Compte rendu de la réunion du comité de pilotage du Master de cryptographie du 4 octobre 2022

Présents: Delphine Boucher, Amélie Bru (M2 l'an dernier), Sylvain Duquesne, Emmanuel Fleury, Baptiste Mougeot (M2 l'an dernier, en visio), Pierre Loidreau (en visio), Maël L'hostis (M1 l'an dernier)
Absents: Marion Videau

Transformation du comité de pilotage en "conseil de parcours"

SD : Le conseil de l'UFR Mathématiques a décidé en septembre de :

- conserver le conseil de perfectionnement commun à la licence et au master dans sa composition actuelle
- mettre en place des conseils de parcours sur le modèle de ce comité. Il n'y a donc pas de changement à prévoir pour nous autre qu'un changement de nom

Bilan du second semestre de M1

ML : semestre plus tranquille et plus léger que le premier. Avec en plus 2 matières dans le coeur du domaine (Crypto et codes correcteurs). Globalement bien et ça fait du bien de retrouver du présentiel mais gros point noir avec le cours de machine learning.

- « Machine learning »
  ML : ce module ne s'est pas bien passé. Le contenu est intéressant mais la forme n'est pas bien adaptée. Les étudiants n'ont pas compris ce qu'on attendait d'eux, comment ils seraient évalués et n'ont pas adhéré au cours et en particulier aux TP python. Plusieurs intervenants.
  AB : même problème avec les codes python l'an dernier en même temps prémachés et difficile de s'y retrouver dedans
  EF : même type de retour des étudiants en informatique attribué à un contenu trop math
  ML : Pas vraiment un problème de prérequis, concepts pas si compliqués. Même impression des étudiants de CSM aussi. Pas de réponse à une sollicitation sur les MCC.
  DB : Point commun avec ALBA de l'an dernier sur le nombre d'intervenants qui rend les attendus plus difficiles à cerner.
  AB/BM : c'était le cas aussi cette année en codes correcteurs et c'est vrai que c'est plus compliqué à appréhender car plus difficile de cerner l'objectif général du cours et de savoir où on va.
  SD : Thématiques en tension et donc compliqué de trouver des intervenants. Je vais discuter avec le responsable de cours pour améliorer cette année. Ce cours deviendra optionnel à la rentrée 2023
- « Complexité»
  ML : Pas un gros module, qui s'est plutot bien passé, pas de retours particuliers ou de grosses difficultés
- « Codes correcteurs (COCO)» et « Cryptographie (CRYP)»
  ML : Très bien passé, bons résultats. Content de se lancer dans le coeur du sujet. Ca a remotivé certains étudiants et ca permet de bien se lancer tout le monde dans la formation.
- « Anglais»
  ML : Pas toujours très motivant mais OK
- « Projet tutoré»
  ML : Bonne alternative au stage, permet de travailler sur ce qui a le plus intéressé pendant l'année ou découvrir autre chose permet. Ca peut aussi servir à étoffer le CV et valoriser les candidatures en stage.

SD : 21 étudiants ont validé l'année et 7 n'ont pas validé. Il y a également eu 1 abandon en début d'année. Encore plus de décrochage que l'an dernier qui était déjà pire que les années précédentes. C'est probablement un effet post-covid. La plupart redoublent et ça ne devrait pas leur porter préjudice pour la suite car les âges sont très variables dans les promos en général et on ne constate pas d'influence sur la réussite ou l'obtention d'un stage/emploi.

Bilan du second semestre de M2

AB/BM : Passé vite mais globalement intéressant et bien, mais ceux qui n'avaient pas encore trouvé de stage étaient plus concentrés sur la recherche de stage

- « Cryptographie quantique »
  AB :Difficile à suivre manque peut-être des prérequis, heureusement il y avait des rappels à chaque cours. Pas clair si il faut savoir ou comprendre l'idée générale. Examen final OK. Avec le recul ça va, mais sur le coup, pas évident à suivre.
  SD : Beaucoup de prérequis (physique, analyse) nécessaire pour tout bien comprendre et on ne peut clairement pas tout mettre dans la formation
  EF : Ca pourrait être bien d'avoir une approche plus algorithmique
  AB/ML : Pour les prérequis ça dépend d'où viennent les étudiants et même pour les rennais ca dépend si ils ont fait le parcours GM ou recherche en L3. Beaucoup de concepts à assimiler en peu de temps 2 mois
- « Théorie algorithmique des nombres pour la cryptographie »
  AB : Cours de la partie cryptanalyse plutôt bien, mais mauvais choix de langage pour le TP (au final, python n'était pas adapté). La partie théorie des nombres à proprement parler était un peu dure par moments mais très intéressante. Les étudiants ont apprécié de passer au tableau et la correction d'un examen type. Timing trop tendu à la fin, certains n'ont pas réussi à faire en même temps le dernier TP et le projet.
  BM : Très utile pour les stages pour beaucoup d'étudiants.
- « Codes correcteurs en cryptographie» :
  AB : perturbant d'avoir plusieurs intervenants au niveau organisation. Première partie très intéressante mais niveau élevé et beaucoup de nouvelles notions en peu de temps. Alternance exo/cours appréciée. TP très intéressant mais comptait trop peu dans la note finale et pas assez pratique.
  Deuxième partie très intéressante, plus culturelle, nécessite moins de travail. Pas clair ce qu'il fallait réviser au final dans l'équilibre entre les 2 parties du cours.
  DB : Dommage que tout le monde n'ait pas compris que les 2 heures de cours faites par le troisième intervenant sur les soumissions au NIST étaient pour la culture
  SD : A partir d'un certain niveau, c'est compliqué de tout comprendre en peu d'heures. C'est important et utile aussi d'avoir une culture générale large de l'existant quitte à rentrer plus tard dans les détails en cas de besoin.
- « Anglais » :
  AB : Beaucoup d'activités orales intéressantes mais pas de corrections donc les erreurs restent. Trop de temps passé sur les origami. Ce serait mieux d'avoir de la lecture d'articles scientifiques et les présenter.
  BM : Enseignante très investie, peut être l'aiguiller sur des articles liés à la crypto. Manque de vocabulaire technique
  SD : Pas facile car ça multiplie les difficultés et enseignants pas forcément à l'aise , mais on va essayer de voir si on peut lui soumettre une base de données d'articles scientifiques de type grand public. Le but c'est avant tout de travailler l'anglais mais c'est mieux si c'est un peu plus motivant
- Cours du parcours recherche
  AB/BM : Évaluation sous forme de DM bien car ça permet de prendre son temps et de bien travailler la matière. Certains modules trop durs (géométrie torique, ED algébriques par exemple) mais intéressants. Charge de travail mieux répartie.
- « Sécurité des implémentations (SIMP)»
  AB : Très bien, très pratique/appliqué. Enseignant très disponible malgré le nombre d'étudiants en TP. Vu comme l'un des cours les plus importants
  EF : Cette année, les TP sont dédoublés et moins suivi par les cyber (passé optionnel)
  SD : C'est clairement un des cours les plus important et il va y avoir une suite l'an prochain
  ML : 4h d'un coup c'est pas évident
  SD/EF : Souvent comme çà pour les intervenants extérieurs

Bilan des stages de M2

AB : Très bonne expérience, pas mal d'offres partagées, idem pour les thèses et les emplois. Temps pour trouver un stage assez variable

SD : Encore une fois, les retours des entreprises sur les stages sont globalement positifs. Malgré une grosse promo la plupart des étudiants a trouvé assez facilement un stage et cette année on a commencé à recevoir des offres très tôt. Il y avait 21 étudiants inscrits dont 2 encore en double diplôme avec Karlsruhe. 18 ont validé l'année et 2 redoublent. A ce jour 13 d'entre eux ont trouvé un emploi ou une thèse (6 dont 5 du parcours recherche). Ceux qui ont eu le plus de mal à trouver n'avaient pas ou peu cherché avant la fin de leur stage. C'est similaire aux années antérieures. Peu de CIFRE mais ça semble plutôt venir des étudiants que de l'offre.

Point sur la rentrée

SD : toujours plus de candidatures chaque année en M1. 177 cette fois, dont bon nombre de très bonne qualité, plus que les 24 places officiellement disponibles en tous cas. Ça commence à devenir problématique car on est obligés de refuser des bons dossiers ou des dossiers de la licence de maths de Rennes qui satisfaisaient aux critères demandés. Comme l'année dernière, la sélection a été faite avec l'aide de la cyberschool et des bourses ont pu être distribuées. Il y a finalement 34 étudiants dans la promo cette année dont 11 étudiantes. C'est beaucoup mais en partie du au nombre important de redoublants.

EF : Attention aux sureffectifs. Un des objectifs de la cyberschool est de former beaucoup plus d'étudiants dans le domaine de la cybersécurité, mais il faut rester raisonnable sur la taille des promos. On s'oriente probablement vers une sélection de type parcours-sup pour les master

SD : On est clairement sur une fourchette haute de promo voire sur un pic. C'est à peu près tenable en M1 (dédoublement de TD en codes correcteurs par exemple) même si ca demande des moyens humains, mais de telles promos en M2 ne sont pas tenables (projets, stages, emplois)

DB : Que faut il dire aux étudiants de L2 qui veulent faire le master crypto avec la disparition du parcours GM (fusionné avec le parcours MEEF) ? Ont ils toutes leurs chances si ils ont un bon dossier dans ce nouveau parcours ou vaut il mieux qu'ils aillent en parcours recherche de L3 ?

SD : C'est clair qu'au niveau visibilité pour les étudiants, la disparition du parcours GM n'est pas une bonne chose. Les 2 populations peuvent accéder au master mais en général un étudiant de L3 recherche qui valide son année est quasi sûr d'être pris. Les dossiers GM sont étudiées de façon plus détaillée et çà continuera probablement comme çà.

ML : Pour avoir expérimenté les 2 parcours, le niveau est bien différent et le choix entre les 2 n'est pas évident.

SD : Le niveau attendu pour le master crypto se situe entre les 2 comme c'est généralement le cas dans les universités où il n'y a qu'un seul parcours de licence de maths.

EF : très difficile de trouver des logements pour les nouveaux arrivant

SD/AB : Il faut se mettre très tôt à chercher (mars/avril), avant même d'être accepté ce qui est forcément problématique

EF : Les étudiants ont l'air d'avoir un bon niveau. Meilleures notes que les cyber cette année sur la première évaluation

DB: Bonne impression aussi mais déjà quelques devoirs non rendus

DB: Pour les groupes de TD de codes, vaut il mieux mélanger avec les étudiants de maths fonda ou faire un groupe spécifique crypto quitte à ce que les groupes soient déséquilibrés ?

AB/ML : En général, on ne se mélange pas avec les autres étudiants de maths ou de cyber, même si on crée des liens.

SD : plus simple aussi au niveau emploi du temps

SD : En M2, il y avait 15 candidatures qui n'avaient pas fait le M1 crypto à Rennes et 4 sont venus (3 agrégés, un polytechnicien), dont 3 en parcours recherche car les prérequis sont importants pour le parcours classique et donc difficiles à rattraper.

Il y a finalement 24 étudiants inscrits. Il faut rajouter à cela 1 étudiant du double diplôme actuellement en Allemagne.

ML : rentrée sympa et conviviale. Événements organisés par le BDE et avec l'aide des coordinatrices de la cyberschool qui permettent de rencontrer les M1 et les cyber. C'est amené à se développer et c'est une très bonne chose
DB : Les M1 n'ont pas encore de représentants
SD : C'est vrai que ça peut être embêtant pour l'organisation en début d'année mais ils ne se connaissent pas encore bien

Maquette définitive 2023-2027
Les maquettes pour la prochaine habilitation (effective à la rentrée 2023) sont quasi actées. Plus précisément, elles ont été validées par le conseil de l'UFR maths mais pas encore par l'ISTIC. Des dénominations et des volumes horaires sont donc encore susceptibles de changer à la marge. Pas de changement fondamentaux par rapport à la maquette actuelle, si ce n'est

- un rééquilibrage de volume horaire entre les semestres 1 et 2 du M1 suite aux discussions de ce comité
- un nouveau cours de méthodes formelles en M1
- L'introduction d'un choix de cours au second semestre de M1
- La démutualisation de cours avec des publics trop hétérogènes (Réseaux en M1, Java en M2) problèmes également identifiés par les dernières réunions de ce comité
- La création de nouveaux cours de M2 obligatoires (cryptanalyse) et optionnels (droit, preuves de sécurité, C++2, sécurité des implémentations 2) et la suppression de cours optionnels peu pris ou peu adaptés (Challenges de sécurité, Sécurité des données)

Master 1 2023-2027

	ECTS	CM	TD	TP	total	
Semestre 1						
Algèbre de base	5	22,5	22,5	4,5	49,5	
Algorithmique de base	5	22,5	22,5	12	57	
Low Level programming	5	20		20	40	
Méthodes formelles	5	14	0	22	36	mineure
Outils en probabilités et statistique pour l'ingénierie mathématique et l'intelligence artificielle	5	22,5	22,5	12	57	mineure
Théorie de l'information	2	12	12		24	
Anglais	3		30		30	
total	30				293,5	
Semestre 2						
Cryptographie	5	22,5	15	15	52,5	
Codes correcteurs	5	21	19,5	12	52,5	
Compléments en cryptographie	2	6	6	6	18	
Complexité	3	15	15		30	
Apprentissage statistique	5	18	0	18	36	mineure au choix
Algèbre commutative et géométrie algébrique		22,5	22,5			
Histoire des maths		22,5	22,5			
Théorie des nombres		22,5	22,5			
Network security	5	20	10	16	46	
Projet R&D	5				0	
total	30				235	

Master 2 2023-2027

	ECTS	CM	TD	TP	total	mutualisation	Parcours
Semestre 1							
Courbes elliptiques en cryptographie	5	21	15	9	45		Commun classique/recherche
Réseaux euclidiens en cryptographie	4	21	15	3	39	ISTIC	
Programmation Java pour la cryptographie	3	**9**		**21**	30		Classique
Cryptanalyse	3	12		20	32	Cyber	
Sécurité réseaux	3	12	4	16	32	Cyber	
Sécurité des implémentations	3	12		20	32	Cyber	
	3 UE au choix						Mineures classique
Sécurité des protocoles	3	20			20	ISTIC	
C++, les bases	3	12		12	24	CSM	
C++, compléments	3	12		12	24	CSM	
Programmation parallèle, GPU	3	12	16		28	CSM	
Blockchain	3	12		20	32	Cyber	
preuves de sécurité	3	12		20	32	Cyber	
droit de la cybersécurité	3	16	16		30	Cyber	
Sécurité des implémentations 2	3	12		20	32	Cyber	
Algèbre et Géométrie 1	6	24			24	MFA	Recherche
Algèbre et Géométrie 2	6	24			24	MFA	
Séminaire	6				0	MFA	
Anglais	3		30		30		
Semestre 2							
Théorie Algorithmique des nombres pour la cryptographie	3	**15**	12	6	33	MFA	Commun classique/recherche
Codes correcteurs en cryptographie	3	**15**	12	6	33		
Cryptographie quantique	3	15	15		30		
Anglais	3		30		30		Classique
stage	18				0		
Algèbre et Géométrie 3	6	24			24	MFA	Mineure Recherche
stage	15				0		Recherche