— Master AA —

Master Recherche & Professionnel

Spécialité :

Algèbre Appliquée

(cryptographie et calcul formel)

Universités

Versailles

Paris-Saclay

Responsables de la formation :

Nicolas Perrin
nicolas.perrin@uvsq.fr
Équipe algèbre et géométrie

Mohamed Krir
mohamed.krir@uvsq.fr
Équipe algèbre et géométrie

Jacques Patarin
jacques.patarin@uvsq.fr
Équipe cryptographie

Contact électronique : mohamed.krir@uvsq.fr

Candidature en M2

Les dossiers de candidature se font exclusivement par internet à travers le site de l'Université Paris-Saclay sur le lien suivant : **https ://apply-tc.ecp.fr/**

Table des matières

1 Synthèse de la formation en M2

Les Unités d'Enseignement (UE) suivantes sont proposées en M2 ; Les enseignements sont étalés sur deux périodes chacune d'une durée de 7 semaines. Chaque UE est organisée sous forme de 3 heures de CM et de 3h de TD par semaine.

Première période (durée 7 semaines)

- Courbes algébriques (MSMA912) (6 ECTS)
- Algèbre commutative et effectivité (MSMA910) (6 ECTS)
- Algorithmes avancés de la cryptographie, Cryptanalyse (MSIM913) (6 ECTS)
- Algorithmique et Langage C I (50% de MSIM914)

Deuxième période (durée 7 semaines)

- Courbes elliptiques (MSMA911) (6 ECTS)
- Complexité algébrique et cryptographie (MSIM915) (6 ECTS)
- Algorithmique et Langage C II (50% de MSIM914)

Le cursus peut être complété avec des Unités d'Enseignement des autres spécialités du master, ou, après accord avec les responsables, avec des UE d'autres masters en convention (par exemple le M2 Analyse, arithmétique et géométrie d'Orsay ou l'UE de calcul formel de l'université Paris Diderot).

Stage et séminaire étudiant

L'étudiant doit faire un stage dans une entreprise ou dans un laboratoire de recherche. Il aura alors à lire, comprendre et appliquer un ou plusieurs articles de recherche ou développement industriel. Ce stage comporte obligatoirement un projet de programmation, et commence en avril. Un *Mémoire et projet de programmation (MSMA9ST) (21 ECTS)* doit être réalisé sous la responsabilité d'un enseignant-chercheur associé au master. La soutenance a lieu devant le jury au mois de septembre.

Au mois de juin les étudiants doivent obligatoirement participer au *Séminaire étudiant (MSMA9SE) (3 ECTS)* comptant pour 3 ECTS : le travail consiste en la présentation des premiers travaux du stage ainsi qu'en la présence active à toutes les présentations.

2 Débouchés professionnels

Les principaux secteurs d'activité visés par cette formation sont la recherche fondamentale et appliquée tant dans le secteur public que privé dans les domaines liés à la cryptographie, la modélisation algébrique, l'automatique. Nous distinguons trois principaux types de débouchés :

- La préparation au concours de l'agrégation externe de mathématiques ;
- La recherche fondamentale en géométrie algébrique effective, calcul formel, cryptographie ;
- La recherche appliquée et l'ingénierie mathématique.
- Secteur privé ou public en sécurité informatique et en cryptographie

2.1 Préparation à l'agrégation

Un étudiant désirant passer l'agrégation peut suivre un parcours adapté. Il suffit de suivre au niveau M1 les modules fondamentaux qui recouvrent le programme de préparation à l'écrit et de compléter sa formation par les unités d'enseignement de M2. La formation dispensée permet en outre aux étudiants d'envisager une préparation à l'agrégation après le master.

2.2 Recherche fondamentale

La formation théorique amène les étudiants en deux ans au niveau de la recherche internationale. Un étudiant se destinant à la recherche fondamentale doit choisir un stage l'y préparant : il doit donc prévenir son directeur de stage qui saura lui présenter un sujet adapté à ses ambitions.

Bourses de thèse

À l'issue du M2, des allocations de recherche sont proposées sur concours au sein de l'école doctorale de Paris-Saclay, de la Direction Générale de l'Armement, de l'INRIA ou du Ministère pour les candidats admis à continuer en thèse. Les candidats doivent se faire connaître des responsables du master le plus tôt possible, si possible avant le début du second semestre de leur année M2. Les actes de candidature proprement dits sont déposés en juin auprès du secrétariat de l'école doctorale (plus tôt pour les autres organismes), et doivent être accompagnés d'un rapport du futur directeur de recherche, et d'un curriculum vitæ du candidat.

2.3 Recherche appliquée et ingénierie mathématique

On ne sait pas assez que l'algèbre a des applications dans l'industrie. Une des ambitions de la spécialité est de mettre les étudiants ayant un goût pour l'algèbre en contact avec l'industrie.

Calcul formel

Les grands systèmes de calcul formel tels que Maple, Mathematica ou Magma offrent de nombreuses possibilités pour résoudre des problèmes concrets posés dans l'industrie. Par exemple, les problèmes statiques peuvent être modélisés par des systèmes d'équations polynomiales résolus par la théorie de l'élimination algébrique. Les résultats sont garantis, contrairement aux méthodes numériques classiques.

Cryptographie

Inutile de présenter la cryptographie qui a une utilité cruciale dans le secteur privé (sécurité informatique). Les succès des applications des méthodes formelles ne sont plus à démontrer et font l'objet d'une attention grandissante de la part des grands centres de recherche publics ou privés.
Louis Goubin, Antoine Joux et Jacques Patarin, de l'équipe CRYPTO, sont des experts reconnus dans le domaine de la cryptographie aussi bien académique que privée. Ils entretiennent des contacts étroits avec : France Télécom, Cegetel, le GIE CB, la DCSSI (Direction Centrale de la Sécurité des Services Informatiques), DGA/CELAR, Thalès, Axalto (Schlumberger) et Viaccess.

3 Objectifs pédagogiques

L'objectif est de former des chercheurs en calcul formel, géométrie et cryptographie pour la recherche fondamentale et le développement dans l'industrie.

Une part croissante des mathématiques vraiment appliquées s'appuie sur des domaines se rattachant en totalité ou partiellement à l'algèbre : c'est le cas pour la cryptographie, pour le calcul formel et la géométrie effective. Une formation dans ces domaines exige un niveau élevé de compétences théoriques en mathématiques, ainsi que la maîtrise des aspects algorithmiques, jusqu'à leur implémentation informatique.
L'objectif de la spécialité *Algèbre Appliquée* est donc de proposer une formation de haut niveau en mathématiques, avec une spécialisation dans les domaines de l'algèbre les plus pertinents en cryptographie et calcul formel, alliée à une formation solide en informatique.

À l'issue de cette formation, les étudiants maîtriseront la majorité des techniques d'algèbre moderne, sur les plans théoriques et pratiques. En particulier, il seront capables de modéliser un problème concret par des modèles algébriques, de donner un ordre d'idée de la difficulté à résoudre ce problème et enfin d'utiliser et adapter des algorithmes récents rapides pour procéder à la résolution.
À l'issue de la formation, ils devront savoir rédiger un texte scientifique en LaTeX et dominer la programmation en C et C++.

3.1 Cryptographie

Une définition moderne de la Cryptographie peut être : la science des communications sécurisées. Cela comprend principalement les fonctions d'authentification, de chiffrement, et de signatures électroniques. Dans un monde où les besoins en informatique et en communication d'une part, et en sécurité d'autre part sont fondamentaux et en forte croissance, il n'est donc guère étonnant que les besoins en cryptographie deviennent de plus en plus importants. En fait, chaque jour presque chaque citoyen utilise, souvent sans le savoir, de la cryptographie : lorsqu'il utilise son téléphone portable, lorsqu'il paye avec sa carte bancaire, lorsqu'il utilise sa carte vitale, lorsqu'il regarde des chaînes de télévision payantes, ou lorsqu'il utilise internet pour ses achats, par exemple. De plus, l'électronique devient présente dans de plus en plus d'objets courants, la cryptographie s'introduit souvent dans les objets les plus classiques (par exemple pour ouvrir sa voiture, ou mettre en marche son auto-radio). Au fur et à mesure que les mauvais systèmes de sécurités sont attaqués, les besoins en solutions cryptographiques solides deviennent évidents. Ceci offre de nombreuses opportunités pour les étudiants qui auront suivi une formation en cryptographie dans les années qui viennent.
Cette discipline est à la frontière des mathématiques et de l'informatique, et elle nécessite une formation spécialisée dans ces domaines : l'histoire de la cryptographie montre de façon évidente que les solutions développées par les non spécialistes sont en général très peu sûres.

3.2 Calcul formel

Le développement scientifico-technologique de la société pose des problèmes qui, moyennant simplifications et modélisations, se traduisent en général par des systèmes d'équations et d'inéquations, classiques ou différentielles, et nécessitent des solutions, c'est-à-dire, des processus capables de résoudre de tels systèmes. Afin que les solutions obtenues soient réellement utiles, elles doivent avoir une précision adaptée à la nature du problème original et doivent pouvoir se calculer de façon efficace.
Il existe deux méthodes traditionnelles pour aborder ces questions : la numérique et la symbolique. La tradition numérique a produit des algorithmes hautement efficaces, en termes de complexité algébrique. Néanmoins, ces algorithmes souffrent de grands inconvénients quand on considère la complexité binaire du problème d'approximation. Ces inconvénients proviennent de limitations qui s'expliquent à partir de la géométrie diophantienne. En outre, les algorithmes numériques ne permettent pas le traitement direct et efficace des singularités et des dégénérescences. Les algorithmes symboliques ne souffrent pas de ces derniers inconvénients. Le développement de tels algorithmes symboliques constitue l'objet d'étude du calcul formel et nécessite des connaissances approfondies en algèbre.

4 Équipes pédagogiques et laboratoires

— Équipe Algèbre et Géométrie : Laboratoire de Mathématiques de Versailles, UMR 8100, Université de Versailles – Saint-Quentin-en-Yvelines, bâtiment Fermat, 45, avenue des États-Unis, F-78035 Versailles cedex (France).

— Équipe CRYPTO : Laboratoire de Mathématiques de Versailles, UMR 8100, Université de Versailles – Saint-Quentin-en-Yvelines, bâtiment Fermat, 45, avenue des États-Unis, F-78035 Versailles cedex (France).

— Département de Mathématiques d'Orsay, Équipe Arithmétique et Géométrie Algébrique, Université Paris-Sud, bât. 425, 91405 Orsay cedex.

— Laboratoire d'informatique de l'Ecole polytechnique (LIX) équipe MAX, École polytechnique, Route de Saclay, 91128 Palaiseau cedex.

— Projet Algorithmes, INRIA Rocquencourt, domaine de Voluceau Rocquencourt, BP 105, 78153 Le Chesnay

— Laboratoire d'Informatique de Paris 6 (LIP 6), équipe projet PolSys, UMR 7606, Site Passy-Kennedy, 104 av. du Président Kennedy, 75016 Paris

Partenaires Industriels :
France Télécom, Cegetel, le GIE CB, la DCSSI (Direction Centrale de la Sécurité des Services Informatiques), DGA/CELAR, Thalès, Axalto (Schlumberger) et Viaccess.

5 Contenu des Cours de M2

Algèbre commutative et effectivité (MSMA910) 6 ECTS

Objectifs.
— Bases de Gröbner, algorithme de Buchberger.
— Théorie de l'élimination.
— Résultants.
— Applications.

Références bibliographiques :
— D. Cox, J. Little et D. O'Shea, *Ideal, varieties and algorithms*, Springer, 1997.
— D. Cox, J. Little et D. O'Shea, *Using algebraic geometry*, Springer, 1998.
— T. Becker et V. Weispfenning, *Gröbner Bases : A Computational Approach to Commutative Algebra*, Springer-Verlag, 1993.
— D. Eisenbud, *Commutative Algebra with a View toward Algebraic Geometry*, Springer-Verlag, 1995.
— *Computations in algebraic geometry with Macaulay 2*, édité par D. Eisenbud, D. R. Grayson, M. E. Stillman, and B. Sturmfels, Springer, 2001.

Répartition de l'enseignement : 21 heures de cours et 21 heures de TD
Prérequis : Algèbre commutative (6 ECTS), Calcul formel (6 ECTS)

Courbes algébriques (MSMA912) 6 ECTS

Objectifs.
— Topologie de Zariski.
— Variétés projectives, courbes projectives planes.
— Corps de fonctions.
— Morphisme de variétés projectives.
— Diviseurs, diviseurs sur les courbes, degré.
— Groupe de Picard.

— Cas des courbes elliptiques.

Références bibliographiques :
— W. Fulton, *Algebraic curves*, Benjamin 1969.
— R. Hartshorne, *Algebraic Geometry* Springer 1977.
— R.J. Walker, *Algebraic curves* Princeton University Press.
Répartition de l'enseignement : 21 heures de cours et 21 heures de TD
Prérequis : Algèbre commutative (6 ECTS), Calcul formel (6 ECTS)

Algorithmique et Langage C I & II (MSIM914) 6 ECTS

Il s'agit d'un seul module réparti sur les deux semestres.
Objectifs. Le but de ce cours est l'apprentissage de techniques algorithmiques visant à programmer efficacement, ainsi que du langage C, afin d'illustrer ces techniques. Un aperçu des outils d'analyse et de débogage gprof et gdb, ainsi que de la librairie de grands nombres GMP vient compléter ces objectifs.
Chaque cours consiste en une étude approfondie d'un exemple, choisi en relation avec les autres modules du master. L'objectif étant, pour chacun d'eux, de comprendre les facteurs limitants et d'étudier comment les contourner afin d'obtenir des performances améliorées.
— Multiplication de matrices 32×32 dans $GF(2)$.
— Eléments de base de calcul dans $GF(p)$, avec les opérateurs C d'abord (limite à 16 puis 32 bits environ), avec la librairie GMP ensuite. Illustration sur RSA. Calcul de racines carrées.
— Calcul sur les polynômes à une et plusieurs variables.
— Algorithmes de Tri. Algorithmes de tri à base d'arbres équilibrés.
— Applications en cryptographie et théorie des nombres des algorithmes de tri. « Collisions généralisées » entre 4 listes.
— Courbes elliptiques. Comptage de points par pas de bébé – pas de géant.
— Compléments sur les courbes elliptiques : diviseurs, fonctions, couplage de Weil–Tate. Algorithmes pour les couplages. Applications cryptographiques : Diffie–Hellman tripartite, chiffrement basé sur l'identité, signatures courtes.
— Transformées de Fourier et applications. Multiplication de polynômes, recherche d'approximation linéaires.
— Problématique des accès en mémoire et des effets de cache. Application au crible d'Eratostène.
— Algèbre linéaire et calcul de base de Gröbner sur GF(2).

Références bibliographiques :
— *Introduction to Algorithms (Second Edition).* Cormen, Leiserson, Rivest et Stein, MIT Press et McGraw-Hill, 2001.
— *A course in computational algebraic number theory.* Henri Cohen. Springer GTM 138.
Répartition de l'enseignement : 42 heures de cours et TD

Courbes elliptiques (MSMA911) 6 ECTS

Objectifs. Ce cours est consacré à l'étude des courbes elliptiques en vue de leurs utilisations en cryptographie. Nous développons les points suivants :
— Courbes planes affines et projectives : propriétés locales, diviseurs.
— Courbes elliptiques : généralités, forme de Weierstraß, loi de groupe, couplage de Weil.
— Courbes elliptiques sur les corps finis
— Courbes elliptiques sur le corps des nombres rationnels
— Application des courbes elliptiques

Références bibliographiques :
— D. Perrin, *Géométrie Algébrique, Une introduction*, Savoirs Actuels, 1995.
— W. Fulton, *Algebraic Curves*, Benjamin, 1969.
— J. H.Silverman, *The Arithmetic of Elliptic Curves*, Springer, Graduate texts in Math. 106, 1986.

Répartition de l'enseignement : 21 heures de cours et 21 heures de TD

Algorithmes avancés de la cryptographie, Cryptanalyse (MSIM913) 6 ECTS

Objectifs. L'objectif est ici d'une part de donner aux étudiants une réelle expertise sur les grands algorithmes cryptographiques (la façon de les générer, et de les utiliser pour des applications réelles de l'industrie), et d'autre part d'introduire les principaux axes de recherche en cryptographie actuellement. On met ainsi l'accent sur les diverses techniques modernes de cryptanalyse, sur les contre-mesures de sécurité, sur les techniques de programmation efficaces des algorithmes, et sur divers problèmes ouverts. On détaillera en particulier les points suivants :

- Le RSA revisité : diverses attaques de protocoles RSA, les normes actuelles, programmation rapide du RSA.
- Les techniques de cryptanalyse à clé secrète : cryptanalyse différentielle, cryptanalyse linéaire, cryptanalyse multivariable (algébrique), autres techniques.
- Cartes à puce : présentation des cartes à puces, les attaques physiques (SPA, DPA, DFA, etc.) et contre-mesures, exemples de protocoles pour certaines applications (cartes bancaires, de téléphone, de sécurité sociale, de télévision, etc.).
- Courbes elliptiques et cryptographie : ECC (Elliptic Curve Cryptography).
- La recherche actuelle en cryptographie : les grandes conférences annuelles, les revues et les ouvrages de recherche, les principaux articles récents.

Répartition de l'enseignement : 42 heures cours et TD.

Complexité algébrique et cryptographie (MSIM915) 6 ECTS

Objectifs. L'objectif du cours est d'aborder les notions modernes de sécurité pour les algorithmes cryptographiques, en particulier dans le cas asymétrique. Dans ce modèle, l'attaquant échange des messages avec un système et, en les utilisant, espère pouvoir mettre en défaut les objectifs visés (confidentialité, intégrité, authenticité...) par différentes techniques de cryptanalyse. La cryptographie récente s'efforce donc de construire des schémas avec si possible des preuves relatives de sécurité contre ce type d'attaque, en admettant la difficulté de certains problèmes algébriques, au sens de la théorie de la complexité.
À partir de résultats de théorie algorithmique des nombres, on étudiera la sécurité des algorithmes de chiffrement et de signature qui s'appuient sur la factorisation (RSA), le logarithme discret sur le groupe multiplicatif des entiers modulo p (ElGamal, Schnorr, DSA...), ou encore la réduction de réseaux (Merkle–Hellman, Chor–Rivest, NTRU...). Pour le cas de RSA, on analysera les attaques multiplicatives, et on étudiera les preuves relatives de sécurité pour les protocoles proposés ces dernières années pour le chiffrement (PKCS#1v1.5, OAEP, REACT...) ou pour la signature (ISO/IEC 9796, Full-domain-hash, Probabilistic Signature Scheme...). On donnera également des méthodes algébriques pour construire un générateur pseudo-aléatoire prouvé sûr (notamment à partir du problème de la résiduosité quadratique), ainsi que pour tester la primalité des entiers (Solovay–Strassen, Miller–Rabin, AKS).
Pour le logarithme discret, on verra comment il permet de résoudre le problème de la « chasse au pirate » (Boneh–Franklin) avec des applications à la diffusion sécurisée de contenus audiovisuels. Dans une autre direction, on s'intéressera également au problème du logarithme discret sur d'autres groupes, comme celui des points d'une courbe elliptique (avec comme application les algorithmes de signature ECDSA et Nyberg–Ruppel), ou encore la jacobienne d'une courbe hyperelliptique. Par ailleurs, on donnera des applications cryptographiques du « couplage de Weil » sur les courbes elliptiques, qui permettent d'obtenir des fonctions rares, comme des signatures extrêmement courtes (Boneh–Franklin), ou encore des algorithmes de chiffrement « basés sur l'identité » (Boneh–Franklin, Boneh–Boyen).
Une autre partie du cours sera consacrée aux cryptosystèmes « multivariables », qui s'appuient sur le problème MQ de résolution des systèmes d'équations polynomiales quadratiques à plusieurs variables, sur la notion d'isomorphismes de polynômes (IP), et sur la détermination d'une combinaison linéaires de matrices ayant un petit rang (MinRank). On détaillera notamment les algorithmes C* (Matsumoto–Imai) et HFE, en montrant comment certaines variantes fournissent des signatures électroniques ultra-rapides (SFLASH) ou extrêmement courtes (QUARTZ). On montrera également que l'approche multivariable donne naissance à de nouvelles techniques de cryptanalyse, y compris dans le modèle symétrique (AES, algorithmes de chiffrement par flot).

Dans les modèles de sécurité, on tient compte également, depuis quelques années, des « attaques physiques ». Ce nouveau concept prend en considération non seulement la sécurité des cryptosystèmes au sens mathématique, mais aussi les aspects liés à la nature physique des calculs. Ces attaques nouvelles sont particulièrement menaçantes pour les systèmes embarqués tels que les cartes à microprocesseur, contre lesquels l'adversaire peut mobiliser des moyens d'analyse de plus en plus sophistiqués. On en donnera des exemples dans le cas asymétrique, avec comme application des attaques par injection de faute sur RSA, par mesure de la consommation électrique sur les courbes elliptiques, ou encore par mesure du temps de calcul sur le protocole SSL, utilisé pour la sécurisation du paiement sur internet.

Références bibliographiques :

- Douglas Stinson, *Cryptographie – Théorie et Pratique* (Vuibert, 2003)
- Gilles Zemor : *Cours de Cryptographie* (Cassini, 2000)
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1997)
- Oded Goldreich, *Foundations of Cryptography – Volume I : Basic Tools* (Cambridge University Press, 2001)
- Oded Goldreich, *Foundations of Cryptography – Volume II : Basic Applications* (Cambridge University Press, 2004)
- Neal Koblitz, *A Course in Number Theory and Cryptography* (GTM 114, Springer, 1994)
- Neal Koblitz, *Algebraic Aspects of Cryptography* (Springer, 1998)
- M. Garey, D. Johnson, *Computers and Intractability* (Freeman, 1979)
- Eric Bach, Jeffrey Shallitt, *Algorithmic Number Theory – Volume I : Efficient Algorithms* (MIT Press, 1996)
- Henri Cohen, *A course in computational algebraic number theory* (4^{e} édition, GTM 138, Springer-Verlag, 2000)
- Henri Cohen, *Advanced topics in computational number theory* (GTM 193, Springer-Verlag, 2000)

Répartition de l'enseignement : 42h cours et TD.