Compte rendu de la réunion du conseil de parcours du Master de cryptographie du 11 février 2025

Présents: Arthur Baudy (M1), Delphine Boucher, Sylvain Duquesne, Mathieu Goessens, Pierre Loidreau, Alban Perreaux (M2)
Absente : Marion Videau

Bilan du premier semestre de M1

SD : Effectif de 21 étudiants cette année. 15 devraient valider leur S1 ou en être très près (il manque encore les notes d'anglais). Il y a donc 6 étudiants en difficultés ce qui est beaucoup par rapport aux années précédentes. Il y a aussi 6 PAEH, ce ne sont pas exactement les mêmes mais il y a quand même une grosse intersection.
AB : Semestre assez dense comme annoncé, en particulier certaines semaines où il y a des TP à rendre. Ce serait bien de mieux d'étaler les cours jusqu'à décembre. Plusieurs CC ou TP à rendre sont arrivés trop tôt. Sinon bonne ambiance dans la promo, entraide.
SD : emploi du temps compliqué à gérer, mais on doit effectivement pouvoir étaler, au moins placer les CC finaux plus tard. En particulier l'enseignante d'OPS est partie au 1er décembre ce qui a rajouté des contraintes.

- **« Algorithmique de base (ALBA) »**
  AB : Contenu assez dense mais résultats corrects. Les TP demandent beaucoup de travail, ce n'est pas un problème en soi mais dommage que ça ne rentre pas plus en compte dans l'évaluation finale (bonus). Anglais potentiellement gênant pour certains étudiants mais c'est bien que les sujets de CC soient en français.
  PL : Est-ce que les étudiants sont prévenus en amont que certains cours sont en anglais
  SD : Oui, c'est écrit sur la page web et ils sont prévenus avant la rentrée

- **« Algèbre de base (ALGB) »**
  AB : Résultats catastrophiques aux CC1 et 2, le CC final a bien rattrapé mais c'est un peu démoralisant. Ce serait mieux de rééquilibrer. Il y a eu des échanges avec l'enseignant qui est conscient du problème mais c'est compliqué de gérer 3 groupes (crypto, maths fondas, magistère). En TD ce serait bien d'avoir des exercices plus ciblés sur ce qui va servir dans la suite de la formation.
  SD : c'est effectivement à corriger, on sait que c'est un module difficile mais je ne me souviens pas qu'il y avait un tel décalage entre les différents CC. Il serait intéressant de savoir si ce décalage se retrouve aussi dans les autres groupes, je demanderai.
  AP : Un peu quand même, surtout le premier. Le second était plus facile et au dernier il y avait un exercice spécifique pour le groupe crypto.

- **« Outils de probabilités et statistiques (OPS) »**
  AB : Plutot bien dans l'ensemble.
  SD : l'an dernier, il n'y avait pas eu assez de temps pour la partie stats. On avait supprimé la partie chaines de Markov (faite en Théorie de l'information) pour laisser de la place aux stats. Ca a été le cas ?
  AB : oui, pas de soucis.
  SD/DB : pour l'instant, on n'a personne pour l'an prochain. C'est un cours de base donc plein de collègues pourraient le faire (Stéphane Leborgne par exemple) mais les besoins en proba/stats sont importants pour peu d'intervenants disponibles.

- **« Théorie de l'information (TINF) »**
  AB : petit cours terminé mi-novembre, un peu trop rapide sur la fin du cours alors que

c'était plus compliqué et théorique (Théorème de Shannon)
SD : et-ce qu'il faut plus étaler ce cours sur le semestre ?
AB : non, c'est bien comme çà, ca permet de dégager du temps en novembre/décembre pour les projets de C.
SD : Effectivement, c'est pour çà qu'on l'avait concentré en début de semestre, on garde donc ce principe.

- **« Low level programming (LLP) »**
  AB : On se prend un mur dès le début**. P**remiers TP assez abstraits et rudes. Difficile de comprendre où on va et plusieurs semaines avant de sortir la tête de l'eau mais la fin est plus intéressante. Beaucoup d'entraide mais insuffisant car la plupart des étudiants sont dans le même brouillard. Un TP préliminaire en septembre, ce serait bien pour ne pas attaquer directement les vrais TP sans savoir faire un makefile.
  MG : quelques heures de mise à niveau cette année mais concentrés sur la prise en main de Linux et insuffisant, en particulier tous n'avaient pas installé Linux avant les premiers cours. On rappelle que vous pouvez solliciter l'équipe pédagogique, la cyberschool et les M2 pour aider à préparer vos machines. Ce serait bien que l'UFR maths prenne en charge ces heures de mise à niveau.
  SD : Effectivement, l'ISTIC ne veut plus les prendre en charge (MG a du utiliser des heures de Réseaux du S2), mais çà reste hypothétique coté UFR maths car elle sera dissoute en fin d'année universitaire. On ne connaît pas encore notre interlocuteur à la fac des sciences pour ce type de question.
  AP : Les M2 ont été pas mal sollicité pour ce cours là et ont plutôt répondu présent.
  MG : Retour de l'enseignante qui a du mal à réduire le gap entre les groupes (qui arrivent avec des bases très éloignées). Ca se ressert en général en fin de module où c'est moins technique et avec plus de réflexion sur le fond du problème proposé.
  AB : C'est vrai mais c'est dommage qu'il ne reste plus que quelques semaines de cours à ce moment là
  MG : l'université peut proposer des contrats de monitorat étudiant pour formaliser et rémunérer le support des M2 aux M1. C'est sous réserve mais la cyberschool pourrait financer.
  SD : c'est une très bonne idée, on va se renseigner et essayer de mettre çà en place pour l'an prochain. Même pour la remise à niveau, ca peut être plus positif si ca vient d'étudiant qui ont rencontré les mêmes difficultés les années précédentes.

- **« Analyse et conception formelle »**
  AB : Plutôt apprécié. Dommage qu'il n'y ait pas de retour sur les TP plus réguliers. Contenu intéressant.

- **« Anglais »**
  AB : Pas très emballé par les thèmes abordés très éloignés de la formation. Demande beaucoup de travail. Très scolaire et très littéraire.
  SD : C'est des retours qu'on leur fait régulièrement et ca ne semble pas impossible de choisir des thèmes plus technologiques
  AP : L'an dernier, c'était bien, on avait carte blanche sur un sujet de notre choix. C'était sympa mais l'enseignante ne comprenait pas tout.
  PL : Ce n'est pas si évident, ils ont une formation littéraire et c'est plus difficile de juger si l'anglais est de bonne qualité sur des thématiques plus spécialisées. Ça demanderait aussi beaucoup plus de travail d'adapter les thèmes pour chaque formation.
  SD : J'en discuterai avec l'intervenante. En général ils sont receptifs et s'adaptent mais les intervenants changent souvent

MG : Avez vous des retours sur l'école d'hiver et les jeudis cyber organisés par la cyberschool
AB : On est venus à la plupart des évènements. C'est difficile de se sentir concernés thématiquement. Le plus intéressant c'était la table ronde sur les métiers des mathématiques, plus concret.
SD : Cette évènement là était organisé par le SOIE, pas par la cyberschool. C'est vrai que les jeudi cyber sont plus pensés cyber, mais ca reste intéressant et important de s'ouvrir aux thématiques connexes, en particulier pour l'insertion professionnelle.
AP : Très bien pour l'école de recherche même si on n'est pas allé à tout et que la partie crypto était très redondante avec les cours. Même retour que pour les M1 pour les jeudi cyber, même quand c'était orienté crypto, ca parlait très peu de cryptographie. Mais globalement ca reste intéressant et c'est une très bonne initiative La cyberweek c'était très bien, même si il n'y avait pas beaucoup de stage disponibles à cause de la situation politique. Le forum centrale était beaucoup moins convaincant, les entreprises ne cherchent que des profils cyber et ont pratiquement toutes dit qu'ils n'avaient rien à proposer. Le séminaire crypto était très intéressant mais les étudiants ne viennent pas. Peut-être parce que c'est plus dur de se motiver le vendredi après midi et qu'il n'y avait pas cours après.
DB : C'est dommage car ça donne un aperçu des sujets actuels, d'autant plus que c'est prévu dans l'emploi du temps

Bilan du premier semestre de M2
SD : 22 étudiants mais pas de résultat semestriel pour le moment, à vrai dire, je n'ai quasiment aucune note pour le moment. 1 étudiant a abandonné. 2 sont en situation difficile.
AP : On n'a quasiment aucune note, dont certaines datent de novembre. C'est dommage car çà permet de savoir où on en est. Dans l'ensemble les retours sont neutres à satisfaits. Quelques problèmes d'emploi du temps. Contenu des cours intéressant mais on se demande pourquoi certains cours sont là ou au moins sont obligatoires. Très bonne cohésion, y compris avec les M1. Bon dialogue avec les enseignants.
SD : C'est très bien d'avoir pu mettre en place des échanges avec les M1. Il faudra essayer de perpétuer çà.
AP : quelques retours sur les cours d'1h30, certains préféraient 2h.
DB: c'est vrai que pour les TP par exemple, c'est trop cours. Peut-etre essayer de coller 2 séances quand c'est le même sujet.
AP : Le BDE de la cyberschool un peu inutile, ne fonctionne pas bien.
MG : Ils ont effectivement eu des difficultés administratives cette année. Il est surtout poussé par la Cyberschool, mais il faut que les étudiants s'en emparent. Et sur un an et demi de présence sur site pour la formation, ca fait court pour mettre des choses en place.

- **« Courbes elliptiques en cryptographie »**
  AP : Les cours de la partie théorique étaient très bien et allaient à la bonne vitesse. Par contre, pas de vrais TD (en autonomie et/ou révisions) c'est dommage car la pratique permet de mieux comprendre les motions assez théoriques vues en cours. Les CC étaient assez bizarres, basés sur des QCM et avec une nouvelle méthode de notation qui avait comme conséquence de rechercher les petites erreurs dans l'énoncé plutôt que de répondre à la question avec nos connaissances.
  Vraiment compris les courbes elliptiques grâce à la partie crypto. Celle-ci s'est très bien passée, TP et système de notation très bien, manque peut-être un peu de TD. Très intéressant
  SD : C'est une bonne nouvelle que les cours se soient bien passés. Ce n'était pas le cas les années précédentes et çà veut dire que l'enseignant s'est bien adapté au public. Reste à améliorer la partie TD/évaluation, quitte à reporter une partie des TD sur la partie crypto du cours.

- **« Réseaux euclidiens en cryptographie »**

AP : Première partie très bien. Notation sur un projet en sage. Très bonne approche. Plus mitigé sur la partie crypto, en particulier car c'était des blocs de 3h (Cours + TD). Le TD portait directement sur le cours et donc ce n'était pas possible de s'y préparer. Ce serait bien d'introduire un décalage entre cours et TD. Plus théorique que la première partie, compliqué à suivre pour les étudiants qui n'ont pas suivi PRS. Poly très bien écrit (dommage de le découvrir en live). La fin était très bien (Kyber et Dilithium) → plus de participation en TD.
SD : On va essayer de mettre en place ce décalage entre cours et TD et de faire en sorte que le poly soit communiqué en avance.

- **« Sécurité réseaux (SRES) »**
  AP : Cours catastrophique déjà remonté à Thomas Genet. Beaucoup de redites de ce qui a été fait en M1. Par contre les TP sont très bien avec apport de crypto de la part de l'enseignant. CC décalé 4 fois, plusieurs mois après le dernier cours et sans aucune info. Même retour des étudiants de Cyber → a mettre plutôt en optionnel.
  MG : intervenant de CM trouvé dans l'urgence et a du être remplacé. Sur le fond du cours, c'est vrai qu'il y a beaucoup de redites, il y a des plans pour refonder le cours plus en lien avec mais pas encore eu le temps de mettre çà en place.
  SD : On peut rendre le cours optionnel l'an prochain, à rediscuter avec l'équipe du master cyber. Dans tous les cas, c'est bien qu'on ait mis la main sur un bon enseignant de TP.

- **« Cryptanalyse »**
  AP : Cours trop dense (fait en 3 semaines en janvier, avec plusieurs CM d'un coup). CC compris dans les 3 semaines et dans de mauvaises conditions (manifestation). Ressenti assez négatif sur la première partie car c'est beaucoup de la redite de M1 crypto (Pollard rho, anniversaire). Pas assez de détails sur la cryptanalyse différentielle. Même ressenti des cyber. Beaucoup de TP (intéressants) donc ce serait bien qu'ils soient notés. Ce serait bien de l'étaler sur décembre pour rendre çà moins dense. 2eme partie plus intéressante mais déjà faite en PRS. Retours déjà fait directement auprès des enseignants.
  SD : l'objectif du cours, c'est au moins de bien comprendre la cryptanalyse différentielle. Je discuterai avec les enseignants pour rehausser le niveau.
  MG : Ce n'est pas un problème si c'est trop compliqué pour les cyber, ils sont de toutes façons déjà découragés à choisir cette option. Par contre, ce cours est aussi proposé en SIF et c'est pour çà qu'il est tassé en janvier.
  SD : L'an dernier, la partie asymétrique du cours avait été jugée sans intérêt. C'est bien qu'elle ait effectivement disparue, mais il y a encore clairement des ajustements à faire.
  PL : C'est dommage quand même de ne pas faire de cryptanalyse sur les réseaux.

- **« Sécurité des implémentations »**
  AP : Première partie sur Raspberry vraiment très bien (sauf l'évaluation un peu bizarre). 2eme partie très bien avec ChipWhisperer (attaque de l'AES). Compliqué au début, mais très positif, en particulier pour les stages. Deadline un peu flottantes pour les rapports de TP.
  DB: Quid des side-channel sur les codes correcteurs d'erreurs ? Avant c'était dans le cours de Jade.
  SD : C'est vrai que çà a disparu avec le départ de Tania Richemond. C'est dommage d'autant qu'il n'y a plus que du symétrique dans ce cours. L'objectif est avant tout d'apprendre à manipuler, mais c'est une piste à creuser.

- **« Programmation objet, Java »**
  AP : Très bien (contenu, enseignant, charge de travail), si possible il faut garder cet enseignant. Doublon très clair entre Java et C++ donc CM pas très utiles (il y en a peu). Introduction des graphes UML appréciable. Premiers TP pas très intéressants mais la suite était en mode projet donc très bien.

- **« Anglais »**
  AP : Avec les cyber (mais aussi les maths fondas), enseignantes très bien mais sujets toujours déconnectés de la formation. Beaucoup de travail de groupes et sur des projets, et 1h30 c'est trop court, c'était beaucoup mieux quand c'était des créneaux de 3h.
  SD : Est ce que vous vous êtes rapproché de ce que font les cyber plutôt que les maths ?
  AP : Non, mais au final, ca ne changerait pas grand-chose, les thématiques restent basiques.

- **Options**
  « C++, les bases (POCB) »
  AP : Tout est très bien (cours, TP, enseignants), pris par quasiment tout le monde, dommage d'être noté sur un CC écrit pour un cours de programmation

  « C++, compléments (POCC) »
  AP : Retours globalement négatifs, noté en projet. Ce n'est pas un problème de contenu (c'est la suite logique du premier cours).

  « Sécurité des protocoles (SEP) »
  AP : Très bien passé, pas tant de charge de travail qu'annoncé à la réunion de rentrée. Très peu d'étudiants dans le cours (4 ou 5 en tout).
  SD : C'est plutôt positif que la charge de travail ne soit finalement pas un obstacle pour ce cours. C'est peut-être par exemple dû à l'introduction d'ACF en M1 qui permet d'avoir les bases pour suivre ce cours.

  « Preuves de sécurité (PRS) »
  AP : Globalement satisfaisant. Ce cours mériterait d'être obligatoire car il est utilisé dans plusieurs autres cours. TD un peu moyens (beaucoup de démonstrations à retravailler chez eux). CC durs et dommage de ne pas avoir de retour dessus.
  SD : La question se posait déjà l'an dernier de le passer en obligatoire, l'information a été donnée lors de la réunion de rentrée mais çà semble clairement opportun de le passer officiellement en obligatoire. On va faire le nécessaire et si on y arrive pas à temps, on l'imposera officieusement au moment de la réunion de rentrée.
  AP : Solutions envisagées pour passer PRS en obligatoire : passer SRES en optionnel, introduire un choix entre Java et C++.
  SD : Passer Java en optionnel risque de le faire disparaître car il n'est pas mutualisé.
  PL/MG : Important de le garder car considéré indispensable dans beaucoup d'entreprises.

  « Programmation parallèle et sur GPU »
  AP : Tout est parfait, c'est plus du parallèle que du GPU mais on en fait quand même. Toujours pas de notes alors que les CSM les ont eu...

  « Blockchain (BLK) »
  AP : Souffre du fait que c'est condensé sur 4 semaines mais moins gênant que cryptanalyse car c'est des TP. Intéressant sur le fond mais peu suivi, retours déjà faits aux enseignants. Un CC écrit surprise alors que c'était annoncé comme étant évalué sur les TP (bug de communication). TP sur bitcoin très bien. Partie sur les smartcontracts impeccable aussi.

  « Introduction au droit de la cybersécurité (IDC) »
  AP : Très positif.

<u>Point sur les stages</u>

SD : 4 étudiants n'ont pas encore trouvé de stage. C'est classique à cette période de l'année.

Ce n'est pas spécialement inquiétant (il reste 8 mois pour effectuer un stage de 4 mois) mais stressant pour les étudiants concernés d'autant plus que les offres de stages sont plus rares.

AP : Au moins 3 des étudiants concernés continuent de chercher activement, ont des entretiens et attendent des retours.

MG : Si certains étudiants ont besoin d'un coup de main pour leur CV ou leur lettre de motivation, il ne faut pas hésiter à nous solliciter.

AP : C'est super d'avoir plein d'offres de stages qui sont transmises mais il y a beaucoup de stages en labo de recherche

SD : C'est vrai, mais ce sont en général des stages intéressants et ça ne ferme pas du tout les portes pour un recrutement en entreprises après. Un étudiant a eu des problèmes de ce type l'an dernier et çà a entraîné une appréhension dans la promo sur ces stages, mais ce n'est pas représentatif du cas général.

AP : Beaucoup de retard de réponses à cause de la situation politique, les entreprises ont beaucoup temporisé. Il ne s'est rien passé jusque début décembre.

SD : C'est tout à fait vrai et c'est pareil pour les étudiants de l'an dernier en recherche d'emploi.

<u>Point divers</u>

MG : Problème d'utilisation par les étudiants de l'IA générative qui va de plus en plus se poser (pas identifié en crypto mais çà viendra).

SD : D'un côté c'est important pour les étudiants d'apprendre à se servir de ces outils, de savoir prendre du recul sur les résultats obtenus, etc. D'un autre coté çà pose des problèmes pour nos évaluations car çà élimine les parties en autonomie qui sont à la fois les plus motivantes et les plus pertinentes à ce niveau de formation.

MG/PL : Effectivement, il ne reste plus que le CC sur table avec un papier et un crayon !

DB : En L2 on fait des évaluations par TP surveillés sans accès internet.

AP : On en a parlé avec l'enseignante de GPU qui suggère d'avoir une formation dessus comme les CSM et comme l'université propose de financer.

SD : J'en discuterai avec les responsables de CSM pour avoir des précisions sur ce qu'ils font et comment on peut le généraliser.