Rapport de Monitorat 2003-2006

Pascal Lafourcade

5 juin 2006

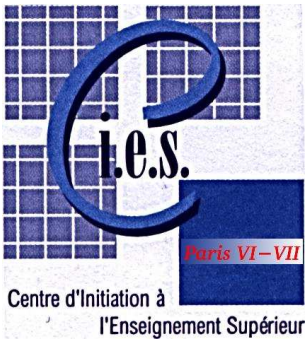

Table des matières

1 Enseignements.

1.1 Cours dispensés.

Mes expériences d'enseignements ont été réalisées en informatique en tant que moniteur et vacataire et en technique d'apprentissage comme assistant. La figure 1 donne un résumé chronologique des différents enseignements dispensés.

Public	Intitulé	Nature	Responsable	Eq TD	Année
1ère Année INSA	Programmation en ADA95	TP	G. Motet	20h	2003-2004
1ère Année DEUG MIAS	Initiation à la Programmation en C	TD	D. Beauquier	32h	2003-2004
	Initiation à la Programmation en C	TP	D. Beauquier	32h	2003-2004
1ère Année IUT	Bases de données	TD	R. Laleau	12h	2005-2006
	Projet Php & Mysql	Projet	F.Semmak	20h	2005-2006
	Base de la Programmation en C	TD	P. Ciegelski	32h	2005-2006
	Bases de données	TD	R. Laleau	32h	2004-2005
2ème Année IUT	Système & Réseaux	TP	K. Verchinine	32h	2004-2005
Moniteurs	Représentations mentales & Motivation	TD	A. Finkel	8h	JAM 2005
2ème Année IUT	Motivation & Mémorisation	TD	A. Finkel	8h	2005-2006
Moniteurs	Émotions et Motivation	TD	A. Finkel	8h	JA 2006

FIG. 1 – Résumé chronologique des enseignements dispensés

Nous détaillons maintenant de manière chronologique le contenu de chaque enseignement par matière et par année.

1.1.1 En informatique :

J'ai effectué mes enseignements en informatique en tant que : Vacataire à l'INSA Toulouse durant l'année scolaire 2002-2003 et moniteur à l'université Paris XII Créteil de 2003 à 2006. Ma tutrice de monitorat est Madame Danièle Beauquier, professeur à l'université Paris XII. Ma première année de monitorat s'est déroulée à l'université Paris XII avec un public en DEUG MIAS 1ère année. Les deux autres années de monitorat ont étés effectuées à l'Institut Universitaire Technologique de Fontainebleau avec des étudiants de première et deuxième année.

1.1.2 Détail des enseignements en informatique par année et par matière.

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

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

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

Initiation à la Programmation en C :
- *Durée* : 32 heures de TD et 32 heures (eq. TD) de TP.
- *Public* : 2 groupes de 40 étudiants en première année de DEUG MIAS.
- *Responsable* : Danièle Beauquier : beauquier@univ-paris12

– *Description* : Ce module a pour but d'apprendre les bases de la programmation à travers le langage C à des étudiants qui n'avaient jamais programmé et étaient sans aucune connaissance en informatique. Les étudiants apprennent les principales notions de la programmation en informatique. En particulier, ils manipulent les notions de tableaux, itérations (boucles), conditions, chaînes de caractères et pointeurs.
– *Réalisation* : Site web pour les étudiants avec les sujets et corrigés des Travaux Dirigés et Travaux Pratiques. Aide à la préparation des sujets de Travaux Pratiques, Travaux Dirigés et du sujet d'examen.

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 lamanage SQL. Les étudiants abordent les concepts de clé primaire, clé étrangère, jointure naturelle, entité relation, requête, dépendance fonctionnelle, forme normale et normalisation.
– *Réalisation* : participation à l'élaboration des sujets de Travaux Pratiques, de Travaux Dirigés et du sujet d'examen.

Système et Réseaux :
– *Durée* : 32 heures (eq TD) de TP.
– *Public* : 2 groupes de 16 étudiants en seconde année d'IUT informatique.
– *Responsable* : Konstantin Verchinine : verko@capet.iut-fbleau.fr
– *Description* : Nous introduisons les concepts de système de fichiers, tube de communication, fork, socket. Ces éléments seront ensuite utilisés pour mieux comprendre les notions qui sont liées au 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 de mes Travaux Dirigés.

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

– *Description* : Après avoir appris les bases de la programmation en Php, les étudiants appliquent concrètement les notions de bases de données. Exemple : ils mettent en oeuvre un site web pour la gestion d'un site en ligne d'achat de livre, la gestion d'un site d'inscription à une conférence ou encore la gestion d'un vidéo club. Cela va de l'analyse du problème jusqu'à la réalisation, sous forme de projet, du site web.
– *Réalisation* : participation à l'élaboration du sujet, à l'encadrement des projet en TD et TP, et à la notation finale des projets lors de présentations orales.

1.1.3 En technique d'apprentissage.

J'ai eu l'occasion d'assister Alain Finkel lors de ses cours sur les techniques d'apprentissage destiné au public universitaire, pour aider les étudiants sur leurs motivations et leurs techniques de travail. Je suis actuellement inscrit au Diplôme Universitaire de l'École Supérieure de Cachan NTCA (Nouvelles Techniques Cognitives d'Apprentissage) pour parfaire ma formation dans ce domaine.

Assistant aux journées apprentissages de Marseille 2005 (JAM 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* : Dans un premier temps les moniteurs découvrent et explorent leurs propres représentations mentales. On s'aperçoit ainsi que chacun possède sa propre représentation mentale de notion aussi simple que le point en géométrie. Ensuite les moniteurs apprennent à expliciter une prise de décision anodine. Finalement ils découvrent comment motiver leurs élèves en se servant des techniques de prise de décision, d'explicitation et des notions apprises sur les représentations mentales.
– *Réalisation* : participation à l'élaboration de ces séances.

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

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

Assistant au journées apprentissages 2006 de Cachan (JA 2006).

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

1.1.4 Documents pédagogiques réalisés :

Le site web pour les étudiants de DEUG première année ainsi que les autres supports pédagogiques réalisés se trouvent à l'adresse suivante :

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

- 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.
- correction de copies d'examen des partiels sur machine de système.
- évaluation des projet de Php & Mysql
- réalisation des sujets de TD en base de la programmation en C.

1.2 Analyse et impressions.

1.2.1 Analyse :

Ma tutrice officielle est Danièle Beauquier, j'ai travaillé en collaboration en d'excellents termes avec Mme Beauquier lors de ma première année de monitorat à l'Université de Créteil (Paris XII). Cette collaboration m'a permis d'apprendre à organiser une séance de TD et de TP, mettre en place des contrôles de connaissance continus et de voir comment construire un examen de fin d'année. Lors de cette première année de monitorat, j'ai aussi découvert le déroulement de l'enseignement à l'université, avec les difficultés liées à l'organisation, la planification et au nombre d'étudiants. Ces difficultés sont propres à l'université et ont été surmontées dans d'excellentes conditions grâce à Mme Beauquier. La suite de mon monitorat s'est déroulée à l'IUT de Fontainebleau, où j'ai collaboré avec Régine Laleau et Farida Semak pour les bases de données, Patrick Ciegelski et Luc Hernandez pour la Base de la programmation et enfin avec Konstantin Verchinine et Selma Naboulsi pour le module système et réseaux. J'ai eu l'occasion de m'impliquer dans l'organisation des trois principales équipes de l'IUT. Lors de cette expérience je me suis aperçu que chacune de ces équipes avait son propre mode de fonctionnement. J'ai pu aussi voir les différentes organisations mises en place dans chacune de ces deux entités que sont l'université et l'IUT.

1.2.2 Impressions :

Ces expériences m'ont appris l'importance de la bonne ambiance, du dynamisme, et de la coopération entre les différents membres d'une équipe pédagogique, chose qui n'est pas évidente à mettre en oeuvre et qui dépend beaucoup de la personnalité propre de chacun et du responsable du module. J'ai aussi pu comparer sur le terrain les différences entre l'université Paris XII à Créteil, une grande structure, et l'IUT de Fontainebleau, une plus petite. Chacune de ces structures possédant ses propres avantages et inconvénients.

2 Activités de formation.

Impressions et suggestions année par année des différentes formations obligatoires et optionnelles proposées par le C.I.E.S. de Jussieu aux moniteurs.

2.1 Journées de formation en 1ère année.

2.1.1 Formation commune.

- *Durée* : 2 jours.
- *Descriptif* :
  - Première journée :
    - Structure de l'université .

    - Résultats de l'enquête nationale sur le devenir des moniteurs.
    - C.I.E.S structure et fonctionnement.
  - Seconde journée :
    - François Marchand : Motivations maturations psychologiques et problèmes de relations dans l'enseignement.
    - Technologie de la formation et communication et innovation dans l'enseignement.
- *Impressions* : Connaître le devenir des moniteurs, apprendre comment fonctionne l'université et le CIES sont des connaissances importantes dans la formation des futurs enseignants que sont les moniteurs. L'aspect psychologique est trop souvent oublié dans notre formation et l'intervention de M. Marchand était bien venue. Finalement l'idée de nous présenter les nouvelles technologies pour l'enseignement est très bonne. Malheureusement l'intervention n'était pas à la hauteur de mes espérances, ceci à cause de la manière dont le sujet fut traité.

2.1.2 Module : Les étudiants et nous

- *Animateur* : Hervé Raynaud
- *Durée* : 3 jours
- *Descriptif* : Cette formation est destinée aux Moniteurs qui ont connu des agrégés mauvais enseignants qui se défient de l'académisme didactique et qui aimeraient ne pas faire subir à leurs enfants les mauvais traitement qu'ils ont subis ! Ce stage est centrés sur l'observation et l'utilisation des registres émotionnels mis en jeu dans la communication pédagogique.
  Il connaît un franc succès chez les Moniteurs dans la moitié des CIES de France, en raison de l'impasse habituelle faite sur ce sujet "tabou". Il donne des raisons purement psychologiques à la fréquence des dépressions et des névroses d'angoisse en milieu enseignant, met en place les moyens de prévention des accidents psychologiques.
  Ce stage attaque les mêmes sujets que le stage "Pour sortir des recettes toutes faites", mais sous un autre angle nettement plus psychologisant. Les candidats stagiaires qui se savent dans une mauvaise passe psychologique ne doivent pas s'inscrire à ce stage - qui appelle un chat un chat - qu'après avoir consulté l'animateur, au moins par émail. Ce stage n'a rien d'une psychothérapie, même si l'on peut considérer qu'il cherche l'épanouissement personnel des enseignants chercheurs.
- *Impressions* : Pour moi cette formation fut très enrichissante, elle m'a permis de mieux me connaître au travers de différents tests de personnalité proposés par Hervé Raynaud. Ainsi une meilleur appréhension de ma relation avec les autres, de mon mode de vie, de ma personnalité. Cela m'a permis une remise en question constructive de mon attitude, de mon comportement quotidien et dans mon rôle d' enseignant. Cette formation m'a également apporté de nombreux points constructifs pour devenir un meilleur enseignant.

2.1.3 Modules Obligatoires.

- *Animateur* : Marie-Martine Paget & Felix Paoleti
- *Durée* : 2 jours
- *Description* : Comment donner un cours en informatique théorie (F. Paoleti) et pratique (M-M. Paget : TD sur les pointeurs en C). Comment Faire un exposé scientifique en informatique.
- *Impressions* : L'idée de nous apprendre à donner un cours est très bonne. Malheureusement à cause du calendrier ce module arrive trop tard, car pour la plupart d'entre nous, nous avions déjà effectué plus de la moitié de notre service d'enseignement. L'exposé scientifique quant à lui arrive selon moi trop tôt, car en début de thèse nous n'avons pas forcément de résultat à présenter. Je suggère donc de transformer cela en préparation d'exposé pour notre première conférence ce qui serait à mon avis plus réaliste et profitable pour tous.

2.2 Journées de formation en 2ème Année.

2.2.1 Formation commune (vendredi 13 Janvier 2006).

- *Durée* : 1 jour.
- *Descriptif* :

  - Patrick Vincelet : Éléments de base de la psychanalyse pour la compréhension des mécanismes de l'apprentissage de l'étudiant.
  - Palais de la découverte
- *Impressions* : Le point de vue psychologique abordé ici lors de la matinée entre à mon avis parfaitement dans la formation que le CIES doit apporter aux moniteurs. Par contre une plus grande interaction de la part des moniteurs serait souhaitable, ainsi ils pourraient partager leurs expériences et parfaire leur formation d'enseignant. La visite au palais de la découverte offre une ouverture sur la culture scientifique en général, aspect que je trouve essentiel dans la formation d'un moniteur.

2.2.2 Module : Raynaud 2

- *Animateur* : Hervé Raynaud
- *Durée* : 3 jours
- *Descriptif* : Tandis que le stage de première année s'attaquait au plus pressé - à savoir ne pas nuire aux étudiants - le stage de deuxième année serre les boulons de votre "vocation" d'enseignant chercheur.
  Après vous être demandé si vous étiez assez "solide" pour supporter cette activité passablement pathogène, le stage vous conduira à voir si vous êtes bien en accord, dans votre structure psychologique même, avec l'avenir que cette profession vous trace.
  La deuxième partie du stage se concentre sur les ressources que vous pouvez mettre en oeuvre pour mieux vous épanouir dans cette activité : gestion du temps, changement de comportement, actions de développement personnel ... ou sur l'utilisation de votre expérience de Moniteur à des fins différentes de la profession d'enseignant chercheur.
- *Impressions* : Après avoir suivi le premier module proposé par Hervé Raynaud, j'ai voulu poursuivre le travail sur ma réflexion personnelle commencé lors de ce premier module. Au travers d'exercices et d'échanges en petit groupe j'ai pu mieux comprendre mon fonctionnement. Cette compréhension de ma personnalité, en fonction de ma propre histoire, m'a permise de mieux percevoir mes motivations personnelles et d'améliorer mes relations avec les autres. Mieux se connaître permet à mon avis d'améliorer ses relations et ses attitudes avec le public auquel j'enseigne. Je recommande fortement ces formations qui m'ont étés extrêmement utiles lors de ma formation d'enseignant en m'ouvrant sur moi même et les autres. Je remercie Hervé Raynaud pour ses conseils et le CIES pour m'avoir permis d'assister à cette formation.

2.3 Journées de formation 3ème Année.

2.3.1 Formation commune (Lundi 31 Octobre 2006).

- *Durée* : 1 jour
- *Descriptif* :
  - Présentation du programme de bourse Marie Curie.
  - L'Association Bernard Gregory (ABG).
  - Visite du Muséum d'histoire naturelle.
- *Impressions* : La présentation des bourses post-doctorales existantes m'a permis de concrètement commencer à faire des dossiers de bourse pour l'éventualité d'un post-doc l'an prochain. Je trouve extrêmement pertinent d'avoir ce genre d'intervention et il me semble que proposer des ateliers pour aider les moniteurs à trouver les bourses existantes dans chaque domaine et constituer les dossiers peut être une formation fort utile pour un moniteur en dernière année. La visite du muséum d'histoire naturelle a enrichi ma culture générale et m'a beaucoup intéressée.

2.3.2 Modules Obligatoires.

- *Animateur* : Nicolas Sabouret
- *Durée* : 1 jour
- *Descriptif* : Mieux se préparer aux concours de l'enseignement en informatique.

– *Impressions* : Cette présentation jeune, dynamique et interactive des différentes démarches pour préparer une candidature CNRS ou maître de Conférence dans notre discipline, nous donne une bonne vision pour notre avenir proche en informatique et nous donne de précieux conseils pour se préparer au mieux à notre recrutement futur.

2.3.3 Diplôme Universitaire : NTCA

– *Animateur* : Alain Finkel
– *Durée* : 290 heures
– *Descriptif* : Nouvelles Techniques Cognitives d'Apprentissage. Cette formation répond à la demande de nombreux enseignants, formateurs et psychologues qui souhaitent mettre à jour leur pratique professionnelle en complétant leurs connaissances théoriques et pratiques en pédagogie. Objectifs de cette formation : Former les enseignants (et les enseignants en formation) et les autres professionnels de l'enseignement et de la formation aux Nouvelles Techniques Cognitives d'Apprentissages.
– *Impressions* : Grâce à cette formation j'ai acquis les compétences nécessaires afin de participer en tant qu'assistant aux TDs durant les JA 2006. Cette formation très complète qui se termine en Septembre 2006, m'a permis de devenir un meilleur pédagogue et d'approfondir ma réflexion sur les méthodes à utiliser pour donner un enseignement de qualité.

2.3.4 Journées Apprentissage 2006 à Cachan (JA 2006).

– *Animateur* : Alain Finkel
– *Durée* : 2 jours
– *Descriptif* : Le thème de ces journées était "Motivations et émotions pour les apprentissages" (`http://www.lsv.ens-cachan.fr/~finkel/ja2006`). But et objectif de ces deux journées : Former les enseignants (et les enseignants en formation) aux nouvelles techniques d'apprentissages.
  – La première journée intitulée "Bases théoriques sur les émotions et les motivations pour les apprentissages" sera constituée de présentations scientifiques.
  – Au cours de la deuxième journée intitulée "Formation pratique des enseignants" des exercices de mise en situation seront proposés.
– *Impressions* : J'ai participé à l'organisation de ces journées. J'ai encadré un groupe de TD lors de la seconde journée. Cette expérience fut très enrichissante et m'a permis de découvrir que la plupart des enseignants du supérieur n'avaient pas reçu de formation adaptée pour devenir enseignant.

3 Activités de Recherche.

3.1 Résumé.

Actuellement, dans nos sociétés modernes l'informatique est omniprésente. Ceci change nos modes de consommation et de communication. Lors de communications, certaines informations sensibles, tel le code confidentiel des cartes bancaires, circulent sur le réseau. Il serait souhaitable que ces informations ne tombent pas entre de mauvaises mains. Pour garantir un certain niveau de confidentialité, les protocoles de communication utilisent des algorithmes de chiffrement pour sécuriser les échanges de messages. Malheureusement cette méthode ne suffit pas pour garantir qu'une information confidentielle reste secrète. Tous les jours de nouvelles failles sont découvertes sur des protocoles cryptographiques. L'exploitation de telles failles entraîne une perte économique considérable, il faut alors retirer momentanément le système pour soit le corriger, soit le remplacer. Afin de garantir la sécurité des utilisateurs, il est donc primordial de vérifier qu'il n'existe pas d'attaques sur un protocole cryptographique avant sa mise en service.

En 1996, Lowe découvrit une attaque sur le protocole dit de Needham-Schroeder, 17 ans après sa publication. Ce célèbre exemple fit prendre conscience à la communauté scientifique qu'un protocole n'est pas forcément un échange de messages sûr, même si toutes les informations transmises sont cryptées. En raison de la conception même du protocole, des informations confidentielles peuvent donc être découvertes par un intrus bien que tous les messages soient cryptés par un chiffrement incassable. Depuis la découverte de cette faille, la vérification de protocoles cryptographiques s'est considérablement développée et ne porte plus uniquement sur l'étude des méthodes de chiffrement. La sécurité de ces protocoles n'est pas uniquement garantie par l'usage de méthode de chiffrement cryptographique mais aussi par une vérification formelle du protocole lui-même. La complexité des protocoles cryptographiques rend très difficile, même pour un spécialiste, de trouver "à la main" une attaque sur un protocole. L'attaque de Lowe fut découverte à l'aide d'un outil automatique de vérification de protocoles cryptographiques. Il est nécessaire d'automatiser la vérification des protocoles cryptographiques pour permettre une recherche systématique des attaques et pour qu'un utilisateur non expert puisse vérifier simplement un protocole.

Les premières approches formelles considéraient l'hypothèse de chiffrement parfait : le seul moyen pour déchiffrer un message chiffré est de connaître la clef de déchiffrement. Les fonctions de chiffrements sont alors vues comme des "boîtes noires" qui encapsulent les messages chiffrés. Cette hypothèse de chiffrement parfait a permis de trouver certaines attaques et donc de corriger des protocoles. Cependant, il existe des protocoles prouvés sûrs sous cette hypothèse, qui possèdent une attaque. Il est donc nécessaire d'affaiblir cette hypothèse, par exemple en considérant les théories équationnelles qui sont, soit explicitement utilisées dans le protocole lui-même, soit utilisées par la méthode de chiffrement employée. Ainsi un intrus est modélisé de façon plus précise et a plus de pouvoir pour essayer d'obtenir une information supposée secrète dans le protocole. Cela permet de vérifier d'une manière plus réaliste les protocoles.

La vérification de protocoles de télécommunications est un thème de recherche étudié depuis plusieurs années déjà au Laboratoire Spécification et Vérification (LSV) à l'ENS Cachan. Durant ma thèse au sein de l'équipe SECSI du LSV, j'ai travaillé sur l'affaiblissement de l'hypothèse du chiffrement parfait en augmentant le pouvoir de l'intrus. Pour cela, j'ai d'abord relevé dans les protocoles cryptographiques existants les propriétés utilisées pour chiffrer les messages par les algorithmes de chiffrement et aussi utilisés pour le déroulement même des protocoles. Grâce à cette étude préliminaire, publiée dans une revue internationale [CDL06], j'ai pu dégager les propriétés pertinentes à étudier pour pouvoir vérifier de manière plus sûre les protocoles cryptographiques. Je me suis ensuite focalisé sur l'étude plus précise d'une classe de propriétés algébriques utilisant un opérateur homomorphique. J'ai d'abord commencé à regarder comment modéliser un intrus dit *passif* en prenant en compte cette nouvelle classe de théorie équationnelle, ce qui à donné lieu à une publication dans la conférence internationale RTA 2005 [LLT05]. Un intrus passif est un intrus qui ne peut qu'écouter les messages échangés sur le réseau et essayer de déduire à partir de ces capacités déductives de nouvelles informations. Nous avons étendu ces résultat au cas où l'opérateur homomorphique est aussi l'opérateur de chiffrement, ce travail est en cours de soumission à un journal international. Une fois ce problème résolu j'ai regardé le cas de l'intrus dit *actif*, cet intrus peut lui aussi écouter et analyser les messages échangés lors de l'exécution normale d'un protocole mais il peut aussi jouer le protocole avec des participants honnêtes et se faire passer pour un participant honnête. Ce problème de l'intrus actif en considérant un opérateur homomorphique est beaucoup plus difficile que le cas de l'intrus passif. Nous l'avons récemment résolu dans le cadre d'un nombre borné de sessions lors d'un travail publié à ICALP 2006 [DLLT06]. Notons qu'il est connu que dans le cas d'un intrus actif, si nous ne bornons pas le nombre de sessions, le problème de vérification d'un protocole cryptographique même sans théorie équationnelle est indécidable.

3.2 Impressions sur mon expérience de moniteur.

L'équilibre entre enseignement et recherche est pour moi nécessaire au bon fonctionnement de la vie d'un enseignant chercheur. Cette répartition entre diffusion de l'information lors de séance d'enseignement permet de redonner de l'énergie au chercheur. Réciproquement la recherche permet de donner de nouvelles perspectives à l'enseignement. Cette complémentarité m'a permis de me motiver quand la recherche stagnait et de pouvoir aborder avec un esprit plus ouvert mes travaux de recherches grâce aux séances d'enseignement.

3.3 Sentiment sur le dispositif actuel.

Le système français actuel offre la possibilité aux doctorants, grâce au monitorat, de pouvoir effectuer à la fois le travail de recherche demandé par la thèse et de goûter au plaisir de l'enseignement dans le supérieur. Je pense que le volume horaire de 64 heures de TD par an est un bon équilibre pour allier travail de recherche et enseignement.

Par contre je déplore que, pour la plupart d'entre nous, nous commencions à enseigner sans aucune formation à ce propos. Il serait souhaitable de diminuer le service d'enseignement d'un moniteur lors de la première année, et de faire commencer les enseignements des moniteurs uniquement au second semestre. Il serait alors possible de consacrer ces heures à une formation pédagogique concrète et spécifique à chaque discipline aux futurs enseignants du supérieur, ce qui est ,à mon avis, le rôle du CIES.

Références

[CDL06] Véronique Cortier, Stéphanie Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1) :1–43, 2006.

[DLLT06] Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis in presence of a homomorphism operator and *exclusive or*. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06)*, Lecture Notes in Computer Science, Venice, Italy, July 2006. Springer. To appear.

[LLT05] Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Intruder deduction for AC-like equational theories with homomorphisms. In Jürgen Giesl, editor, *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *Lecture Notes in Computer Science*, pages 308–322, Nara, Japan, April 2005. Springer.