Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 15 septembre 2009

Présents: Didier Alquié, Sandrine Blazy, Christophe Chabot (invité), Sylvain Duquesne, Lionel Fourquaux, Pierre Loidreau, David Lubicz (invité), Soline Renner.

Rôle du comité

- Tout le monde doit être au courant des problèmes en cours et donc être à même d'aider à les résoudre.
- Soulever et gérer les problèmes qui apparaissent en cours d'année (sans toutefois attendre les réunions du comité pour soulever un problème).
- Répartir certaines tâches, comme par exemple la recherche des stages de M2.
- Sur le plus long terme, le but est d'encourager et d'accompagner l'évolution de la formation.

Fonctionnement du comité

- Il est constitué de 2 représentants de l'UFR de maths (Sylvain Duquesne et Lionel Fourquaux), 2 représentants du CELAR (Didier Alquié et Pierre Loidreau), un représentant de l'IFSIC (Sandrine Blazy, responsable de la spécialité SSI du Master d'informatique), un représentant des étudiants de M2 (Soline Renner) et un représentant des étudiants de M1 (non désigné à ce jour). Suivant l'ordre du jour, peuvent s'y ajouter des invités.
- Il se réunit fin septembre, début janvier, fin avril et si besoin fin juin.
- Un compte rendu de chaque réunion est mis en ligne (en accès restreint) sur la page de la formation.

Présentation rapide de la formation

Formation dans le cadre de la collaboration CELAR/IRMAR.
Son objectif est de former des ingénieurs mathématiciens spécialisés dans les technologies de l'information, plus précisément sur les aspects codes et cryptographie. L'essentiel des débouchés se trouve donc au niveau des équipes de R&D du secteur privé, même si des débouchés plus académiques (doctorats) restent possibles.
Cette formation s'adresse en priorité à des étudiants ayant une licence de Maths, ce qui implique un rattrapage en informatique et plus particulièrement en programmation. La maquette originale de 2008 a été légèrement modifiée dans ce sens.
La prochaine occasion de modifier la formation est cette année (mi-parcours). Les modifications seront effectives pour la rentrée 2010. La suivante sera une nouvelle habilitation entrant en vigueur pour la rentrée 2012.

Présentation et bilan du M1

- Les cours « algèbre de base », « théorie des nombres » et « algèbre commutative et géométrie algébrique » n'ont pas posé de problèmes particuliers.
- Le programme de « algorithmique de base » a été mis à jour pour éviter les redondances avec les autres cours. Les TD et TP seront plus en relation avec le cours que l'an dernier.
- Le programme de « Probabilités et statistiques pour l'ingénieur » est inadapté. La partie proba a déjà été faite en L et la partie stat est très réduite. Les étudiants ne voient pas l'utilité d'un tel module dans la formation. Sylvain Duquesne va rencontrer Bernard Delyon pour discuter du contenu et de l'ajout d'exemples/applications en cryptographie.

- Le cours « Pratique de logiciels scientifiques », inadapté selon l'avis de tous, est remplacé par un cours accéléré de C.
- Les TP de « Théorie de l'information, codage et cryptographie » n'ont pas bénéficié d'un suivi suffisant. Ce sera corrigé cette année. Pour permettre aux autres étudiants du Master de maths (en particulier les magistériens) de suivre ce module en surnuméraire, il est envisagé de le séparer en un module de théorie de l'information, codage de 3 ECTS et un module de cryptographie de 6 ECTS. Il ne serait d'ailleurs pas absurde que la première partie fasse 6 ECTS également.
- Le module « Optimisation discrète et recherche opérationnelle » paraît inadapté et inutile aux étudiants. Une possibilité est de voir avec Fabrice Mahé si son cours peut être adapté pour tenir compte de la formation cryptographie, une autre est de le remplacer par le module « logique, théorie des modèles, complexité », bien que la partie théorie des modèles paraisse peu adaptée à la formation. Sylvain Duquesne s'occupe de ce problème.
- L'anglais pose également des problèmes car il est déconnecté de la formation. S'agissant d'un enseignement à l'échelle de l'université, le problème doit être abordé en conseil d'UFR. On remarque toutefois que les étudiants sont peu enclins à accepter des références bibliographiques en anglais.
- Les étudiants déplorent l'absence d'un enseignant référent pour les questions de programmation. L'enseignant responsable du cours « Programmation C » (Christophe Chabot cette année) peut jouer ce rôle.
- Sylvain Duquesne se charge de demander à ce que les étudiants de M1 aient accès à la bibliothèque de l'IRMAR.
- Pour les projets tutorés, les étudiants souhaitent être davantage suivis/accompagnés dans leur travail. Par ailleurs, ils souhaitent que la présentation finale de leur travail soit plus formelle (jury).

Effectifs 2009-2010

- En M1, pas encore de chiffres exacts, à priori 9 dont au moins 5 extérieurs. Il faut donc faire plus de pub en licence, portes ouvertes, salons étudiants, …
  Pour l'instant ils paraissent plus nombreux en cours (ALBA, Programmation C).
- En M2, 11 inscrits dont 3 non issus du M1.

Page Web de la formation

- Faire apparaître le partenariat avec CELAR
- Améliorer la présentation de la cryptographie et des débouchés (cf page de Bordeaux)
- Énoncer les objectifs et mettre en avant les points forts

Pierre Loidreau fait le point

Modules optionnels du M2

- Un seul étudiant de l'IFSIC a choisi eVote. Le module n'est donc pas censé ouvrir. Comme il y a entre 4 et 6 étudiants de maths qui l'ont choisi, Sylvain Duquesne et Sandrine Blazy vont essayer de le faire ouvrir quand même, quitte à ce que ce soit l'UFR de maths qui paye l'intervenant (sous réserve que l'UFR de maths soit d'accord bien sûr).
- Les cours de l'IFSIC ont lieu en grande partie au semestre 3, ce qui surcharge l'emploi du temps des étudiants de la formation. De plus la présence de « Cartes à puces » en S4 empêche les étudiants de l'IFSIC de le prendre autrement qu'en surnuméraire. Une solution plus simple doit être trouvée en collaboration avec l'IFSIC.
- Le module « Environnement économique et juridique de l'entreprise » doit passer en S4 pour alléger l'emploi du temps de S3.

Mutualisation avec l'IFSIC

- Une page web sécurité à Rennes existe déjà mais est vide. L'idée est d'avoir une page chapeau avec une présentation de la sécurité en général, une explication des spécificités de chacune des 2 formations, un lien vers chacune des formations et éventuellement quelques informations communes (offres de stages, interventions de professionnels, anciens élèves).
- L'an dernier, avait été avancée l'idée de publicité dans des revues spécialisées. L'impact paraît toutefois limité. Pierre Loidreau se renseigne avant un abandon définitif de l'idée.
- Il doit être possible de mutualiser les interventions de professionnels entre les 2 formations.
- L'association des étudiants pourrait éventuellement se faire avec les étudiants de SSI.

Divers

- Création de listes de diffusion pour les étudiants de M1 et de M2
- L'objectif en anglais en M2 est le passage du CLES niveau 2 (le document transmis par la responsable de l'anglais est disponible sur la page de la formation). On se demande pourquoi une préparation au TOEIC n'est pas plutôt envisagée comme dans les écoles d'ingénieur.
- David Lubicz encourage les étudiants à créer une association des étudiants afin de garder contact avec eux et qu'ils puissent garder contact entre eux par la suite, comme cela se fait dans les écoles d'ingénieurs. Il se renseigne pour savoir si l'université peut héberger une page web. La démarche est simple et peu contraignante.
- Il faudrait apprendre aux étudiants à rédiger un CV, passer un entretien, chercher un emploi. Cela peut se faire via des interventions (DRH, ANPE), peut être via l'école doctorale. Il y a également un module dans ce sens à l'IFSIC au second semestre. Peut être que les étudiants pourraient y assister (en espérant qu'il n'y ait pas de problèmes d'effectifs).
- Le développement d'une bibliothèque de cryptographie par les étudiants serait une bonne chose pédagogiquement. A priori, le but ne serait pas d'en faire un produit diffusable et utilisable largement.
- Des moyens financiers seraient appréciables pour les interventions de professionnels, pouvoir ouvrir des modules à faibles effectifs ou nouveaux, dédommager l'IFSIC ou Supelec pour les cours donnés aux étudiants de la formation. 2 sources de financement sont possibles : demander à nos contacts industriels de flécher leur taxe d'apprentissage vers l'UFR de Maths plutôt que vers la chambre de commerce et d'industrie et l'ouverture de la formation à la formation continue. Il n'est pas clair que ce soit simple à mettre en pratique. Sylvain Duquesne s'occupe de ce point.

Stages

- Les membres du CELAR et Sylvain Duquesne suscitent des propositions de stage auprès de leurs contacts industriels.
- Sylvain Duquesne fait suivre ces offres et d'autres non sollicitées aux étudiants qui prennent alors contact par eux même avec les entreprises. Les étudiants peuvent bien sûr également chercher de leur coté.
- Une réunion spécifique sera organisée pour traiter le problème d'éventuels étudiants qui rencontreraient des difficultés à trouver un stage.