Contacts :

- Nicolas Perrin
email : nicolas.perrin@uvsq.fr
tél. : 01 39 25 36 22
bureau : bâtiment Fermat, 3306

- Jacques Patarin
email : jacques.patarin@uvsq.fr
tél. : 01 39 25 43 16
bureau : bâtiment Descartes, 309C

Les candidatures se font en ligne sur le site d'admission de l'université Paris-Saclay. Pour les étudiants étrangers résidant à l'étranger (hors CE), l'application Campus France est obligatoire.

Tous les cours se déroulent à Versailles au 45 avenue des États-Unis.

http://www.departement.math.uvsq.fr/
http://www.universite-paris-saclay.fr/fr/formation/master/mathematiques-et-applications

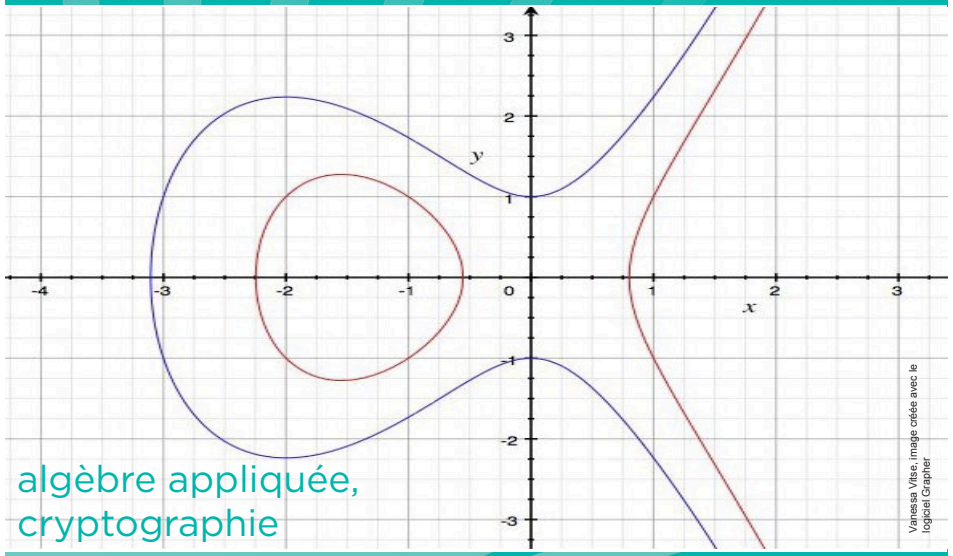
LMV
Laboratoire de mathématiques de Versailles - CNRS UMR 8100

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

université PARIS-SACLAY

MASTER 2
Algèbre appliquée, cryptographie

proposé à l'Université de Versailles St-Quentin-en-Yvelines



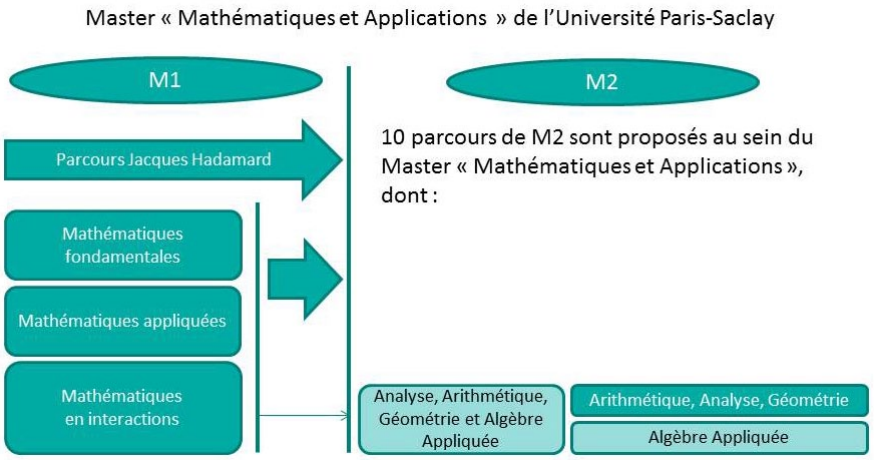
algèbre appliquée, cryptographie

Vanessa Vitse, image créée avec le logiciel Grapher

Master 2 «Algèbre Appliquée »

Responsables : Nicolas Perrin, Jacques Patarin

Le Master 2 « Algèbre Appliquée » proposé à l'université de Versailles Saint-Quentin-en-Yvelines fait partie du parcours « Analyse, Arithmétique, Géométrie et Algèbre Appliquée », qui est l'un des dix parcours du Master 2 « Mathématiques et Applications » de l'Université Paris-Saclay.
Ce master est ouvert à tout étudiant titulaire d'un Master 1 ou équivalent en mathématiques



Objectifs du Master

Le Master 2 « Algèbre Appliquée » est destiné à des étudiants désirant acquérir une formation solide et moderne en calcul formel, géométrie et cryptographie pour la recherche fondamentale et le développement dans l'industrie.

À l'issue de cette formation, les étudiants maîtriseront des techniques d'algèbre moderne sur les plans théorique et pratique. Ils seront capables de modéliser algébriquement un problème concret, d'estimer la difficulté à résoudre ce problème, et enfin d'utiliser et adapter des algorithmes récents rapides pour procéder à sa résolution.

Un stage de six mois en laboratoire (de mathématiques ou d'informatique) ou en entreprise permet d'assurer l'insertion des étudiants dans le tissu industriel ou de mettre en place un projet de thèse, universitaire ou en partenariat avec l'industrie.

Originalité des cours de cryptologie

La formation en cryptologie proposée dans le Master 2 « Algèbre Appliquée » est une des rares formations complètes en cryptologie en Île-de-France, menant à la fois vers des débouchés académiques (thèse, puis recherche à l'université ou au CNRS, INRIA, etc.) et des débouchés dans la recherche appliquée (dans des entreprises de haute technologie liées à la sécurité informatique).

En comparaison à d'autres formations en Île-de-France qui abordent la cryptologie, le volume d'heures consacrées à la cryptologie dans le Master 2 « Algèbre Appliquée » est très important, avec à la fois un cours sur les algorithmes avancés de la cryptographie et la cryptanalyse, un cours sur la complexité algébrique et la cryptographie et un cours d'algorithmique et de langage C pour les applications en cryptologie. Les étudiants disposent ainsi d'un parcours complet allant des aspects les plus théoriques (hypothèses calculatoires en théorie des nombres, preuves de sécurité, techniques de cryptanalyse) jusqu'aux problématiques les plus récentes d'implémentation optimisée ou sécurisée (algorithmique fine sur les corps finis, sur les courbes elliptiques, problématiques d'attaques physiques). Ceci leur permet ensuite d'aborder dans les meilleures conditions soit une thèse, soit une activité d'ingénieur R&D dans le monde industriel.

Débouchés

Les étudiants bénéficient de nombreux partenariats académiques (CEA, École polytechnique, ENS Ulm, IRMAR, INRIA, LORIA, UPMC, etc.). Ils peuvent s'orienter vers une thèse universitaire, éventuellement en partenariat avec l'industrie, puis vers un poste de Maître de conférences à l'université, de Chargé de recherche au CNRS ou à l'INRIA, etc. En dix ans, 32 étudiants du Master 2 «Algèbre Appliquée» ont poursuivi par une thèse, dont 24 en cryptographie.

Ils peuvent également s'orienter vers les métiers d'ingénieurs en Cryptographie ou Recherche & Développement dans une entreprise liée à la sécurité informatique (Accenture, Bull, Crédit Agricole, CryptoExperts, CS Communication & Systèmes, Dictao, Gemalto, Morpho, Ingenico, Oberthur Technologies, Orange, Sogeti, Viaccess-Orca, etc.).

Cours du Master 2 «Algèbre Appliquée»

- Algèbre effective
- Algorithmique, langage C
- Complexité algébrique et cryptographie
- Courbes algébriques
- Courbes elliptiques

Options

- Algorithmes avancés de la cryptographie
- Théorie algébrique des systèmes