Recrutement

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

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

Débouchés

Les étudiant·es bénéficient de nombreux partenariats académiques (CEA, École polytechnique, ENS Ulm, IRMAR, INRIA, LORIA, UPMC, etc.). Ils·elles 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 étudiant·es du Master 2 «Algèbre Appliquée» ont poursuivi par une thèse, dont 24 en cryptographie.

Ils peuvent également s'orienter vers les métiers d'ingénieur·es en Cryptographie ou Recherche & Développement dans une entreprise liée à la sécurité informatique (Accenture, Bull, Crédit Agricole, CryptoExperts, CS Group, IDEMIA, Ingenico, Orange, Sogeti, Thales, Viaccess-Orca, etc.)

Contacts

Coordonnées

UFR des Sciences
45 avenue des
Etats-Unis
78035 VERSAILLES

Responsables de la formation

- Ana-Maria Castravet (M1)
  ana-maria.castravet@uvsq.fr
- Pierre-Guy Plamondon (M2)
  pierre-guy.plamondon@uvsq.fr

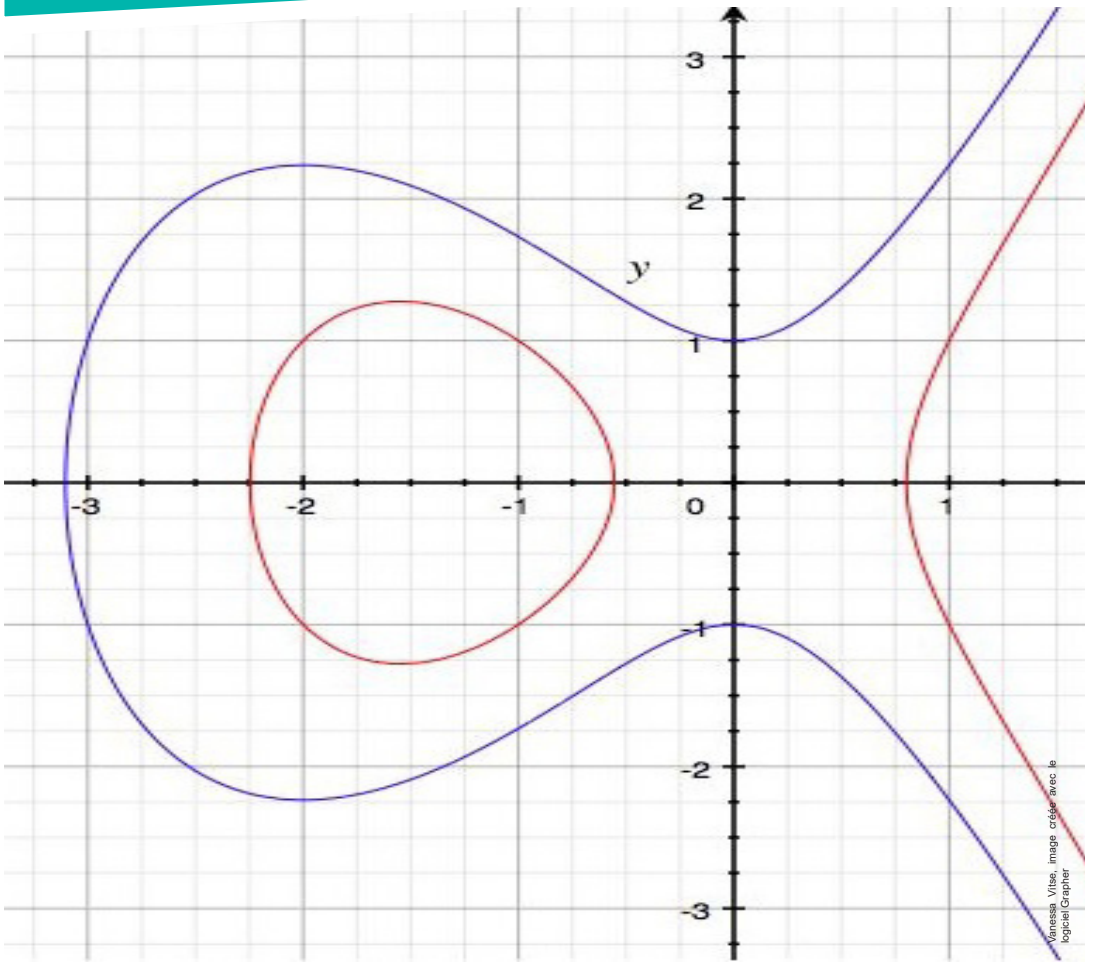
UVSQ
université PARIS-SACLAY

université PARIS-SACLAY

MASTER AA
Mention Mathématiques et Applications

UVSQ
université PARIS-SACLAY

Algèbre appliquée



Vanessa Vitse, image créée avec le logiciel Grapher

- Master Paris-Saclay opéré par l'UVSQ
- UFR des Sciences

Présentation

Le Master (M1 et M2) « Algèbre Appliquée » proposé à l'Université de Versailles Saint-Quentin fait partie du Master « Mathématiques et Applications » de l'Université Paris-Saclay.

Ce Master est ouvert à tout étudiant titulaire d'une Licence de Mathématique, Mathématique-Informatique, Mathématiques-Physique ou l'équivalent.

Objectifs du master

Ce master est destiné à des étudiant·es 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 étudiant·es maîtriseront des techniques d'algèbre moderne sur les plans théorique et pratique. Ils·elles 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 étudiant·es dans le tissu industriel ou de mettre en place un projet de thèse, universitaire ou en partenariat avec l'industrie.

Plus d'informations

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

Originalité des cours de cryptographie

La formation proposée dans les programmes de Master M1-M2 Algèbre Appliquée est une des rares formations complètes à la cryptologie en Ile-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 étudiant·es 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·e R&D dans le monde industriel.

Programme

M1 - 1er semestre

- Algèbre générale
- Théorie des nombres et cryptographie
- Cryptographie
- Introduction au calcul formel et projet
- Probabilités
- Anglais

M1 - 2e semestre

- Algèbre commutative
- Introduction aux courbes elliptiques
- Calcul sécurisé
- Analyse d'algorithmes, programmation
- Introduction au calcul scientifique et projet
- Théorie de l'information

M2

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

Options

- Algorithmes avancés de la cryptographie
- Théorie algébrique des systèmes