

Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 15 octobre 2021

Présents: Delphine Boucher, Amélie Bru (M1 l'an dernier), Sylvain Duquesne, Emmanuel Fleury, Baptiste Mougeot (M1 l'an dernier), Marion Videau (en visio).

Absents excusés: Pierre Loidreau, Romane Arvier (M2 l'an dernier)

Bilan du second semestre de M1

AB/BM : semestre globalement intéressant et apprécié, plus orienté crypto/plus concret. Charge de travail bien répartie. Sauf pour un étudiant qui travaillait en parallèle et a eu des difficultés à gérer les 2. Dur de suivre les cours sur un écran. La motivation est plus dure à tenir en distanciel. En grande majorité, les étudiants préfèrent largement le présentiel.

EF : seriez vous OK pour continuer certains cours en distanciel si il y a le choix avec du présentiel

AB/BM : Non. Certains étudiants préfèrent le distanciel dans certains cas, mais dans la très grande majorité de cas, le présentiel est très nettement préférable.

- « Complexité»

BM : beaucoup ont aimé surtout quand ca devient concret (TD biens pour comprendre les cours).

SD/EF : pour l'instant pas de lien avec la crypto. Ce serait peut être bien d'ouvrir un peu sur les preuves de complexité, les preuves par réduction → ça motivera plus et ça rentrera dans l'esprit de la cyberschool et de la future mineure en méthodes formelles.

Ne serait-ce que mettre en perspective ce qui est fait par rapport aux applications crypto.

SD : l'intervenant actuel va bientôt partir à la retraite. Il faudra trouver quelqu'un pour la rentrée 2023 et il y aura peu de candidats à l'UFR maths.

EF : il y a du monde à l'IRISA qui peut faire ça, mais sans lien avec la cryptographie.

SD : pourquoi pas aussi les personnes impliquées dans la mineure/majeure méthodes formelles en réorientant un peu le cours.

- « Codes correcteurs (COCO)»

AB : TB, même en distanciel, cours bien adapté à l'hybride

BM : Assez complet et intéressant d'avoir le lien abstrait/concret

DB : Ce n'était pas gênant d'être aussi nombreux ?

BM : Ca allait car beaucoup de choses à distance de toutes façons et c'était par exemple très bien d'avoir des supports pour les corrections.

DB : encore une cinquantaine d'étudiants prévus cette année. A voir comment il va falloir gérer en présentiel. L'idéal aurait été d'avoir 2 groupes de TD mais pas d'intervenant disponible. On va donc probablement rester sur le même type de fonctionnement avec moins de participation mais plus de supports, d'autant plus que c'est apprécié par les étudiants.

AB : oui et système de notation plutôt bien apprécié aussi.

EF : Pourquoi pas limiter les effectifs de maths fondas ou qu'ils ne suivent que le cours ?

BM : ou vrai TD une semaine sur 2 seulement ?

SD : il faut une solution qui permettent à tous de suivre le cours dans de bonnes conditions. Si ce type d'effectif se confirme, il faut prévoir de dédoubler et donc trouver de potentiels intervenants.

- « Machine learning »

AB/BM : intégralement en distanciel. Cours trop dense mais intéressant de voir les concepts. Difficile de voir une notion en 2h. Dommage qu'il y ait eu peu de retour sur les TP et commentaires pas assez clair ou en décalage avec la note (d'autant plus que c'était la seule note).

SD : liens avec la sécurité (pas facile pour les intervenants car ils n'ont pas de formation en sécurité).

AB/BM : cours commun avec les CSM et les maths fondas donc le cours ne peut pas être trop orienté sécurité. Quelques liens en fonction des projets. Pas mal d'offres de stage secu/machine learning.

- « Cryptographie (CRYP)»

AB : bien, intéressant. C'est pour ça qu'on est là. TP/TD bien aussi. Distanciel bien géré.

Séances supplémentaires sur Discord pour préparer les CC → très apprécié.

- « Anglais »
AB : pas de problème particulier, bien de travailler l'oral.
- « Projet tutoré »
AB : Plutôt bien d'avoir un bon mois pour le faire. Dommage que les consignes aient été données un peu trop tard. Bien de voir ce que les autres ont fait.

SD : 16 étudiants ont validé l'année et 4 redoublent. Il y a également eu 2 abandons en début d'année. Plus de décrochage que les années précédentes. C'est clairement un effet Covid et pas d'inquiétude sur la capacité à réussir cette année. Ça ne leur portera préjudice pour la suite car âges très variables dans les promos en général et sans influence remarquable sur la réussite/stage/emploi.

AB : effectivement, il n'y a que 3 étudiants dans la promo de l'année officielle d'un Bac+5.

BM : effet Covid clairement ressenti aussi. Bonne ambiance dans la promo et entraide.

Bilan du second semestre de M2

La représentante est absente mais a fait passer ses retours par email: semestre moins apprécié que le premier dû au confinement. Aucun ou très peu de cours sur place et tous les examens en présentiel.

- « Cryptographie quantique » : cours pas adapté au travail à distance on recopié juste des diapo et les exercices n'étaient pas très interactifs. Sinon le cours avec le pdf en ligne était intéressant et abordable et l'examen plutôt adapté.
- « Théorie algorithmique des nombres pour la cryptographie »
Partie 1 (Lorenzo) : Méthode du TD (chacun avait des exercices à faire et à rendre) pas apprécié par tout le monde. On avait pas forcément la correction des exercices non rendu ou pas bien réalisés, pas évident pour réviser. Cours compliqué examen pas adapté au cours à distance.
Partie 2 (Derbez) : A commencé très tard pendant le début des stages alors qu'elle aurait pu commencer plus tôt. Intéressant mais pas le temps d'y consacrer beaucoup sur le projet à rendre avec le début du stage.
- « Codes correcteurs » : Apprécié par la majorité, cours et TD intéressants. Travaux à rendre adaptés au confinement.
- « Anglais » : Un peu désorganisé, examen écrit en visio un peu étrange. UE pas très adapté au distanciel...

Bilan des stages de M2

RA : En globalité les réponses sont très mitigées, certains ont eu des sujets changés, une ou plusieurs fois, au dernier moment et n'ont pas vraiment apprécié leurs stage. D'autres ont trouvé leur stage très enrichissant et en sont satisfait.

SD : Encore une fois, les stages se sont globalement très bien passés à part un ou deux stages problématiques. Il y avait 18 étudiants inscrits et 15 présents dont 14 ont validé l'année. A ce jour 10 d'entre eux ont trouvé un emploi ou une thèse et 3 font une formation complémentaire. Ceux qui ont eu le plus de mal à trouver n'avaient pas ou peu cherché avant la fin de leur stage. Il semble que la situation sanitaire n'ait pas vraiment eu d'impact sur les débouchés car ces chiffres sont similaires aux années antérieures.

BM : Ça veut dire quoi un stage problématique

SD : C'est rare, mais il arrive qu'il y ait une incompatibilité entre l'entreprise et le stagiaire, souvent des problèmes de personnes et/ou de manque d'encadrement. Pour l'instant ça n'est jamais arrivé que le stagiaire ne fasse pas son travail. Les situations sont variées et peuvent aller jusqu'à des abus au code du travail de l'entreprise.

MV : Ça arrive par exemple, en particulier en période Covid, où le manque de proximité fait que le stagiaire demande moins facilement en cas de problème, l'encadrant est moins disponible et la situation peut s'envenimer par manque de communication.

EF : Y penser pendant les entretiens, ça doit être à double sens. Il faut poser des questions sur l'entreprise, ce qu'on attend de lui et sonder si le courant passera avec l'encadrant. Un entretien c'est dans les 2 sens. Il ne faut pas hésiter à chercher ailleurs sinon.

MV : Il y a plein d'offres de stages, ça vaut le coup de multiplier les pistes. En plus les entreprises attendent aussi des candidats qui sont curieux, qui prennent des initiatives, qui s'investissent, ... Un entretien ou vous êtes aussi activement impliqué est donc positif dans tous les cas et permet de montrer vos qualités.

Point sur la rentrée

SD : plus de communication que d'habitude avec la montée en puissance de la Cyberschool. 143 candidatures ont été reçues en M1. C'est comme l'an dernier où il y en avait eu plus que d'habitude, mais surtout on note une hausse qualitative des dossiers. Cette année la sélection a été faite avec la cyberschool (notamment avec une phase de présélection) et des bourses ont pu être distribuées.

DB : j'ai l'impression qu'il y a plus d'étudiants en provenance du parcours GM de L3.

SD : c'est vrai. On a plus clairement ouvert aux étudiants de GM à partir du moment où ils choisissent les module optionnels d'algèbre en L3 (en particulier ANAR).

51 ont été acceptés en LP ou en LA. 35 ont confirmé leur venue et se sont inscrits, 2 ne sont jamais venus et 4 ont changé d'orientation depuis la rentrée. La promo s'est donc stabilisée à 29, ce qui est déjà beaucoup et nous oblige à trouver des solutions de dédoublement de TP et ça va avoir un impact sur les projets.

EF : pas clair que les bourses aient un impact significatif pour attirer des étudiants.

SD : En M2, il y avait 15 candidatures qui n'avaient pas fait le M1 crypto à Rennes et 2 sont venus (en M1 maths fondas l'an dernier), tous en parcours recherche car les prérequis sont importants pour le parcours classique et donc difficiles à rattraper.

Il y a finalement 19 étudiants inscrits dont 6 dans le parcours recherche. Il faut rajouter à cela 2 étudiants du double diplôme actuellement en Allemagne.

Pour l'instant tout en présentiel et pas trop de complications avec l'emploi du temps.

AB : Inquiétude pour après les vacances de la Toussaint avec un module (SRES) entièrement sur une semaine à 8h par jour

EF : c'est parce que c'est des intervenants industriels qui doivent poser des congés pour faire les cours et on beaucoup d'autres contraintes. C'est un format assez classique de cours de formation continue. C'est clairement compliqué et pas idéal mais on n'y peut pas grand-chose.

Autre point

Prochaine habilitation devra être opérationnelle pour la rentrée 2023. Le gros du travail sera probablement fait au printemps et ce point sera donc à l'ordre du jour de la prochaine réunion du comité. Les membres du comité, et plus généralement tous ceux qui lisent ces lignes, sont invités à réfléchir aux améliorations qui pourraient être apportées à la formation et à faire remonter des remarques sur du contenu qui manquerait, de meilleurs équilibres à trouver, etc...

Plusieurs pistes commencent à être discutées :

- reverse engineering, mais ce n'est pas l'objectif du master. Par contre c'est important de savoir discuter avec les personnes qui en font. Pareil pour la micro-électronique ou d'autres domaines connexes. Ce serait utile de favoriser ce type de compétence. Par exemple avec plus d'interactions avec les étudiants du master cybersécurité. C'est un bon objectif pour la cyberschool.
- Dans la maquette actuelle, il n'y a pas de programmation en L3, même en génie mathématique. C'est dommage d'avoir un trou dans la formation alors que les étudiants qui passent par ce type de licence seront professionnellement amenés à beaucoup utiliser les outils informatiques