Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 5 octobre 2012

Présents: Delphine Boucher, Xavier Caruso, Sylvain Duquesne, Cécilia Gallais (M2 l'an dernier), Pierre Loidreau, Kelly Resche (M1 l'an dernier)

Invité : David Lubicz

Il y a eu des changements dans la composition du comité. Pierre Alain Fouque ayant remplacé Sandrine Blazy pour le master SSI, il la remplace aussi ici. Antoine Chambert Loir est parti et Xavier Caruso et Delphine Boucher arrivent.

Bilan du second semestre de M1

- « Algèbre commutative et géométrie algébrique (AGCA)»
  KR : bien, utile, difficulté correcte, certaines notions comme les résultants n'ont pas été abordées alors qu'elles sont utiles en M2.
  SD : le problème des résultants est déjà remonté par J. Sebag et est déjà réglé.
- « Logique, Théorie des modèles et Complexité (LTMC) »
  KR : bien fait, intéressant, pas assez d'exercice en complexité
  SD : même problème que l'an passé dû à un trop faible volume horaire. On va voir comment ca se passe cette année avec la scission de la logique et le changement d'intervenant (Dimitri Petritis)
- « Théorie de l'information, codage et cryptographie (THIC)»
  KR : théorie de l'information bof, erreurs, sinon TB
  SD/PL/DB : La partie théorie de l'information est maintenant séparée et bénéficiera donc de plus de temps. De même pour les codes correcteurs.
- « Projet tutoré»
  KR : OK, meme l'anglais (uen tous cas pour la partie écrite). Pas de souci d'accompagnement
- « Anglais»
  KR : OK car ca se passe toujours TB avec Nicolas André. Dommage qu'il n'y ait pas eu des groupes de niveau (il y en a cette année et c'est bien)
- Bilan global : 11 étudiants ont suivi le parcours, 8 sont reçus et passent en M2

Bilan du second semestre de M2

- « Cartes à puces »
  CG : cours intéressant, beaucoup d'informations mais il insiste sur ce qui est important. Méthode d'évaluation (lecture d'articles) TB.
- « Codes correcteurs »
  CG : bien
  l'intervenant a laissé les TD et une partie des cours à un thésard. SD a laissé faire car les retours des années passées sur cet intervenant ne sont pas mirobolants. Une discussion s'engage sur le contenu de ce cours et si il ne faudrait pas plus les y préparer pendant le cours de codes de M1. A priori ça relève plus du nouveau cours de théorie de l'information et on avisera donc quand celui ci aura eu lieu.
- « Stages »
  CG tous plutôt bien encadrés, contents.
  Pas de retours négatifs sur l'adéquation enseignements/stage malgré le fait que plusieurs stages étaient très peu crypto.

  Globalement pas assez de temps pour approfondir mais sinon, TB

Association des anciens étudiants

Le format facebook ne semble pas le mieux adapté (plusieurs anciens n'y sont pas, en particulier la première promo, la situation professionnelle n'apparait pas). **KR** indique qu'elle a lancé un forum et du coup l'idée d'une page hébergé par l'université refait surface. **DL** se rerenseigne à ce sujet.
Il semble important que les adresses mails et les situations professionnelles soient à jour.
PL évoque l'idée d'un mail Rennes 1 que les étudiants garderaient à vie (genre m4x.org).
D'autre part, une demande de subvention raisonnable au CEVU (1000-2000€), sera probablement acceptée. Ça permettra d'organiser plus facilement des rencontres entre anciens, quitte à avoir un ou 2 invités pour faire une conférence.

Point sur la rentrée

Encore pas mal de dossiers pour le M2 dont une majorité d'étrangers.
10 étudiants en M2 cette année (8 venant du M1, 1 du M2R de Strasbourg et un d'un Master de crypto russe) et une bonne vingtaine en M1.

Avenir de la formation (Master à faible effectif)

Autant du coté de l'université que du coté du ministère, il y a des attaques sur les Master à faible effectif (moins de 15 selon le CEVU). Ce master tourne à une dizaine d'étudiants et c'est un bon compromis en terme d'insertion professionnelle. Il n'y a pour l'instant rien d'urgent, car on devrait être protégé par, la jeunesse de la formation et son coté « à la mode ». Il semble toutefois important de discuter dès maintenant des alternatives qui s'offrent à nous.

3 possibilités se dégagent

- Faire un master commun avec le master SSI
  Avantages : déjà pas mal de synergies.
  Inconvénient : risque de perdre la spécificité (master pro fortement orienté maths) du Master en se retrouvant dans une configuration similaire à tous les autres master crypto de France.
- Faire un Master commun avec le master recherche de maths
  Avantages : soutenue par les collègues de l'UFR, permet d'ouvrir une possibilité officielle de parcours crypto/recherche (avec objectif thèse académique), en particulier pour les élèves de l'ENS
  Inconvénients : risque de perte d'autonomie, dommage de se refermer sur les maths alors que l'objectif initial était justement de s'ouvrir, en particulier en termes de débouchés.
- Lutter pour maintenir la formation telle qu'elle est
  Avantages : permet de garder l'indépendance et la philosophie initiale de la formation.
  Inconvénients : ça ne résout pas vraiment le problème et il faut donc falloir convaincre (la taxe d'apprentissage peut être un argument si ça se confirme qu'on en récupère grâce au master crypto)

Le consensus qui ressort s'oriente vers la 3ème solution. Toutefois, il serait bon d'imaginer une possibilité de parcours crypto/recherche contenant par exemple les cours de crypto du Master crypto et ceux d'Algèbre du master de maths.