Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 3 octobre 2016

Présents: Delphine Boucher, Sylvain Duquesne, Pierre Loidreau, Angèle Bossuat (M1 l'an dernier), Christophe Ritzenthaler.
Absents : Pierre Alain Fouque, Xavier Caruso, Mickael Sagliano (M2 l'an dernier)
Invitée : Kelly Resche

Le master va être parrainé par l'entreprise Amossys qui prend régulièrement des stagiaires (et en général les recrute). Une cérémonie de lancement officiel de ce parrainage aura lieu lundi 10 octobre. D'autres actions seront organisées pendant l'année (intervention sur l'évaluation crypto, remise de diplômes, …). Il est proposé, et accepté, que la marraine, Kelly Resche, intègre le comité de pilotage afin d'apporter un regard extérieur sur la formation.

Bilan du second semestre de M1

AB : globalement plus intéressant que le premier.

- « Algèbre commutative et géométrie algébrique (ACGA)»
  AB : Difficultés importantes dans ce module liées à la fois à sa difficulté intrinsèque, au fait d'être mélangés avec des magistériens et à la personnalité de l'enseignant. L'examen était loin de ce qui avait été fait en TD. Globalement, ce module a plombé les moyennes. Par contre les TP étaient très bien et ont beaucoup aidé à comprendre les bases de Groebner.
  SD : Pas facile de s'adapter aux 2 publics. Un TD spécifique aux étudiants de crypto a été crée afin d'améliorer les choses et a quand même permis d'avoir plus d'explications mais ce n'est visiblement pas suffisant.
- « Complexité (LTMC1)»
  AB: Pas assez de complexité, pas assez de TD. Des DM ce serait pas mal pour que les étudiants puissent travailler concrètement.
  SD : C'est un retour récurrent. Le volume horaire de ce cours va passer de 24 à 32h à partir de l'an prochain.
- « Codes correcteurs (COCO)»
  AB : ♥♥♥. Très intéressant et très bien. examen un peu long.
  DB: L'examen long est un choix par contre un peu trop de calculs.
- « Cryptographie »
  AB : ♥♥♥. Ce serait bien d'avoir plutôt des TP en C. Bon enchaînement CM/TD/TP la même semaine. Examen trop long.
  SD : Pour l'examen, c'est voulu aussi. Pour les TP en C, personne n'a malheureusement les compétences nécessaires à l'UFR.
  PL : Dommage ce serait bien
- « Projet tutoré»
  AB : Pas très tutoré. Ce serait bien d'avoir plus de dates limites pour poser des jalons dans l'avancement des projets. Certains y ont passé beaucoup de temps et d'autre moins.
  SD : C'est vrai que ce n'est pas très tutoré et je le regrette mais il n'y a pas eu de sollicitations ni de demandes d'aide, de conseils ou d'avis.
- « Anglais»
  AB : problème d'organisation: il manquait un bout de sujet à l'examen. Problème de contenu des sujets étudiés qui sont liés au maths mais pas à la crypto. Du coup ca n'apporte rien d'utile en terme de vocabulaire technique et autant travailler sur des vrais sujets d'ouverture.

  Bilan global : 19 étudiants ont suivi le parcours, 14 passent en M2

Sont également évoqués les problèmes rencontrés en début de M2 comme l'absence des

enseignants de SRI ou le fait que le cours de courbes algébriques soit effectué en anglais difficile à suivre pour certains (cumule de la difficulté de la langue et technique). Une alternative pourrait être de passer à des TD en français mais de garder les cours en anglais car c'est quand même formateur et surtout ca devient obligatoire l'an prochain dans toutes les formations d'avoir un module en anglais.
Ce serait bien aussi d'avoir accès à une formation au latex (maths et multimédia en L3 en surnuméraire par exemple)

Bilan du second semestre de M2
Mickael Sagliano travaillant maintenant à Mulhouse n'a pas pu venir. Voici toutefois son retour écrit

- « Sécurité des implémentations »
  Prof très bien et cours bien construits. TD/TP peut-être un peu difficiles mais bien dans l'ensemble. Projets intéressants, idée à garder.
- « Environnement économique et juridique de l'entreprise »
  Prof excellente, elle arrive à nous faire nous intéresser à un domaine que l'on n'aimait pas plus que ça au départ. Cours interactifs, tout le monde participe, c'est vraiment une bonne idée. Le format du cours est bon aussi, plus long ce ne serait plus forcément aussi bien.
- « Théorie algorithmique des nombres »
  Comme d'habitude, prof super mais cours compliqués dans l'ensemble. Beaucoup de notions vues sur très peu de temps de cours, cela mériterait un peu plus de temps (même si l'on sait que ce semestre est particulièrement écourté par le stage). TD très bien aussi, le roulement pour passer au tableau est toujours une bonne idée.
- « Sécurité prouvée »
  Première partie du cours géniale, prof vivant et faisant beaucoup participer, TD/TP super. Deuxième partie bien plus difficile et beaucoup plus « molle », très difficile de tenir 2h en tout début ou toute fin de journée.

SD : Encore une fois, les stages se sont globalement très bien passés sauf 1 et 1 autre qui n'a pas trouvé de stage. Les 12 étudiants assidus ont validé leur année (1 absent). Au 1er octobre, 3 ont trouvé un emploi, 2 sont en thèse, 2 ou 3 ont des difficultés et les autres sont en bonne voie (plusieurs entretiens).

Point sur la rentrée

Encore pas mal de dossiers pour le M2 dont une majorité d'étrangers et quasiment tous réorientés en M1.
17 étudiants inscrits en M2 cette année dont 2 sont à Karlsruhe dans le cadre du double diplôme (14 viennent du M1, 1 bourse Lebesgue venant de Lille, 1 enseignant en formation continue, 1 redoublant, personne dans le parcours recherche).
Autour de 28 étudiants en M1 mais plutôt une vingtaine de présents en pratique.

Habilitation 2017

Une proposition de maquette est présentée (cf ci dessous) pour les prochaines années avec peu de changements : essentiellement des augmentations de volume horaire là où des manques avaient été relevés lors des précédentes réunions de ce comité et de nouvelles options de M2 partagées avec le M2 SSI. Une discussion s'engage sur l'intérêt de conserver le module « Environnement économique et juridique de l'entreprise » alors que des modules qui semblent fondamentaux comme « sécurité prouvée » sont optionnels. Il est décidé de le supprimer et de le remplacer par un 3ème choix d'option. Les aspects propriété intellectuelle pourraient être couverts par une intervention du SATT ouest valorisation sur les brevet.

Mathématiques de l'information, Cryptographie

Semestre 7

- **Algèbre de base** (8 ECTS/coef 6, mutualisé avec le parcours maths fonda, 36CM/36TD/6TP)
- **Algorithmique de base** (6 ECTS, non mutualisé, 24CM/24TD/12TP)
- **Probabilités pour la théorie de l'information** (6 ECTS, non mutualisé, 30CM/30TD)
- **Programmation Scientifique 1** (6 ECTS, mutualisé avec le M1 modélisation, 18CM/12TD/18TP)
- **Architecture, systèmes, réseaux** (4 ECTS, non mutualisé, 18CM/18TP)
- **Réussir son insertion professionnelle** (0 ECTS, assuré par le SOIE, 10TD)

Semestre 8

- **Algèbre commutative et géométrie algébrique** (6 ECTS, mutualisé avec maths fonda, 24CM/24TD/6TP)
- **Codes correcteurs** (6 ECTS, mutualisé avec le parcours maths fonda, 24CM/16TD/12TP)
- **Cryptographie** (6 ECTS, non mutualisé, 24CM/16TD/16TP)
- **Projet tutoré** (6 ECTS, non mutualisé)
- **Complexité** (3 ECTS, mutualisé avec le parcours maths fonda, 16CM/16TD)
- **Anglais** (3 ECTS, 30TD)

Semestre 9

- **Théorie des nombres** (6 ECTS, mutualisé avec le M1 Maths, 24CM/24TD/6TP)
- **Programmation 1** (6 ECTS, mutualisé avec L3 Mention informatique parcours MIAGE, 32TD/22TP)
- **Sécurité des réseaux informatiques** (3 ECTS, mutualisé avec M2 Mention Informatique parcours « Sécurité informatique », 16CM/4TD/12TP)
- **Courbes algébriques** (3 ECTS, non mutualisé, 12CM/12TD)
- **Courbes elliptiques pour la cryptographie** (3 ECTS, non mutualisé, 12CM/8TD/8TP)
- **Réseaux euclidiens en cryptographie** (3 ECTS, non mutualisé, 20CM/16TD/2TP)
- **Spécialisation en cryptographie 1** (3 ECTS, cf ci dessous)
- **Anglais** (3 ECTS, 30TD)
- **Réussir son insertion professionnelle** (obligatoire sauf en recherche, 0 ECTS, assuré par le SOIE, 10TD)
- **Interventions de professionnels** (0 ECTS, 10TD)

Semestre 10

- **Théorie algorithmique des nombres pour la cryptographie** (3 ECTS, non mutualisé, 16CM/12TD/6TP)
- **Sécurité des implémentations** (3 ECTS, mutualisé avec M2 Mention Informatique parcours « Sécurité informatique », ISTIC, 16CM/16TD)
- **Environnement économique et juridique de l'entreprise** (3 ECTS, non mutualisé, 12CM/12TD)
- **Spécialisation en cryptographie 2** (3 ECTS, cf ci dessous)
- **Stage** (18 ECTS)

Spécialisation en cryptographie 1 et 2

- **Cryptographie quantique** (non mutualisé, 16CM/16TD)
- **Cryptographie avancée** (mutualisé avec M2 Mention Informatique parcours « Recherche», 20CM)
- **Sécurité prouvée** (mutualisé avec M2 Mention Informatique parcours « Sécurité informatique», 20CM)
- **C++, les bases** (mutualisé avec le M2 modélisation, 12CM/12TP)
- **Programmation parallèle et sur GPU** (mutualisé avec le M2 modélisation, 12CM/16TP)
- **Sécurité des données** (mutualisé avec M2 Mention Informatique parcours « Recherche», 20CM)
- **Hacking** (mutualisé avec M2 Mention Informatique parcours « Sécurité informatique», 16CM/16TP)

En M2, il existe un variante orientée recherche très sélective (une place par an) dans laquelle
- en S9, Théorie des nombres (6), Programmation 1 (6), Sécurité des réseaux informatiques (3) et Spécialisation en cryptographie 1 (3) sont remplacés par 2 modules d'Algèbre-Géométrie (2x6) et le séminaire (6) du parcours recherche du M2 maths-fonda.
- en S10 Sécurité des implémentations (3), Environnement économique et juridique de l'entreprise (3) et Stage (18) sont remplacés par Cryptographie quantique (3), un module d'Algèbre-Géométrie (6) et le mémoire (15) du parcours recherche du M2 maths-fonda