Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 4 octobre 2017

Présents: Angèle Bossuat (M2 l'an dernier), Delphine Boucher, Patrick Derbez, Sylvain Duquesne, Eric Gousset, Elisa Lorenzo-Garcia, Sarah Paardekooper (M1 l'an dernier), Christophe Ritzenthaler.
Absents : Pierre Loidreau, Kelly Resche (remplacée par Eric Gousset)

Bilan du second semestre de M2

- « Sécurité des implémentations »
  AB : Très contents. Tout le monde a trouvé ça bien mais avec un poly ce serait mieux. Dommage de ne faire que des simulations et de ne pas avoir de vrai matériel. Il y en aura cette année.
- « Environnement économique et juridique de l'entreprise »
  AB : Intéressant sauf pour les étudiants étrangers. Un peu trop brouillon, part un peu dans tous les sens car les étudiants sont novices en droit et posent beaucoup de questions.
  SD : ce cours n'existe plus dans la formation mais il devrait quand même y avoir une intervention de 3h sur ce thème commune avec le master cybersécurité.
- « Théorie algorithmique des nombres »
  AB: Cours et examen difficiles.
  CR/SD : On est au courant mais c'est normal et assumé.
- « Sécurité prouvée »
  AB : Très bien mais la partie preuve était un peu dense.
  SD : Il n'y a plus de preuves de sécurité cette année, seulement des protocoles.

Les autres modules ont déjà été traités lors du précédent comité.

Bilan des stages de M2

SD : Encore une fois, les stages se sont globalement très bien passés sauf une entreprise qui a été très problématique (entraînant un abandon) et même totalement hors-la-loi. Au moment des soutenances, 9 des 12 étudiants ayant validé leur année ont trouvé un emploi ou une thèse. Les 3 autres n'avaient pas commencé à chercher.

Bilan du second semestre de M1

SP : C'est dommage de pas faire de théorie des nombres.
SD : C'est vrai, c'est à cause de la transition entre les accréditations et on ne pouvait rien y faire car il est maintenant au second semestre et les étudiants de M2 ne sont pas disponibles tout le semestre.

- « Algèbre commutative et géométrie algébrique (ACGA)»
  SP: TP très bien. Il y a eu des créneaux de 4h de cours de suite et c'est trop. Globalement trop de contenu en trop peu de temps.
  SD : La partie AG a maintenant disparue du master
- « Complexité (LTMC1)»
  SP: intéressant, difficile à suivre sans le poly. Pas assez de complexité
  SD : C'est comme les années précédentes. Le volume horaire a été augmenté.
- « Codes correcteurs (COCO)»
  SP: Très bien, tout le monde est très content et remercie **DB**
- « Cryptographie »
  SP: Très bien. Trop rapide sur la fin du cours (signatures, PKI). Attention aux devoirs pendant les vacances d'été car tout le monde n'est pas disponible surtout ceux qui vont en Allemagne.
  SD : Ce sera envoyé plus tôt cette année et ça n'a de toute façons aucun sens pour les doubles diplômes.

- « Projet tutoré»
  SP: Dommage de pas avoir de remarque ou d'avis sur les choses à améliorer. Trop libre. Ce serait bien d'avoir des dates limites intermédiaires et une présentation plus approfondie des sujets.
- « Anglais»
  SP: cours sur les sujets d'actualités pas très intéressant. Par contre le PEP (projet) l'est beaucoup plus car les étudiants choisissent le sujet..

  Bilan global : 24 étudiants ont suivi le parcours, 20 passent en M2

Parrainage du master

Le master est parrainé par l'entreprise Amossys. Une cérémonie de lancement officiel de ce parrainage a eu lieu le 10 octobre 2016. Kelly Resche, la marraine, est en congés en ce moment et est remplacée par Eric Gousset, nouvellement arrivé chez Amossys.
Les étudiants n'ont pas eu de retour sur leurs candidatures aux stages de cette année ce qui est regrettable. Cette année une intervention sur l'évaluation est encore prévue et Amossys fera suivre ses offres de stage. **EG** interroge sur la pertinence de proposer des stages sur des sujets hors crypto. **SD** répond qu'au contraire c'est une très bonne chose tant que ca reste dans le domaine de la sécurité. Il rappelle que le stage fait partie de la formation au sens où les étudiants sont censés y apprendre de nouvelles choses et y développer de nouvelles compétences. Il rappelle également que les étudiants du master sont particulièrement appréciés pour leur capacité d'adaptation et leur faculté à apprendre vite.
L'an dernier il avait aussi été question qu'Amossys propose des sujet de projets tutorés mais ce n'est pas allé plus loin. A relancer cette année.
Il est également envisagé une cérémonie de remise de diplômes en Novembre comme l'ISTIC. Cela pourrait être couplé avec l'intervention sur l'évaluation mais il faut trouver une place dans l'emploi du temps et surtout il faut trouver un créneau où le maximum de personnes peuvent venir. L'ISTIC fait ca le samedi.

Point sur la rentrée

Cette année la sélection se fait en M1, 150 candidatures dont 17 de Rennes, 8 du périmètre CHL, 34 de France et 61 via Campus France. 32 ont été acceptés (+10 sur Campus France) et finalement 21 inscrits (+0 Campus France). L'extrême maximum est de 24 car les salles de TP ont 20 à 24 places.
En M2, il y avait encore une sélection à titre transitoire. 41 candidatures + 8 Campus France dont 25 de Rennes, 1 du périmètre CHL, 11 d'ailleurs en France. 23 acceptés ont été acceptés (dont 5 n'ayant pas suivi le M1) + 1 Campus France (bourse CHL). L'effectif final est de 19 étudiants (dont 2 n'ayant pas suivi le M1) + 5 en Allemagne. 2 étudiants sont inscrits dans le parcours recherche.

Il y a eu des soucis d'emploi du temps en ce début d'année car l'ISTIC a placé certains cours très tard. Il y a également des problèmes d'effectifs dans les cours d'info (RCS en particulier). **PD** demande si on ne peut pas envisager une forme de filtre pour ce module car il est obligatoire dans le parcours Cyber. Ce n'est peut être pas la peine d'aller jusque là car il y aura moins d'étudiants l'an prochain (3 choix d'options au lieu de 4 et moins d'étudiants dans le master). **SD** insistera en plus lors de la réunion de rentrée sur le fait que c'est un cours qui demande de déjà bien maîtriser la programmation.
Le plus gros problème est venu du module de sécurité des données. C'est un cours du master SIF (Recherche en informatique) avec lequel nous avons un partenariat. Il s'est avéré que ce cours était en fait géré par Supelec qui a également un partenariat avec le master SIF mais il n'y a pas de transitivité. Pour cette année, Supelec accepte que les étudiants suivent le module mais ne les évaluera pas. L'évaluation sera faite par **SD** et Caroline Fontaine (intervenante dans le cours) sur la base d'un rapport sur un article de recherche sur les thématiques du cours. **SD** reprendra les discussions de zéro concernant ce cours pour les années à venir.