de ces protocoles garantissent la propriété de voisinage par une analyse informelle. Actuellement il n'existe que quelques tentatives d'analyse formelle pour des protocoles particuliers [Mea07] et aucune

de ces approches, à ma connaissance, n'a réussi à formaliser de façon satisfaisante la propriété de voisinage.

Proposition d'étude : Dans le cadre de mon stage post-doctoral à l'ETH de Zürich, je participe au projet VerSePro (Verification of Security and privacy Protocols for wireless networks) faisant partie du projet MICS (Mobile and Information Communication Systems). Dans ce projet, à partir des protocoles et des technologies de communication sans fil existants, nous avons proposé une modélisation pour la propriété de voisinage entre deux agents. Cette modélisation inspirée par le modèle de traces de L. Paulson [Pau97] permettra de vérifier automatiquement et formellement si un protocole garantit la propriété de voisinage. Ensuite, en fonction des caractéristiques du médium utilisé dans la communication, il faut modéliser les capacités d'un intrus de nouvelle génération. En effet, dans les communications sans fil l'intrus est capable de relayer un message pour faire croire à un agent qu'il est voisin d'un autre alors qu'en réalité les deux agents ne le sont pas. Tout l'intérêt de ce nouveau thème de recherche consiste à modéliser de la façon la plus réaliste possible les échanges de messages entre les participants. Mes travaux antérieurs, en particulier l'augmentation du pouvoir de l'intrus par de nouvelles propriétés algébriques [5], me permettront par conséquent de modéliser les capacités de ce dernier afin de capturer les spécificités introduites par les réseaux de communication sans fil.

Modélisation et vérification des Web Services.

Objectif : Le second axe de mon programme de recherche consiste à prendre en compte l'implantation des protocoles. Je prévois de modéliser et d'analyser l'interaction entre plusieurs services proposés sur internet, appelés « Web Services », généralement implantés en XML.

Problématique : Lors d'un achat en ligne, la communication entre l'acheteur et le site internet s'effectue grâce à un protocole cryptographique afin de sécuriser les échanges de données confidentielles. De plus, après avoir demandé les coordonnées de l'utilisateur, le site internet contacte l'organisme bancaire indiqué par le client via un autre protocole cryptographique afin d'effectuer la transaction. L'exécution finale de ce protocole doit être paramétrée d'une part par les politiques de sécurité de chaque service et d'autre part par la politique de sécurité globale attendue. Car, même si les différents protocoles employés lors de cet échange sont sûrs et vérifiés indépendamment, une faille peut apparaître lors de leur combinaison et des données confidentielles peuvent être découvertes par l'intrus. Ces attaques reposent sur le fait que les protocoles sont implantés en XML et que les différents services utilisent les mêmes clefs dans différents protocoles. Il est donc important de vérifier automatiquement et formellement l'interaction de ces protocoles.

État de l'art : Peu de travaux jusqu'à présent ont réussi de façon satisfaisante à modéliser et à vérifier l'interaction des Web Services. Cette interaction entre les différents services est une composante importante des protocoles développés de nos jours qui sont de plus en plus complexes et spécialisés utilisant principalement le format XML dans leur implantation.

Proposition d'étude : Fort de mes études sur les protocoles cryptographiques en présence de théories équationnelles, j'envisage d'étudier les Web Services pour assurer aux utilisateurs une plus grande sécurité. Dans mes travaux [6, 4], j'ai analysé l'interaction de différentes théories équationnelles, j'ai montré de quelle façon les opérateurs algébriques s'appliquent et j'ai proposé une procédure de vérification formelle des protocoles cryptographiques en présence de ces théories équationnelles. Les interactions entre les différents Web Services en XML se modélisent de façon naturelle grâce à de telles théories. C'est pourquoi, les objectifs majeurs dans l'étude des Web Services sont d'abord d'arriver à comprendre et à formaliser les interactions qui les composent puis de développer à partir de cette modélisation une procédure automatique de vérification.

Analyse formelle de protocoles de groupe.

Objectif : Ce thème de recherche couvre deux des aspects des protocoles cryptographiques que je souhaite explorer : le premier est de vérifier une propriété du protocole (le secret), et le second est de prendre en compte l'environnement dans lequel il est exécuté (le nombre de participants).

Problématique : Les protocoles de groupe sont utilisés pour distribuer une clef entre les différents participants du groupe. Ils permettent d'introduire un nouveau participant au sein d'un groupe existant, ou d'en exclure un des membres. La spécificité de ces protocoles vient de leur conception même car ils sont élaborés pour un nombre quelconque d'agents. Ces protocoles fonctionnent grâce à un échange de messages récursifs entre les différents participants. C'est-à-dire que les différents traitements sur les messages sont effectués de manière récursive. Ce procédé permet au protocole d'être applicable quel que soit le nombre d'agents. Il est donc particulièrement important de vérifier ces protocoles pour un nombre quelconque de participants.

État de l'art : Ces protocoles ne sont vérifiés pour le moment que pour un nombre fixé de participants [KT07, SBM04] alors qu'ils sont conçus pour un nombre arbitraire d'agents. Les nombreux outils et méthodes de vérification développés jusqu'à présent analysent ces protocoles pour un nombre fixé de participants, souvent deux ou trois. Ces techniques ne sont pas adaptées à la vérification pour un nombre quelconque d'agents en raison de leur conception même : elles nécessitent de définir le rôle de chacun des participants.

Proposition d'étude : Je souhaite donc étudier les protocoles de groupe afin d'en dégager une classe de protocoles « récursifs ». A cet égard, une modélisation en clauses de Horn me permettra de déterminer une sous-classe de protocoles « récursifs » pour laquelle la vérification de la propriété de secret sera décidable. Cette abstraction par les clauses de Horn permettra de capturer le caractère récursif de ces protocoles cryptographiques.

J'envisage dans un deuxième temps de regarder s'il n'est pas suffisant de vérifier les protocoles « récursifs » pour un nombre borné d'agents en m'inspirant du résultat obtenu par V. Cortier et H. Comon [CLC04] selon lequel il suffit d'un seul intrus en plus des participants honnêtes pour analyser les protocoles.

Vérification de protocoles de vote et de vente aux enchères.

Objectif : Les protocoles de vote et de vente aux enchères utilisent souvent, pour garantir certaines propriétés, des opérateurs algébriques munis de théories équationnelles particulières. Ces deux classes de protocoles peuvent être analysées du point de vue des opérateurs algébriques utilisés ainsi qu'au travers des nouvelles propriétés qu'ils visent à garantir.

Protocoles de vente aux enchères.

Problématique : Les protocoles de vente aux enchères (*e-auction*) fleurissent de nos jours sur internet. Ces protocoles doivent garantir de nombreuses propriétés comme l'anonymat des acheteurs et des vendeurs, l'équité entre les acheteurs, la confidentialité des propositions d'achat et de vente, l'authentification des participants et la bonne conformité de la procédure de vente. Toutes ces propriétés sont garanties par différentes étapes du protocole et par des opérateurs algébriques dans la spécification même du protocole.

État de l'art : Je n'ai recensé aucune analyse formelle et vérification automatique dans la littérature concernant les propriétés que doivent assurer les protocoles de ventes aux enchères.

Proposition d'étude : En conséquence, fort d'un premier travail [12] dans lequel nous avons trouvé une faille sur un protocole d'enchère électronique, je me propose d'explorer cette nouvelle famille de protocoles. Je pense utiliser le Pi-calcul pour modéliser les propriétés spécifiques que doivent garantir les protocoles de vente aux enchères électroniques, comme l'équité entre les participants ou encore l'anonymat des vendeurs. Ensuite, de nombreuses phases de ces protocoles utilisent des opérateurs algébriques pour assurer certaines de ces propriétés. Mes travaux de thèse [6] sur les théories équationnelles seront de la plus grande utilité pour commencer la vérification de ces protocoles.

Protocoles de vote.

Problématique : Avec la démocratisation d'internet, de nombreux pays songent à employer des protocoles de vote électronique pour leurs élections. Il existe d'ores et déjà de nombreux protocoles de vote électronique. La peur des électeurs face aux fraudes éventuelles dues à ce nouveau système de vote est réelle : comment garantir qu'une personne ne vote qu'une seule fois, l'anonymat des électeurs, la confidentialité des bulletins de vote... Ces propriétés sont

assurées dans de nombreux protocoles de vote proposées par des opérateurs cryptographiques, comme le chiffrement de Naccache et Stern [NS97]. Une analyse formelle permettrait de garantir la sécurité de cette nouvelle procédure électorale et contribuerait sans doute à augmenter la confiance des citoyens.

État de l'art : À ma connaissance, quelques travaux [KR05, DKR06] effectuent une analyse formelle des propriétés que doivent assurer les protocoles de vote. Cependant aucun d'entre eux ne prend en compte les propriétés algébriques des opérateurs employés dans la spécification du protocole.

Proposition d'étude : Fort de mon travail de thèse sur les opérateurs homomorphiques et les chiffrements distributifs [6, 3, 1], j'envisage d'étudier les protocoles de vote qui, pour satisfaire la confidentialité des bulletins de vote, utilisent souvent des fonctions de chiffrement dites « homomorphiques ». Je pense alors proposer une analyse des propriétés requises par un protocole de vote, comme l'anonymat des votants ou la confidentialité des votes, ceci en prenant en compte les propriétés algébriques utilisées. Car, comme mes travaux l'ont démontré, il se peut qu'un protocole soit prouvé sûr et qu'une faille existe en prenant en compte une propriété algébrique utilisée par la spécification du protocole. Il est donc nécessaire d'effectuer une telle analyse pour vérifier correctement les protocoles de vote électronique.

Intégration dans un laboratoire de recherche.

Mon programme de recherche correspond aux thèmes étudiés par l'équipe Verimag à Grenoble. Plusieurs chercheurs de ce laboratoire travaillent sur la sécurité informatique et la vérification formelle de protocoles cryptographiques (Liana BOZGA, Judicaël COURANT, Yassine LAKHNECH, Jean-François MONIN, Michael PÉRIN). Le second et le quatrième volet de mon projet de recherche qui visent respectivement à analyser l'interaction entre plusieurs Web Services et les protocoles de vote et de vente aux enchères, impliquent l'utilisation de notions temporelles, domaine auquel Yassine LAKHNECH et son équipe s'intéresse. De plus, Jean-François MONIN et Judicaël COURANT s'intéressent aux propriétés algébriques des protocoles cryptographiques en utilisant COQ [CM06]. Enfin l'outil Hermes [BLP03] développé par l'équipe Verimag est un des seuls outils à l'heure actuelle permettant de considérer un nombre nonbornés de sessions. Il est donc naturel d'essayer d'implanter dans cet outil mes travaux de thèse sur l'interaction d'un symbole homomorphique et le « ou-exclusif ». Mon programme de recherche s'inscrit bien dans la thématique de l'équipe Verimag, tout en apportant de nouveaux axes de recherche sur la modélisation et la vérification des nouvelles propriétés des protocoles de communication sans fil, de ventes aux enchères et de vote élecrtonique.

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 P. Gardner and N. Yoshida, editors, *Proc. 15th International Conference on Concurrency Theory (CONCUR'04)*, volume 3170 of *Lecture Notes in Computer Science*, pages 177–192, London, England, 2004. Springer-Verlag.

[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.

[BLP03] L. Bozga, Y. Lakhnech, and M. Perin. HERMES : An Automatic Tool for Verification of Secrecy in Security Protocols. In *Computer Aided Verification*, 2003.

[BMV05] D. Basin, S. Mödersheim, and L. Viganò. Ofmc : A symbolic model checker for security protocols. *International Journal of Information Security*, 4(3) :181–208, June 2005. Published online December 2004.

[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.

[CLC04] H. Comon-Lundh and V. Cortier. Security properties : two agents are sufficient. *Science of Computer Programming*, 50(1-3) :51–71, March 2004.

[CM06] J. Courant and J.-F. Monin. Defending the bank with a proof assistant. In *WITS 2006*, Vienna, March 2006. In WITS proceedings.

[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.

[DKR06] S. Delaune, S. Kremer, and M. D. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06)*, pages 28–39, Venice, Italy, July 2006. IEEE Computer Society Press.

[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.

[KR05] S. Kremer and M. D. Ryan. Analysis of an electronic voting protocol in the applied pi-calculus. In M. Sagiv, editor, *Programming Languages and Systems — Proceedings of the 14th European Symposium on Programming (ESOP'05)*, volume 3444 of *Lecture Notes in Computer Science*, pages 186–200, Edinburgh, U.K., April 2005. Springer-Verlag.

[KT07] R. Küsters and T. Truderung. On the automatic analysis of recursive security protocols with xor. Technical report, ETH Zurich, 2007. An abridged version appears in STACS 2007.

[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 Seurity Foundation Workshop (CSFW'96)*, pages 48–62, Kenmare, Ireland, 1996. IEEE Computer Society Press.

[Mea07] *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*, volume 30 of *Advances in Information Security series*, chapter Distance Bounding Protocols : Authentication Logic Analysis and Collusion Attacks, pages 279–298. Springer, 2007.

[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.

[NS97] D. Naccache and J. Stern. A new public-key cryptosystem. *Proc. International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'97)*, 1233 :27–37, 1997.

[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.

[RT01] M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is NP-complete. In *Proc. 14th Computer Security Foundations Workshop (CSFW'01)*, pages 174–190, Cape Breton, Canada, 2001. IEEE Computer Society Press.

[SBM04] G. Steel, A. Bundy, and M. Maidl. Attacking a protocol for group key agreement by refuting incorrect inductive conjectures. In D. A. Basin and M. Rusinowitch, editors, *IJCAR*, volume 3097 of *Lecture Notes in Computer Science*, pages 137–151. Springer, 2004.

[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.

6 Listes des pièces jointes.

Piéces administratives :

- Photocopie de la carte d'identité.
- Déclaration ANTARES.
- 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.

Enseignements :

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

Recherche :

- Lettre de recommandation de Michael RUSINOWITCH.
- Lettre de recommandation de mon responsble de post-doctorat (David BASIN).
- Lettre de recommandation de mes directeurs de thèse (Denis LUGIEZ et Ralf TREINEN).
- Lettre de recommandation d'une de mes co-directrices de DEA (Marie-Christine LAGASQUIE-SCHIEX).

Publications jointes lors de l'audition :

[1] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of abelian groups with distributive encryption. *Information and Computation*, 205(4) :581–623, Apr.

[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.

[4] 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.

[6] 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.

Adresses des personnes m'ayant recommandé :

Prof. Michael RUSINOWITCH
LORIA-INRIA-Lorraine
615, rue du Jardin Botanique, BP 101,
54602 Villers les Nancy Cedex, France
Phone : +33 3 83 59 30 20
Email : `Michael.Rusinowitch@loria.fr`

Prof. David BASIN
ETH Zürich, IFW C 49.2
Haldeneggsteig 4 / Weinbergstrasse
8092 Zürich, SWITZERLAND
Phone : +41 44 632 72 45
Email : `basin@inf.ethz.ch`

Prof. Denis LUGIEZ
Université de Provence Marseille
Centre de Mathématiques et d'Informatique
39 rue Joliot Curie,
13453 MARSEILLE, FRANCE
Phone : (+33) 4 91 11 36 23
Email : `lugiez@cmi.univ-mrs.fr`

Ralf TREINEN, Maître de Conférences
Laboratoire Spécification et Vérification
École Normale Supérieure de Cachan
61, avenue du Président Wilson
94235 CACHAN Cedex - France
Phone : +33 1 47 40 75 67
Email : `treinen@lsv.ens-cachan.fr`

Marie-Christine LAGASQUIE-SCHIEX, Maître de Conférences
Institut de recherche en informatique de Toulouse,
118 route de Narbonne,
31062 Toulouse Cedex 4, France.
Phone : +33 (0)5 61 55 64 51
Email : Philippe.Balbiani@irit.fr

Prof. Danièle BEAUQUIER
Département d'Informatique
Université Paris 12
Bat P2 - 2e étage - Bureau 220
61 Avenue du Général de Gaulle
94010 Créteil CEDEX, France
Phone : +33 01 45 17 16 44
E-mail : beauquier@univ-paris12.fr

Prof. Régine LALEAU
Université Paris 12-IUT
Département Informatique
Route forestière Hurtault
F-77300 Fontainebleau, France
Phone : +33 (0)1 60 74 68 40
E-mail : laleau@univ-paris12.fr