Compte rendu de la réunion du conseil de parcours du Master de cryptographie du 29 septembre 2025

Présents: Gianira Alfarano, Arthur Baudy (M1 l'an dernier), Sylvain Duquesne, Mathieu Goessens, Alban Perreaux (M2 l'an dernier)
Absents : Pierre Loidreau, Marion Videau

Bilan du second semestre de M1

AB : le second semestre a été largement plus positif que le premier. L'emploi du temps est plus condensé et le contenu répondait plus attentes.

- « Codes correcteurs»
  AB : plutot bons retours, un peu livré à eux-mêmes en TP où l'intervenant attend les sollicitations
  SD : les retours de l'an dernier semblent avoir été pris en compte ou en tous cas n'ont pas posé de problèmes particuliers
- « Cryptographie»
  AP : très bons retours aussi. Sauf le symbole de Legendre en CC qui est assez mal passé même si il avait été vu en TD.
- « Compléments en cryptographie»
  AP : organisation pas terrible avec les TP tout à la fin du semestre, ca aurait été mieux de les faire plus tôt, en particulier celui sur ASCON qui a moins de prérequis.
  SD : effectivement, les TP sont arrivés très tard, essentiellement à cause de contraintes fortes de disponibilités des enseignants. On tachera de les faire plus tôt à l'avenir.
- « Complexité»
  AB : pas de soucis sur les CM/TD. Beaucoup de temps passé sur la première partie (automates) et pas assez de temps sur la partie complexité à proprement parler
  SD : c'etait pas le cas les années précédentes à voir avec l'enseignant
  AP : l'an dernier, il y avait même eu un cours de révision à la fin
- « Network Security »
  AB : cours bien, mais certaines formulations en TP pas toujours très claires
  MG : Et en terme de charge de travail (ça avait été relevé l'an dernier) ?
  AB : important mais bien réparti sur le semestre
  MG : contrairement à l'an dernier, les étudiants ont pu accéder à la salle pour terminer les TP. L'enseignant qui reprend le cours cette année est motivé, il construit pour l'instant celui de cyber (au S1) et va devoir l'adapter pour le public crypto. Mais attention, ce cours pourrait être remutualisé à terme et ce serait dommage de perdre cette différentiation entre les 2 populations.
  SD : Effectivement ca paraît plus logique pour les directions d'UFR mais en plus de l'argument de la différentiation pédagogique, c'est aussi important en terme de cohérence car le cours arrivait clairement trop tôt dans la formation quand il était en S1 (et il est bloqué au S1 par l'EIT Digital).
- « Apprentissage statistique » cours optionnel
  AB : lien entre le cours et le TP pas clair. Manque des bases théoriques (optimisation convexe) et TP/projets très appliqués. Les TP manquent d'attendus clairs
  AP : C'était pareil l'an dernier
  SD : on avait déjà fait remonter l'an dernier, on va recommencer.
- « Théorie des nombres » cours optionnel
  AB : organisation plutôt bien mais un peu trop orienté prépa agreg
  SD : effectivement et c'est annoncé qu'il n'y a pas beaucoup d'applications crypto. Ce cours a été très choisi cette année

- « Algèbre commutative et géométrie algébrique » cours optionnel
  AB : bien sur le contenu mais module difficile, en particulier le CC
- « Histoire des maths » cours optionnel non choisi cette année
- « Projet»
  AB : pas trop de remarques, ce serait bien d'avoir plus d'encadrement, par exemple des points d'étapes
  MG : vous commencez tard
  SD : effectivement des points d'étapes permettent de s'y mettre plus rapidement.
  MG/SD : Ne serait-ce qu'un petit rapport un mois avant d'une page pour savoir ou vous en êtes, les sources choisies, la direction envisagée. On va mettre çà en place.

SD : 15 étudiants ont validé l'année et 6 n'ont pas validé et 3 partent sur un redoublement. Plutôt une bonne promo à part ces étudiants en difficulté. Plus hétérogène que la promo précédente.

AB : Les enseignants de C++ et leurs méthodes sont bien appréciés. Ils font un cours de C en M1 CSM, pourquoi ne pas mutualiser avec CSM plutôt que Cyber
SD : Besoin d'aller plus loin en crypto qu'en CSM car le niveau d'exigence et l'utilisation professionnelle est plus élevé à la sortie du diplôme. De plus c'est risqué de s'appuyer à long terme sur le département de maths pour assurer un cours de programmation bas niveau. Mais c'est vrai que la consigne « Commencer au niveau 0 » n'est pas comprise pareil par un enseignant de maths et d'info. J'en discuterai avec les enseignants de CSM.

Bilan du second semestre de M2

Seulement 3 matières officiellement en plus de l'anglais.

- « Théorie algorithmique des nombres pour la cryptographie »
  AP : Rythme soutenu pour la partie sur les bases de Grobner. Il faut suivre et ne pas lâcher 5mn. Trop de bases considérées comme acquises car déjà faites en ACGA. La seconde partie est intéressante, c'est la suite logique du S1 peu captivant et ne tombe pas au bon moment car les stages arrivent très vite. Evaluation par DM pendant les stages.
  SD : Les étudiants doivent pouvoir se consacrer intégralement à leur stage dès le début. Ce sera plus facile cette année car les stages commencent après les vacances, mais sur le long terme il faut changer çà.

- « Codes correcteurs en cryptographie»
  AP : DM pas au dernier moment comme TANC mais encore un peu tard par rapport au stage. Bien organisé, par contre, très théorique, beaucoup de preuves (très intéressant pour ceux qui veulent faire une thèse en codes). Généralement plus apprécié quand c'est devenu un peu plus calculatoire et en TP. Un peu rapide et en anglais. Difficile même pour les maths fondas.
  SD : C'est aussi un choix de l'organisation de mettre les modules les plus théoriques après la recherche de stage car ils sont en pratique moins facile à vendre.

- « Cryptographie quantique »
  AP : Super bien, très bien de pouvoir démarrer en décembre car ca allège le mois de janvier.
  on sent que l'enseignant n'est pas spécialiste du domaine, mais il est très investit et c'est un des meilleurs cours de la formation.

Bilan des stages de M2

AP : C'est super qu'il y ait plein d'offres transmises sur la liste de diffusion. La réunion avant de

partir en stage est utile et les étudiants sont globalement contents de leurs stages. Ce serait bien que la date de rendu du mémoire soit un peu plus claire. Les soutenances sont peut être un peu courtes.
SD : C'est vrai mais il faut que ca reste pas trop dense pour le jury et l'audience
GA : C'est important de savoir condenser et tirer l'essentiel
SD : Encore une fois, les retours des entreprises sur les stages sont très positifs y compris pour les stages thématiquement assez éloignés de la formation (assez nombreux cette année). Ca montre à la fois que les étudiants sont capables de s'ouvrir et que les entreprises ne s'intéressent pas qu'aux compétences déjà acquises. Il y avait 22 étudiants inscrits avec un niveau plutôt bon et assez homogène. 19 ont validé l'année et 2 redoublent. Contrairement à l'an dernier, peu d'étudiants ont trouvé un débouché à ce jour que ce soit dans la continuité du stage ou ailleurs. C'est probablement lié à l'instabilité politique actuelle qui rend les employeurs frileux et inquiétant pour les étudiants.
MG : on observe la même tendance en M2 cyber où la situation s'est inversée par rapport à l'an dernier (où une majorité d'étudiants avaient trouvé un emploi rapidement). Les rapport de stages sont globalement meilleurs qu'en cyber.

SD continue à recevoir des offres de thèse. Comme on ne sait pas quand les adresses Rennes 1 fermeront et qu'il semble compliqué de mettre en place des listes d'alumni, il les postera désormais sur le groupe LinkedIn

AP : Ce serait bien de faire une remise de diplôme.
SD : On ne le fait pas d'habitude car ça a peu de succès mais on va essayer de faire çà si il y a une demande, par exemple pendant la cyberweek.

<u>Point sur les candidatures</u>

SD : Nous avons reçu cette année 151 candidatures en M1 via la plateforme Monmaster, ce qui est plus que l'an dernier pour 20 places ouvertes. 3 étudiants ont également intégré la formation en dehors de la plateforme. La promotion de cette année comporte 25 étudiants dont 7 femmes. C'est à priori raisonnable mais c'est biaisé par la présence de 3 redoublantes. Seules 3 femmes ont intégré la formation via Monmaster. Environ la moitié de la promo vient de Rennes et l'autre moitié vient en grande majorité du grand ouest.
En M2, il y avait une dizaine de candidatures qui n'avaient pas fait le M1 crypto à Rennes et une admission seulement car les prérequis sont importants et donc difficiles à rattraper. Il y a finalement 17 étudiants inscrits dont un en parcours recherche fondamentale.

AP : Comment sont classés les étudiants sur Monmaster ?
SD : Il y a 2 étapes, une première pour répartir les étudiants en 4 groupes (admis à coup sûr, admis à priori, en balance, refusés). Ensuite on calcule un score pour classer au sein de chaque groupe. Les critères principaux qui rentrent en compte dans ce calcul sont les notes de Licence (avec des coeffs plus importants pour les notes d'algèbre ou de L3) et la lettre de motivation.

<u>Point sur la rentrée</u>

SD : Pas de problème important survenu en ce début d'année. Il y a juste les mises à niveau en M1 qui ont été compliquées à mettre en place car je m'y suis pris trop tard. Cette année un tutorat, financé par la cyberschool, est mis en place pour que les étudiants de M2 accompagnent ceux de M1, en particulier pour le cours de C.
AB : Emploi du temps assez léger pour l'instant en M2 car les options choisies commencent tard.
SD : Il va falloir faire attention à ce que ca n'implique pas une grosse surcharge en novembre et janvier. On devrait pouvoir décaler des cours de cryptanalyse en décembre et faire commencer crypto quantique en fin de S1 comme l'an dernier pour alléger janvier/février.