INRIA

Candidat ***Applicant***
Nom *Last Name*
LAFOURCADE
Prénom *First Name*
Pascal

DOSSIER DE CANDIDATURE AU CONCOURS EXTERNE DE CHARGÉS DE RECHERCHE DE DEUXIÈME CLASSE POUR L'ANNÉE 2007

APPLICATION PACKET FOR THE COMPETITIVE SELECTION OF JUNIOR RESEARCH SCIENTISTS FOR YEAR 2007

Formulaire 1/*Form 1*

FICHE INDIVIDUELLE DE RENSEIGNEMENTS
PERSONAL INFORMATION

Nom/*Last Name* : LAFOURCADE Prénom/*First Name* : Pascal
Date et lieu de naissance/*Date and place of birth* : 26/04/1977, Toulouse (France)
Nationalité/*Citizenship* : Française Sexe/*Sex* : M
Adresse postale/*Mailing address* : Information Security
ETH Zürich, IFW C 46.1
Haldeneggsteig 4
CH-8092 Zürich, Suisse
N° de téléphone/*Telephone* : (+41) 44 632 72 72
Adresse électronique/*E-mail* : pascal.lafourcade@inf.ethz.ch
Page Web personnelle/*Web page* : www.inf.ethz.ch/personal/pascall/

DIPLÔMES FRANÇAIS OU ÉTRANGERS[1]/*DIPLOMAS*[2]

Doctorat(s)/*Ph.D.(s)* :

- **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*. Doctorat effectué au sein du Laboratoire Spécification et Vérification CNRS UMR 8643 & INRIA Futurs projet SECSI, dans le cadre de l'ACI sécurité ROSSIGNOL. **Jury** : Claude KIRCHNER LORIA Nancy (président), Yassine LAKHNECH Verimag Grenoble (rapporteur), Luca VIGANÓ ETH Zürich (rapporteur), Ralf TREINEN LSV ENS de Cachan (directeur), Denis LUGIEZ LIF Marseille (co-directeur), Yannick CHEVALIER IRIT Toulouse (examinateur).

Autres diplômes (à partir du niveau maîtrise)/***Other diplomas*** *(Master's and higher)* :

- **Diplôme Universitaire NTCA** (Nouvelles Techniques Cognitives d'Apprentissages) de l'École Normale Supérieure de Cachan, soutenu le 29 Septembre 2006, mention *Assez-Bien*.
- **D.E.A.** Représentation de la Connaissance et Formalisation du Raisonnement, mention *Bien*. Stage de recherche effectué à l'IRIT (Toulouse), sur l'*application de la résolution de conflits « logiques », à l'aide à la décision pour la résolution de conflits des problèmes d'ordonnancement*, obtenu en juin 2003. Co-encadré par Claudette CAYROL, Hélène FARGIER et Marie-Christine LAGASQUIÉ-SCHIEX.
- **Maîtrise** d'informatique option Intelligence artificelle et Image de l'Université Paul Sabatier (Toulouse III), mention *Assez-Bien*, obtenue en 2002 (projet de maîtrise en analyse d'images sur la détection de défauts dans l'assemblage de ballons stratosphériques : conception, réalisation et mise en place du système développé en milieu industriel : ZODIAC Espace) .
- **Maîtrise** de mathématiques fondamentales de l'Université Paul Sabatier (Toulouse III), obtenue en 2001 (mémoire sur la théorie des nœuds).

SITUATION PROFESSIONNELLE ACTUELLE/*CURRENT PROFESSIONAL STATUS*

Statut et fonction/*Position and statute* : Titulaire d'une bourse DGA/CNRS. Post-doctorant dans l'équipe « Information Security » du Professeur David Basin.
Etablissement (ville - pays)/*Institution (city -country)* : ETH Zürich Suisse
Date d'entrée en fonction/*Start* : 1er Octobre 2006
[ ] Sans emploi /*Without employment*

[1] Indiquer l'intitulé précis (doctorat, etc.), la date, le lieu d'obtention et l'établissement d'origine des diplômes. Dans le cas où la thèse s'est déroulée au sein d'un projet INRIA, veuillez indiquer l'unité de recherche.

[2] *Indicate the exact title, the date, the place, and the institution granting the degree. If the thesis took place within an INRIA project, do please indicate the research center.*

FORMATION ET PARCOURS PROFESSIONNEL/ *TRAINING AND PROFESSIONAL HISTORY*

ÉTABLISSEMENTS français ou étrangers *INSTITUTIONS French or foreign*	FONCTIONS ET STATUTS[3] (salarié, boursier, etc.) *POSITIONS AND STATUS[4] (employee, fellow, etc.)*	DATES d'entrée en fonction *Start*	DATES de cessation de fonction *End*	OBSERVATIONS *REMARKS*
ETH Zürich	Boursier DGA/CNRS	01/10/2006	30/09/2007	Suisse
LSV, ENS de Cachan	Allocataire de recherche	01/10/2003	30/09/2006	ACI ROSSIGNOL
Université Paris XII	Moniteur	01/10/2003	30/09/2006	Créteil
Basket Labège Auzeville Club	Emploi jeune	01/09/2001	30/09/2003	Plein temps
Université Paul Sabatier	DEA RCFR (IRIT)	01/09/2002	31/08/2003	Toulouse III
	Maîtrise Informatique	01/09/2001	31/08/2002	
	Licence Informatique	01/09/2000	31/08/2001	
	Maîtrise Mathématiques	01/09/1999	31/08/2001	

[3]Indiquer avec précision chaque situation statutaire. Par exemple : pour une situation d'agent titulaire de la fonction publique, préciser le corps et le grade de rattachement, pour une situation de salarié du secteur privé ou d'agent non titulaire d'un établissement public, préciser la nature du contrat salarial, etc.

[4]*For each position, indicate grade or rank. For example, for a tenured civil service position, indicate the branch and rank, for a private sector position or non-tenured position in a public institution, indicate the nature of the work contract, etc.*

Formulaire 2/*Form 2*

SYNTHÈSE DE LA CANDIDATURE
APPLICATIONS SUMMARY

Nom/*Last name*: LAFOURCADE Prénom/*First name*: Pascal
Projets d'affectation souhaités/Assignation whishes : CASSIS (LORIA), LANDE (IRISA).

1. Résumé de l'activité de recherche/*Summary of research activities*

Mes travaux de thèse ont consisté à étudier la vérification de protocoles cryptographiques en présence de propriétés algébriques. L'objectif était d'affaiblir l'hypothèse du chiffrement parfait qui prévaut dans ce domaine : le seul moyen de déchiffrer un message crypté est d'en posséder la clé. Nous constatons néanmoins l'existence de failles possibles dans de nombreux protocoles qui ne peuvent être modélisées sous cette hypothèse. Elle n'est pas assez réaliste pour assurer la confidentialité d'une information échangée sur le réseau grâce à de tels protocoles. A l'issue de mes recherches, j'ai réussi à augmenter les capacités de l'intrus en formalisant de nouvelles propriétés algébriques afin de vérifier de manière plus concrète les protocoles cryptographiques. Mes travaux montrent ainsi la décidabilité du problème de sûreté des protocoles en présence de théories équationnelles homomorphiques pour un intrus passif et actif.

2. Résumé du programme de recherche/*Summary of research program*

De nos jours, grâce aux récentes avancées technologiques, les nouveaux protocoles de communication sécurisés sont omniprésentes en particulier dans les systèmes embarqués. Il est donc important d'analyser ces nouveaux modes de communications suivant les quatre perspectives suivantes : l'*implantation* spécifique du protocole même, l'*environnement* dans lequel le protocole est exécuté, les *opérateurs algébriques* utilisés lors de sa spécification, et les *propriétés* que le protocole doit satisfaire. Mon programme de recherche a pour but de modéliser et d'analyser les protocoles cryptographiques selon ces quatre axes. Je propose en conséquence les thèmes de recherche suivants :

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

Ces thématiques de recherche me permettent d'envisager une intégration au sein du projet CASSIS à l'INRIA Lorraine ou du projet LANDE à l'INRIA Rennes.

3. Publications/*Publications*

[1] P. Lafourcade, D. Lugiez, and R. Treinen. Intruder deduction for the equational theory of abelian groups with distributive encryption. *Information and Computation*, 2007. To appear. 51 pages.

Dans cet article nous avons résolu le problème de déduction de l'intrus en présence d'un chiffrement distributif sur l'opérateur de groupe abélien. Ce travail a requis l'utilisation de Z-modules pour capturer le nombre infini de coefficients possibles de chaque termes, infinité induite par la structure même des groupes abéliens.

[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] 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.

Dans ce papier, j'élucide le problème de secret pour un intrus passif en présence de chiffrement commutatif et distributif sur le ou-exclusif. Ce travail étend un résultat précédent [5] et nécessite de nouvelles normalisations de preuves dues à la commutativité du chiffrement. Une analyse plus fine de l'interaction des différentes composantes de la théorie équationnelle m'a permis de résoudre ce problème plus complexe.

[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 *LNCS*, pages 132–143, Venice, Italy, July 2006. Springer.

Ce travail montre la décidabilité du problème de secret face à un intrus actif pour un nombre borné de sessions en présence d'homomorphisme et du ou-exclusif. Nous avons développé une procédure d'unification [8] et une méthode de résolution de certains systèmes d'équations diophantiennes quadratiques. De plus cette procédure permet pour la première fois de résoudre de manière satisfaisante le cas d'un intrus actif pour les groupes abéliens. Nous avons étendu depuis ce résultat aux théories monoïdales [7], travail soumis à une revue internationale.

[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 *LNCS*, pages 308–322, Nara, Japan, Apr. 2005. Springer.

[7] S. Delaune, P. Lafourcade, D. Lugiez, and R. Treinen. Symbolic protocol analysis for monoidal equational theories. Research Report LSV-06-17, LSV ENS Cachan, France, Nov. 2006. 47 pages.

[8] 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.

4. Réalisation et diffusion de logiciels/*Software writing and distribution*

5. Valorisation et transfert technologique/*Development and technology transfer*

Durant ma thèse, j'ai participé au Projet RNTL Prouvé (2003-2006 `www.lsv.ens-cachan.fr/prouve/`) en collaboration avec France Télécom et à l'ACI Sécurité ROSSIGNOL (2003-2006 `www.lif.univ-mrs.fr/~lugiez/aci-rossignol.html`) en étudiant les propriétés algébriques utilisées dans les protocoles cryptographiques. Depuis mon arrivée à l'ETH Zürich je participe au projet de recherche VerSePro faisant parti du projet MISC (`www.mics.org/`) sur la vérification des réseaux sans fil.

6. Encadrement d'activités de recherche/*Supervision of research activities*

7. Enseignement/*Teaching*

2006 - 2007 : **Assitant** à l'ETH Zürich du professeur David BASIN, 2^{nd} semestre, 32h de TD en anglais dans le cours « Information and Security » et du professeur Gaston GONNET, 1^{er} semestre, 32h de TD en anglais dans le cours « Modelisation and Simulation ».

2003 - 2006 : **Moniteur** au CIES de Jussieu, à l'Université PARIS XII. Enseignement effectué à l'Université de Créteil avec Danièle BEAUQUIER et à l'IUT de Fontainebleau avec Régine LALEAU, Patrick CEGIELSKI et Konstantin VERCHINI, 192h en 3 ans.

Niveau	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 & Réseaux	TP	32h
		Total	192h

2005 - 2006 : **Assistant** du professeur Alain FINKEL en techniques d'apprentissages, 32h de TD.

2002 - 2003 : **Vacataire** à l'INSA Toulouse avec Gilles MOTET, 1 semestre 32h TP, Initiation à la programmation en AD95.

1995 - 2002 : **Professeur particulier** de mathématiques pour tous les niveaux du collège au lycée.

8. Diffusion de l'information scientifique/*Dissemination of scientific knowledge*

9. Mobilité/*Visits*

Après avoir effectué des études jusqu'en maîtrise de mathématiques fondamentales (mémoire sur la théorie des nœuds) j'ai fait un cursus en informatique : licence, maîtrise et j'ai obtenu un DEA à l'IRIT de Toulouse en Intelligence Artificielle. Ensuite, j'ai changé de thématique et de lieu en débutant une thèse sur la vérification de protocoles cryptographique au LSV à l'ENS de Cachan au sein du projet SECSI de l'INRIA Futurs dans le cadre de l'ACI Sécurité ROSSIGNOL. Durant mes 3 années de thèse, j'ai passé un an au Laboratoire d'Informatique Fondamentale de Marseille CNRS UMR 6166 dans l'équipe MoVe de Denis Lugiez. Enfin, j'ai obtenu une bourse de la DGA pour un post-doctorat à l'ETH Zürich (Suisse) dans l'équipe « Information and Security » de David Basin afin de travailler sur la vérification des protocoles sans fils, un nouveau thème de recherche. Lors de mon enseignement j'ai passé une année à l'Université de Créteil et deux ans à l'IUT de Fontainebleau et je me suis ainsi intégré dans différentes équipes pédagogiques. J'ai également participé, lors de ma thèse, aux écoles internationales suivantes : Dresden 2004 ICCL : « Théorie de la preuve et preuve automatique de théorème », Marseille 2005 « École de printemps sur la sécurité », et Marktoberdorf 2006 « Sûreté et sécurité des systèmes logiciels ».

10. Responsabilités collectives/*Responsibilities*

Organisation de colloques :

- Participation au comité d'organisation de la conférence internationale FORMATS 2006 à Paris du 25 au 28 Septembre 2006, et webmaster du site d'inscription. `www.lsv.ens-cachan.fr/formats06/`
- Membre du comité organisateur des Rencontres Emplois pour les Doctorants de l'EDSP de l'ENS de Cachan en mai 2005, manifestation de 3 jours organisée tous les 18 mois avec une centaine de doctorants.
- Participation au comité d'organisation des Journées Apprentissages 2006 à Paris du 17 au 19 Mai 2006, webmaster du site internet et assistant en TD. `www.lsv.ens-cachan.fr/~finkel/ja2006.html`

Évaluation d'articles :

J'ai évalué des articles pour la revue internationale *Information and Computation* et pour les conférences internationales suivantes : ICALP'07, RTA'06, CADE'05.

Charges administratives :

- Membre de l'équipe SOS, mailing liste d'aide pour les utilisateurs de Linux au sein du 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 d'aide pour l'utilisation du graveur et du scanner du LSV et de recherche bibliographique pour les membres du LSV.

11. Prix et distinctions/*Prizes and awards*

12. Autres éléments/*Miscellaneous*

- **Exposés, séminaires et présentations**.
  - Exposé invité à la Conférence IBIZA'07, 9 fevrier 2007, Kazimierz Dolny Pologne.
  - Séminaire 68NQRT à Rennes à l'IRISA, France, 27 juin 2006. `www.irisa.fr/NQRT/`
  - Séminaire de l'équipe Information Security de l'ETH Zürich, le 8 Septembre 2006.
  - Présentation de papiers à ICALP'06, Secret'06, RTA'05.
  - Exposé à l'école de printemps internationale sur la sécurité à Marseille 2005.
  - Plusieurs exposés à différents groupes de travail de l'équipe SECSI au LSV, équipe MOVE au LIF et aux rencontres de projet RNTL PROUVÉ à Nancy et ACI Sécurité Rossignol à Cachan et à Grenoble.
- **Divers**.
  - Français langue maternelle, anglais courant, espagnol scolaire et allemand débutant.
  - Languages de programmation : C, Pascal, Java, Prolog, Scheme, SQL, Php, ADA95, Maple.
  - Outils de vérification de protocoles : Avispa (Cl-Atse, OFMC), Proverif, Scyther.
  - Pilote de montgolfières dans l'association Air Aventure en Tarn-et-Garonne.
  - Joueur et entraîneur de basket-ball de jeunes et adultes (Emploi jeune pendant 2 ans).
  - Danseur de danses de société : rock, salsa, valse...

Formulaire 3/*Form 3*

PROGRAMME DE RECHERCHE DÉTAILLÉ[5]
DETAILED RESEARCH PROGRAM[6]

Nom/*Last name*: LAFOURCADE Prénom/*First name*: Pascal

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 de 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

[5] En cinq pages maximum.
[6] *Five pages maximum.*

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 quelques protocoles particuliers [MPP+07] 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 séjour 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. Car 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 différentes 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 vérifications 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, la 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 protocoles et par des opérateurs algébriques dans la spécification même du protocole.

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

Proposition d'étude : En conséquence, fort d'un premier travail [7] 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 votes électroniques. 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 votes 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 diminuer la peur des concitoyens.

État de l'art : À ma connaissance, quelques travaux [DKR06, KR05] 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 la plupart du temps 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 le projet INRIA LANDE à l'IRISA.

L'équipe LANDE, conception et validation de logiciels, à l'IRISA constitue une possibilité pour mon intégration à l'INRIA. Le thème de recherche central de ce projet est la conception d'outils d'aide au développement et à la validation de logiciels. Dans ce cadre, la sécurité logicielle est un domaine d'application privilégié, ce qui se traduit par l'élaboration de définitions de propriétés de sécurité et de techniques pour leur vérification automatique. Lors de mes travaux de thèse, consistant à développer des méthodes automatiques de vérification formelles, j'ai utlisé des techniques de réécriture et d'unification. Ces techniques correspondent parfaitement à l'approche utilisée par Thomas Genet à Rennes pour bâtir de nouvelles techniques de vérification développées dans Timbuk [GVTT01]. Ces techniques d'analyse développées par Thomas Jensen et Thomas Genet sont alors appliquées à la formalisation et la vérification de politiques de sécurité d'applications programmées [BJMT01] et à la vérification de propriétés de sécurité de midlets JAVA pour les téléphones portables de France Telecom. L'équipe LANDE collabore également avec Thomson R&D afin de modéliser et vérifier des propriétés de protocoles sans fil [BDJ06]. Ce thème de recherche correspond exactement au premier axe de mon programme recherche.

Références.

[BDJ06] F. Besson, G. Dufay, and T. Jensen. A formal model of access control for mobile interactive devices. In *11th European Symposium On Research In Computer Security (ESORICS'06)*, volume 4189 of *Lecture Notes in Computer Science*. Springer, 2006.

[BJMT01] F. Besson, T. Jensen, D. L. Métayer, and T. Thorn. Model ckecking security properties of control flow graphs. *Journal of Computer Security*, 9 :217–250, 2001.

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

[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.

[GVTT01] T. Genet and V. Viet Triem Tong. Reachability Analysis of Term Rewriting Systems with *timbuk*. In *8th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning*, volume 2250 of *Lectures Notes in Artificial Intelligence*, pages 691–702. Springer Verlag, 2001.

[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.

[MPP+07] C. Meadows, R. Poovendran, D. Pavlovic, L. Chang, and P. Syverson. *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.

[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.

[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.

Formulaire 4/*Form 4*

LISTE COMPLÈTE DES PUBLICATIONS[7]
COMPLETE PUBLICATION LIST[8]

Nom/*Last name*: LAFOURCADE Prénom/*First name*: Pascal

L'ensemble de mes publications est disponible 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*, 2007. To appear. 51 pages.

— **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. Bugliesi, 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.

[7] Les publications les plus significatives devront être consultables sur la page web du candidat.
[8] *Most relevant publications have to be available for consultation via the web page of the applicant.*

Autres publications

— **2007** —

[7] 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.

— **2006** —

[8] 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.

[9] 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** —

[10] 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** —

[11] 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** —

[12] 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.

Rapports de Contract

— **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.

Formulaire 5/*Form 5*

LETTRES DE RECOMMANDATION[9]
RECOMMENDATION LETTERS[10]

5 NOMS AU MAXIMUM/*MAXIMUM 5 NAMES*

Nom du candidat/*Applicant's Last Name*: LAFOURCADE Prénom/*First name*: Pascal

Le candidat est invité à joindre au dossier de candidature les originaux des lettres de recommandation qui lui auront été adressées par des personnalités du milieu académique ou industriel./The candidat may enclose the original of recommendation letters written by references from academia or industry.

Noms et adresses (inclure l'adresse électronique)/*Names and addresses (including email)* :

1. **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`
2. **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`
3. **Prof. Luca VIGANÒ**
   Dipartimento di Informatica
   Facoltà di Scienze Matematiche, Fisiche e Naturali
   Università di Verona
   Strada Le Grazie 15
   I-37134 Verona, Italy
   Phone : +39 4 58 02 70 70
   Email : `luca.vigano@univr.it`
4. **PD Dr. Ralf KÜSTERS**
   ETH Zürich, IFW E 48.3
   Institut für Theoretische Informatik
   Haldeneggsteig 4
   CH-8092 Zürich, Switzerland
   Phone : +41 44 632 55 14
   Email : `ralf.kuesters@inf.ethz.ch`

[9] La direction de l'INRIA demandera aussi un avis au(x) responsable(s) scientifiques(s) du ou des projets de recherche et au(x) directeurs d'unité(s) de recherche concerné(s) par la candidature.

[10] *INRIA will also solicit an evaluation from the research project-team leader(s) and the director(s) of the research center(s) where the candidate wishes to apply.*

5. **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

Formulaire 6/*Form 6*

DÉCLARATION DE CANDIDATURE
STATEMENT OF INTENT TO APPLY

Je soussigné(e)/*I, the undersigned* LAFOURCADE Pascal déclare présenter ma candidature au concours de recrutement de chargés de recherche de deuxième classe de l'INRIA pour l'année 2007/*hereby declare that I apply for the 2007 competitive selection for INRIA junior research scientists (chargés de recherche de deuxième classe) positions.*

Mon programme de recherche s'intitule/*Title of my research program*

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

En cas de réussite au concours je demande à être affecté(e) au sein du (ou des) projets de recherche suivants[11]/*If I am recruited by INRIA I wish to be assigned to the following research project-team(s)*[12] :

Les candidats sont invités à prendre contact avec les chefs des projets dans lesquels ils postulent/Applicants should enter in contact with the project leaders concerned by their applications.

	Projet de recherche *Project-team*
[ ] concours FUTURS BORDEAUX	
[ ] concours FUTURS LILLE	
[ ] concours FUTURS SACLAY	
[√] concours LORRAINE	CASSIS
[√] concours RENNES	LANDE
[ ] concours RHÔNE-ALPES	
[ ] concours ROCQUENCOURT	
[ ] concours SOPHIA ANTIPOLIS	

J'ai pris connaissance des conditions requises pour concourir[13], et je certifie sur l'honneur l'exactitude des renseignements fournis dans ce dossier/*I am aware of the conditions*[14] *required for the consideration of my application and I certify that the information I have supplied is true and correct.*

À/*City* Zürich, le/*Date* 14 février 2007
Signature

[11] Inscrire une croix dans la ou les cases choisies. Les chargés de recherche de deuxième classe de l'INRIA sont recrutés au sein de l'un des projets de recherche existants (ou en cours de création au moment du concours). C'est pourquoi il est demandé aux candidats d'indiquer le ou les projets de recherche auxquels ils souhaitent être rattachés en cas de recrutement (le nombre de projets de recherche indiqués ne doit pas excéder 2). Pour chaque projet de recherche mentionné, indiquer l'unité de recherche considérée : Futurs Bordeaux,Futurs Lille, Futurs Saclay, Lorraine, Rennes, Rocquencourt, Rhône-Alpes ou Sophia-Antipolis ; si le candidat postule à un projet localisé dans deux unités de recherche, il doit mentionner la ou les unités de recherche choisies. Voir la liste des projets de l'INRIA sur `http ://www.inria.fr/recherche/equipes/listes/index.fr.html`. Dans le cadre des souhaits émis par le candidat, la direction se réserve le droit de choisir l'unité de recherche d'accueil.

[12] *Check one or more boxes. INRIA junior research scientists (chargés de recherche de deuxième classe) are recruited within one of the existing project-teams (or in one of the project-teams being currently under creation). The applicant is asked to indicate the project-team(s) he or she wishes to be assigned to (no more than 2 project-teams). For each research project-team mentioned, indicate the research center : Futurs Bordeaux, Futurs Lille, Futurs Saclay, Lorraine, Rennes, Rocquencourt, Rhônes-Alpes or Sophia-Antipolis. If the applicant is applying to a project-team based in two research centers, the chosen research center(s) must be mentioned. See the list of INRIA research project-teams on* `http ://www.inria.fr/recherche/equipes/listes/index.en.html`. *As part of the wishes expressed by the candidate, the management reserves the right to choose the research center assigned.*

[13] Voir la brochure d'information.

[14] *See the information booklet.*