

— MA² —

2009–2010

Université de Versailles – Saint-Quentin-en-Yvelines
Domaine Sciences et Technologies, Santé
Mention Mathématiques et Ingénierie des Mathématiques

Master Recherche

Spécialité :

Algèbre Appliquée

Parcours :

Cryptographie

Géométrie et Calcul formel

Automatique : une approche algébrique

Responsables de la formation :

VINCENT COSSART
Vincent.Cossart@math.uvsq.fr
Département de mathématiques
www.math.uvsq.fr

JACQUES PATARIN
Jacques.Patarin@prism.uvsq.fr
Département d'informatique
www.prism.uvsq.fr

Formation en collaboration avec le Département de Mathématique d'Orsay (Paris-Sud 11), SATIE-ENS Cachan, et le Projet Algorithmes de l'INRIA Rocquencourt.

Secrétariat de la spécialité :

Secrétariat du Département de Mathématique
Université de Versailles – Saint-Quentin-en-Yvelines
bâtiment Fermat
45, avenue des États-Unis
F-78035 Versailles cedex (France)
Téléphone : 01 39 25 46 46 (depuis l'étranger : +33 1 39 25 46 46)
Fax : 01 39 25 46 45 (depuis l'étranger : +33 1 39 25 46 45)
Courrier électronique : ma2@math.uvsq.fr
Site internet : www.math.uvsq.fr/ma2

Inscription en M2 : Les formulaires d'inscription en M2 doivent être envoyés si possible avant le 31 mai 2009 pour les non titulaires d'une maîtrise ou d'un M1 français, le 31 août 2009 pour les autres. Les réponses seront communiquées le plus tôt possible après réception de chaque dossier. Passées ces dates, les dossiers seront examinés au cas par cas. **ATTENTION : Envoyez une copie du dossier complet au Secrétariat de la spécialité (par la poste ou par courrier électronique), en plus du dossier original adressé à l'UFR de Sciences.**

Nous limitons les promotions de M2 à 16 étudiants.

Table des matières

1 Synthèse de la formation	3
1.1 Première année : S1 & S2 (M1)	3
1.2 Seconde année : S3 & S4 (M2)	4
1.3 Exemples de parcours	4
1.4 Modalités d'inscription en M1	7
1.5 Modalités d'inscription en M2	7
1.6 Diplômes intermédiaires transitoires	7
1.7 Passerelles vers les autres spécialités ou mentions	7
2 Débouchés professionnels	8
2.1 Préparation à l'agrégation	8
2.2 Recherche fondamentale	8
2.3 Recherche appliquée et ingénierie mathématique	8
3 Objectifs pédagogiques	9
3.1 Cryptographie	9
3.2 Calcul formel	10
3.3 Automatique	10
3.4 Géométrie algébrique	10
4 Équipe pédagogique et partenaires	10
5 Contenu des cours de S1 & S2 (M1)	12
6 Contenu des cours de S3 & S4 (M2)	15

1 Synthèse de la formation

La formation dure deux ans. La première année est notée M1 et la seconde M2. Le volume horaire global est estimé comme suit :

- **S1** (M1, premier semestre) : 270 heures dont 60 % de TD (Travaux Dirigés) et 40 % de cours.
- **S2** (M1, second semestre) : 216 heures dont 50 % de TD et 50 % de cours.
- **S3** (M2, premier semestre) : 157 heures de cours-TD.
- **S4** (M2, second semestre) : 112 heures de cours-TD.

Le travail personnel est estimé à 480 heures pour chaque semestre de M1, 500 heures pour le premier semestre de M2 et 700 heures pour le dernier semestre.

L'obtention de chacune des deux années est subordonnée à l'obtention de 60 ECTS (*European Credit Transfer System*), répartis selon les règles précisées ci-dessous. La *compensation* annuelle d'une note supérieure ou égale à 7 sur 20 est possible à l'exclusion du projet de M1, du stage de M2, et du séminaire étudiant de M2.

1.1 Première année : S1 & S2 (M1)

Une évaluation du niveau en anglais sera faite au début de l'année. Les étudiants n'ayant pas satisfait au niveau requis devront obligatoirement suivre un module d'anglais de 3 ECTS.

Les modules suivants sont propres à la spécialité ; certains modules doivent être obligatoirement suivis :

S1 (Premier semestre M1)

- Algèbre commutative (6 ECTS) (obligatoire)
- Théorie des nombres et cryptographie (6 ECTS) (obligatoire)
- Cryptographie et sécurité (6 ECTS)

S2 (Second semestre M1)

- Calcul formel (6 ECTS) (obligatoire)
- Géométrie algébrique et topologie (6 ECTS) (obligatoire)
- Géométrie différentielle (6 ECTS)
- Approfondissement (3 ECTS)

Le cursus peut être complété avec des modules d'analyse, de probabilités ou d'informatique des autres spécialités du master, ou, après accord avec les responsables, avec des modules d'autres masters en convention (par exemple le M1 Mathématiques Fondamentales et Appliquées¹ d'Orsay). Néanmoins, les modules les plus adaptés de la mention *Master en Mathématiques et Ingénierie des Mathématiques* de l'université de Versailles – Saint-Quentin-en-Yvelines sont les suivants :

S1 (Premier semestre M1)

- Analyse fonctionnelle appliquée I & II (6 et 6 ECTS)
- Probabilités I (6 ECTS)

S2 (Second semestre M1)

- ÉDP et approximation numérique (6 ECTS)
- Probabilités II (6 ECTS)

Un *Projet scientifique* (6 ECTS) est obligatoire : il s'agit d'un travail personnel ou en petit groupe qui se conclut par la rédaction d'un mémoire et d'une soutenance devant un jury.

¹<http://webens.math.u-psud.fr/~depens/M/Parcours/D4MA10.html>

1.2 Seconde année : S3 & S4 (M2)

Les modules suivants sont proposés en M2 ; certains modules doivent être obligatoirement suivis.

S3 (Premier semestre M2)

- Algorithmique et Langage C I (50% de MSMA420) (obligatoire)
- Courbes algébriques (MSMA311) (6 ECTS) (obligatoire)
- Algèbre commutative et effectivité (MSMA310) (6 ECTS) (obligatoire)
- Algorithmes avancés de la cryptographie, Cryptanalyse (MSMA312) (6 ECTS) (obligatoire pour le parcours cryptographie)
- Modèles et solutions des systèmes linéaires (6 ECTS) (obligatoire pour le parcours automatique)

S4 (Second semestre M2)

- Algorithmique et Langage C II (50% de MSMA420) (obligatoire)
- Courbes elliptiques (MSMA413) (6 ECTS) (obligatoire)
- Complexité algébrique et cryptographie (MSMA412) (6 ECTS) (obligatoire pour le parcours cryptographie)
- Analyse et commande des systèmes linéaires généralisés (6 ECTS) (obligatoire pour le parcours automatique)

Le cursus peut être complété avec des modules des autres spécialités du master, ou, après accord avec les responsables, avec des modules d'autres masters en convention (par exemple le M2 Analyse, arithmétique et géométrie² d'Orsay).

Au second semestre les étudiants doivent obligatoirement participer au *Séminaire étudiant (MSMA418)* (3 ECTS) comptant pour 3 ECTS : le travail consiste en la présentation d'un article de recherche ainsi qu'en la présence active à toutes les présentations.

Un *Mémoire et projet de programmation (MSMA419)* (21 ECTS) doit être réalisé sous la responsabilité d'un enseignant-chercheur associé au master. L'étudiant doit 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. La soutenance a lieu devant un jury constitué du responsable du stage et d'au moins un autre membre de l'équipe pédagogique de la spécialité.

Les prérequis indispensables pour les étudiants arrivant en deuxième année sont essentiellement les concepts algébriques usuels sur les corps finis, les anneaux noetheriens et factoriels, les anneaux de polynômes et séries à plusieurs variables, les réductions et décompositions en algèbre linéaire sur un corps, et enfin les premiers outils en géométrie algébrique (principalement la définition d'une variété affine).

1.3 Exemples de parcours

Les parcours ci-dessous ne sont que des exemples. Les parcours précis seront établis en début d'année par l'étudiant en accord avec les responsables de la formation.

Cryptographie

Cette spécialisation débouche à la fois sur la recherche approfondie (universités et grands organismes), la recherche appliquée (Oberthur, SFR) et sur les applications professionnelles (sécurité informatique, problèmes de certification, d'authentification).

S1 (M1) :

- Algèbre commutative (6 ECTS)
- Théorie des nombres et cryptographie (6 ECTS)
- Cryptographie et sécurité (6 ECTS)
- Probabilités I (6 ECTS)

S2 (M1) :

- Géométrie différentielle (6 ECTS)
- Géométrie algébrique et topologie (6 ECTS)
- Calcul formel (6 ECTS)

²<http://webens.math.u-psud.fr/~depens/M/Parcours/D5MAAAG.html>

- Projet scientifique (6 ECTS)

S3 (M2) :

- Courbes algébriques (MSMA311) (6 ECTS)
- Algorithmique et Langage C I (50% de MSMA420)
- Algorithmes avancés de la cryptographie, Cryptanalyse (MSMA312) (6 ECTS)
- Algèbre commutative et effectivité (MSMA310) (6 ECTS)

S4 (M2) :

- Courbes elliptiques (MSMA413) (6 ECTS)
- Algorithmique et Langage C II (50% de MSMA420)
- Complexité algébrique et cryptographie (MSMA412) (6 ECTS)
- Séminaire étudiant (MSMA418) (3 ECTS)
- Mémoire et projet de programmation (MSMA419) (21 ECTS)

Géométrie et Calcul formel

Cet exemple de parcours touche les applications des méthodes algébriques à la géométrie algébrique effective. La formation dispensée permet en outre aux étudiants d'envisager une préparation à l'agrégation après le master : les cours Algèbre commutative (6 ECTS), Calcul formel (6 ECTS) et Théorie des nombres et cryptographie (6 ECTS) couvrent le programme de l'option *Algèbre et calcul formel* de l'épreuve de modélisation du concours de l'agrégation externe en mathématiques.

S1(M1) :

- Algèbre commutative (6 ECTS)
- Théorie des nombres et cryptographie (6 ECTS)
- Cryptographie et sécurité (6 ECTS)
- Probabilités I (6 ECTS)

S2 (M1) :

- Géométrie différentielle (6 ECTS)
- Géométrie algébrique et topologie (6 ECTS)
- Calcul formel (6 ECTS)
- Projet scientifique (6 ECTS)
- Probabilités II (6 ECTS) (en vue de l'agrégation)

S3 (M2) :

- Courbes algébriques (MSMA311) (6 ECTS)
- Algèbre commutative et effectivité (MSMA310) (6 ECTS)
- Algorithmes avancés de la cryptographie, Cryptanalyse (MSMA312) (6 ECTS)
- Algorithmique et Langage C I (50% de MSMA420)

S4 (M2) :

- Courbes elliptiques (MSMA413) (6 ECTS)
- Algorithmique et Langage C II (50% de MSMA420)
- Séminaire étudiant (MSMA418) (3 ECTS)
- Mémoire et projet de programmation (MSMA419) (21 ECTS)
- à compléter avec par exemple un module d'Orsay.

Automatique, une approche algébrique

Cet exemple de parcours touche les applications des méthodes algébriques à la théorie du contrôle, l'automatique et d'une façon générale au traitement de l'information par des méthodes formelles. La formation dispensée permettra en outre aux étudiants d'envisager une insertion professionnelle dans une entreprise de robotique, télécommunication. . .

S1(M1) :

- Algèbre commutative (6 ECTS)
- Théorie des nombres et cryptographie (6 ECTS)
- Analyse fonctionnelle I et II (6 et 6 ECTS)

S2(M1) :

- Géométrie différentielle (6 ECTS)
- Géométrie algébrique et topologie (6 ECTS)
- Calcul formel (6 ECTS)
- Projet scientifique (6 ECTS)
- ÉDP et approximation numérique (6 ECTS)

S3(M2) :

- Courbes algébriques (MSMA311) (6 ECTS)
- Algèbre commutative et effectivité (MSMA310) (6 ECTS)
- Modèles et solutions des systèmes linéaires (6 ECTS)
- Algorithmique et Langage C I (50% de MSMA420)

S4(M2) :

- Analyse et commande des systèmes linéaires généralisés (6 ECTS)
- Algorithmique et Langage C II (50% de MSMA420)
- Séminaire étudiant (MSMA418) (3 ECTS)
- Mémoire et projet de programmation (MSMA419) (21 ECTS)
- à compléter avec par exemple un module d'Orsay.

1.4 Modalités d'inscription en M1

Les modalités d'inscription sont disponibles à l'adresse internet suivante :

www.uvsq.fr/inscriptions

1.5 Modalités d'inscription en M2

Les formulaires d'inscription en M2 doivent être envoyés si possible avant le 31 mai 2009 pour les non titulaires d'une maîtrise ou d'un M1 français, le 31 août 2009 pour les autres. Les réponses seront communiquées le plus tôt possible après réception de chaque dossier. Passées ces dates, les dossiers seront examinés au cas par cas. **ATTENTION : Envoyez une copie du dossier complet au Secrétariat de la spécialité (par la poste ou par courrier électronique), en plus du dossier original adressé à l'UFR de Sciences.** Nous limitons les promotions à 16 étudiants.

Étudiants étrangers : Les étudiants étrangers sont invités à joindre un curriculum vitæ détaillé, avec les matières suivies selon les années, leur volume horaire et les notes obtenues (en indiquant l'échelle). Aussi, une lettre de recommandation d'un enseignant de l'université d'origine sera appréciée.

Le formulaire de candidature peut être téléchargé sur le site internet :

www.math.uvsq.fr/ma2

Si vous ne disposez pas de connexion internet, vous pouvez demander le formulaire par courrier ou le retirer directement au secrétariat de la spécialité :

Secrétariat du Département de Mathématique
Université de Versailles – Saint-Quentin-en-Yvelines
bâtiment Fermat
45, avenue des États-Unis
F-78035 Versailles cedex (France).

Dans ce cas, la demande doit *impérativement* préciser que vous souhaitez recevoir le formulaire relatif à la spécialité *Algèbre Appliquée* et doit être accompagnée d'une enveloppe format A4 avec votre adresse, timbrée à 1,35 euros.

Principaux critères de sélection pour l'admission en M2. Le M2 est accessible après sélection sur dossier, à des étudiants ayant validé un M1 (ou une maîtrise) de Mathématiques, de Mathématiques-Informatique, d'Informatique, ou 60 ECTS équivalents à un des M1 précédents. Les autres diplômes sont examinés dans le cadre de la validation des études. Les dossiers des salariés sont examinés dans le cadre de la validation des acquis professionnels et de la formation continue.

1.6 Diplômes intermédiaires transitoires

À titre transitoire, la Maîtrise « Sciences et technologies », mention « Mathématique et Ingénierie des Mathématiques », est délivrée après validation de l'année M1.

1.7 Passerelles vers les autres spécialités ou mentions

Les passerelles entre les différentes spécialités de la mention sont complètes puisque toutes les spécialités M1 permettent de postuler à toutes les spécialités M2. Les étudiants sont admis à suivre le M2 de leur choix après examen de leur dossier de candidature et l'avis favorable de l'équipe pédagogique. Le M1 proposé dans chaque spécialité est un indicatif préférentiel de parcours pour suivre dans les meilleures conditions la spécialité ; il n'est pas une obligation de parcours pour accéder au M2 de la spécialité. Après accord avec les responsables de la spécialité, il est possible de valider des cours d'algorithmique, d'algèbre appliquée ou de géométrie algébrique de tout autre master européen.

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, la robotique et le traitement du signal. Nous distinguons trois principaux types de débouchés :

- La préparation au concours de l'agrégation externe de mathématiques³ ;
- La recherche fondamentale en géométrie algébrique, calcul formel, cryptographie ;
- La recherche appliquée et l'ingénierie mathématique.

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. La formation dispensée permet en outre aux étudiants d'envisager une préparation à l'agrégation après le master : les cours *Algèbre commutative (6 ECTS)*, *Calcul formel (6 ECTS)* et *Théorie des nombres et cryptographie (6 ECTS)* couvrent le programme de l'option *Algèbre et Calcul Formel* de l'épreuve de *modélisation* du concours de l'agrégation externe en mathématiques, proposée pour la session 2007. Des informations sur cette épreuve sont disponibles sur le site <http://agreg.org>. Soit l'étudiant s'arrête au niveau M1, soit il continue en M2 en suivant un parcours du type *Géométrie et Calcul formel*, qui renforcera considérablement ses connaissances théoriques en vue de l'épreuve orale de modélisation, et qui le conduira ainsi à la préparation au concours dans des conditions optimales.

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 (SOciété du FuTur, SOFT), 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.

³<http://education.gouv.fr/siac2>

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, du laboratoire PRISM, 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.

Automatique, une approche algébrique

La spécialisation *Automatique* sera à même de fournir les notions algébriques indispensables à la résolution de problèmes en automatique et théorie du contrôle. La résolution de tels problèmes s'avère de plus en plus nécessaire dans l'industrie, et les fondements théoriques demeurent absents du cursus classique de l'ingénieur français. B. Marinescu est ingénieur-chercheur RTE-EDF et maître de conférences PAST SATIE-ENS Cachan.

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, ils 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 devenant 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 va offrir de nombreuses possibilités 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 vraiment 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.

3.3 Automatique

Cette option donne des moyens modernes d'analyse et commande des systèmes dynamiques pour les futurs chercheurs en théorie des systèmes et ingénieurs R&D des différentes branches de l'ingénierie. Les systèmes dynamiques posent différents types de problèmes : modélisation, traitement de l'information, analyse et commande. Traditionnellement, les systèmes sont décrits par des matrices de transfert (dans le cas linéaire), des réalisations d'état, etc. Ces modes d'appréhension des systèmes, qui supposent connues par avance les variables d'entrée et de sortie (commandes et mesures) et qui s'appuient sur un formalisme particulier, sont inadéquates dans des nombreux cas. Cette option propose une approche intrinsèque fondée sur l'analyse algébrique. Elle est plus générale, donne un meilleur reflet de la « vision systémique », et fédère plusieurs domaines de l'ingénierie. Cette approche fournit des méthodes de résolution plus directes en pratique et qui peuvent se mettre en œuvre par du calcul formel. Ces méthodes ont permis de résoudre des problèmes industriels ; certains d'entre eux sont utilisés pour illustrer les cours.

Par ailleurs, des exemples complets d'applications industrielles seront présentés par des intervenants des entreprises avec lesquelles les animateurs de cette option travaillent, notamment EDF-Réseau de Transport d'Electricité (RTE), Commissariat à l'Energie Atomique (CEA) et Peugeot-Citroën (PSA), invités pour des présentations ponctuelles dans les cours.

3.4 Géométrie algébrique

Après accord avec les responsables, les modules d'algèbre et géométrie d'autres universités peuvent être suivis et conduire ainsi à un doctorat en algèbre et géométrie.

4 Équipe pédagogique et partenaires

- LMV (ancien LAMA)⁴ : 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).

Martin Andler (Pr), Vincent Cossart (Pr), Monique Lejeune-Jalabert (DR CNRS), Mireille Martin-Deschamps (Pr), Ariane Mézard (Pr), David Hernandez (CR CNRS), Olivier Piltant (CR CNRS),

⁴<http://www.math.uvsq.fr/lmv>

Grégoire Lecerf (CR CNRS), Aurélie Cortez (MdC), Mohamed Krir (MdC), Guillermo Moreno-Socías (MdC), Nicolas Pouyanne (MdC).

- PRiSM⁵ : Laboratoire d'Informatique, Université de Versailles – Saint-Quentin-en-Yvelines, 45, avenue des États-Unis, F-78035 Versailles cedex (France).

Louis Goubin (Pr), Antoine Joux (Pr ass.), Jacques Patarin (Pr), Michaël Quisquater (MdC).

Équipes et laboratoires extérieurs :

- SATIE-ENS Cachan⁶, Équipe Traitement de l'Information et Multicapteurs, 61 Avenue du Président Wilson, 94235 Cachan Cedex. Bogdan Marinescu (Chercheur PAST), Henri Bourlès (Pr).
- Département de Mathématiques d'Orsay⁷, Équipe Arithmétique et Géométrie Algébrique, Université Paris-Sud, bât. 425, 91405 Orsay cedex.
- Laboratoire LIX⁸, École polytechnique, 91128 Palaiseau cedex : Marc Giusti (DR CNRS), Jean Moulin-Ollagnier (Pr), François Ollivier (CR CNRS), Éric Schost (MdC).
- Projet Algorithmes⁹, INRIA Rocquencourt, 78153 Le Chesnay : Bruno Salvy (DR INRIA).
- Laboratoire d'Informatique de Paris 6, équipe SPIRAL¹⁰, UMR 7606, Site Passy-Kennedy, 104 av. du Président Kennedy, 75016 Paris : Jean-Charles Faugère (DR INRIA).

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.

Abréviations : Pr (professeur), MdC (maître de conférences), CR (chargé de recherche), DR (directeur de recherche).

⁵<http://www.prism.uvsq.fr>

⁶<http://www.satie.ens-cachan.fr>

⁷<http://www.math.u-psud.fr/~geo>

⁸<http://www.lix.polytechnique.fr>

⁹<http://algo.inria.fr>

¹⁰<http://www-spiral.lip6.fr>

5 Contenu des cours de S1 & S2 (M1)

Les modules suivants sont propres à la spécialité.

ALGÈBRE COMMUTATIVE

6 ECTS

Objectifs.

- anneaux noethériens.
- anneaux factoriels
- théorie des modules.
- suites exactes.
- présentation des modules de type fini.
- modules sur les anneaux principaux.
- invariants de similitudes, forme réduite de Jordan.
- extensions de corps.
- théorème de correspondance de Galois,

Références bibliographiques :

- Fulton, *Algebraic curves*
- Lang, *Algebra*, Addison-Wesley.
- Samuel & Zariski, *Commutative algebra*, 2 volumes, Springer.

Répartition de l'enseignement : Cours 27h, TD 27h.

Enseignant : Ariane Mézard.

GÉOMÉTRIE DIFFÉRENTIELLE

6 ECTS

Objectifs.

- Produit tensoriel, produit extérieur.
- Sous-variétés de \mathbb{R}^n ; espace tangent; fonctions de classe C^p .
- Variétés abstraites; espaces tangents; morphismes.
- Fibré tangent d'une variété.
- Variétés orientables.
- Équations différentielles sur une variété.
- Formes différentielles.
- Géométrie riemannienne des courbes et surfaces.

Références bibliographiques :

- Berger et Gostiaux *Géométrie différentielle : variétés, courbes et surfaces*, PUF.
- Whittaker et Watson, *A Course of Modern Analysis*, Cambridge Mathematical Library.
- Henrici, *Applied and computational analysis II*, Wiley.
- Gantmacher, *The Theory of Matrices*, AMS Chelsea.
- Nehari, *Conformal Mapping*, Dover Publications.

Répartition de l'enseignement : Cours 27h, TD 27h.

Prérequis : Algèbre commutative (6 ECTS)

Enseignants : Martin Andler, Vincent Cossart ou Ariane Mézard.

Objectifs. Théorie des nombres et applications à la cryptographie.

- Arithmétique des entiers et des polynômes.
- Racines primitives modulo n , structure du groupe des unités modulo p^r .
- Corps finis, polynômes cyclotomiques, calculs explicites.
- Réciprocité quadratique.
- Cryptographie à clé publique (fonction à sens unique, exponentielle modulaire, logarithme discret, protocole de Diffie–Hellman, RSA, etc.).

Références bibliographiques :

- Ireland & Rosen, *A Classical Introduction to Modern Number Theory*, Springer.
- Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994.

Répartition de l'enseignement : Cours 27h, TD 27h.

Enseignant : Guillermo Moreno-Socías

CRYPTOGRAPHIE ET SÉCURITÉ

6 ECTS

Objectifs. Grands thèmes de la cryptographie.

- Cryptographie à clé secrète.
- Attaques brutales, attaques par rejeu.
- Attaques à chiffré seul, attaques à clair choisi, attaques à clair et chiffré choisis.
- Attaques interactives et non interactives.
- Chiffrement par flot, chiffrement par blocs.
- Transposition, substitution, schémas de Feistel.
- DES, AES.
- Fonctions à sens unique, fonctions de hachage.
- Algorithmes d'échanges de clés.
- RSA, algorithmes zero-knowledge.
- Applications .
- Preuve de sécurité relative en clé secrète : génération d'aléas, générateurs de fonctions pseudo-aléatoires, la théorie de Luby et Rackoff.
- Introduction à la théorie de la complexité pour la cryptographie : la théorie de la NP-complétude, exemples d'algorithmes cryptographiques basés sur les problèmes NP-complets.

Références bibliographiques :

- Blake, Seroussi et Smart, *Elliptic Curves in Cryptography*, Springer.
- Koblitz, *Algebraic Aspects of Cryptography*, Springer.
- Schneier, *Cours de Cryptographie appliquée*, Wiley.
- Zémor, *Cours de Cryptographie*, Cassini.

Répartition de l'enseignement : Cours 24h, TD 24h

Enseignant : Louis Goubin

Objectifs.

- Algorithmes fondamentaux classiques sur les grands entiers et les polynômes : addition, soustraction, multiplication et division euclidienne.
- Applications de l’algorithme de Euclide.
- Multiplication rapide.
- Division euclidienne rapide.
- Évaluation et interpolation classiques et rapides.
- Résultant.
- Algèbre linéaire rapide.
- Bases de Gröbner.

Références bibliographiques :

- Aho & Hopcroft & Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, 1994.
- Bini & Pan, *Polynomial and matrix computations*, Birkhäuser, 1994.
- Cox & Little & O’Shea, *Ideal, varieties and algorithms*, Springer.
- von zur Gathen et Gerhard, *Modern Computer Algebra*, 2nd edition, Cambridge University Press, 2003.

Répartition de l’enseignement : Cours 27h, TD 27h

Prérequis : Algèbre commutative (6 ECTS)

Enseignant : Guillermo Moreno-Socías

GÉOMÉTRIE ALGÈBRE ET TOPOLOGIE

Objectifs.

- Topologie générale.
- Spectre d’un anneau commutatif. Topologie de Zariski : ouverts, fermés.
- Localisation, points fermés.
- Applications aux anneaux de polynômes à plusieurs variables.

Références bibliographiques :

- Lang, *Algebra*, Addison-Wesley.
- Samuel & Zariski, *Commutative algebra*, 2 volumes, Springer.
- Perrin.
- Hartshorne, *Algebraic Geometry*.

Répartition de l’enseignement : Cours 27h, TD 27h

Enseignants : Vincent Cossart, Mireille Martin-Deschamps ou Ariane Mézard

6 Contenu des cours de S3 & S4 (M2)

ALGÈBRE COMMUTATIVE ET EFFECTIVITÉ (MSMA310)

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)

Enseignants : Mireille Martin-Deschamps, Guillermo Moreno-Socías

COURBES ALGÈBRIQUES (MSMA311)

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)

Enseignants : Mireille Martin-Deschamps, Guillermo Moreno-Socías

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 $GF(2)$.
- Éléments 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

Enseignant : Antoine Joux

COURBES ELLIPTIQUES (MSMA413)

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, genre.
- Courbes elliptiques : généralités, forme de Weierstraß, loi de groupe, appariement de Weil.

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

Enseignants : Mireille Martin-Deschamps, Guillermo Moreno-Socías

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.

Enseignant : Jacques Patarin.

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 résiduosit  quadratique), ainsi que pour tester la primalit  des entiers (Solovay–Strassen, Miller–Rabin, AKS).

Pour le logarithme discret, on verra comment il permet de r soudre le probl me de la « chasse au pirate » (Boneh–Franklin) avec des applications   la diffusion s curis e de contenus audiovisuels. Dans une autre direction, on s'int ressera  galement au probl me 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 d'obtenir des fonctions rares, comme des signatures extr mement courtes (Boneh–Franklin), ou encore des algorithmes de chiffrement « bas s sur l'identit  » (Boneh–Franklin, Boneh–Boyer).

Une autre partie du cours sera consacr e aux cryptosyst mes « multivariables », qui s'appuient sur le probl me MQ de r solution des syst mes d' quations polynomiales quadratiques   plusieurs variables, sur la notion d'isomorphismes de polyn mes (IP), et sur la d termination d'une combinaison lin aire de matrices ayant un petit rang (MinRank). On d taillera 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.

Enseignant : Louis Goubin.

MODÈLES ET SOLUTIONS DES SYSTÈMES LINÉAIRES

6 ECTS

Objectifs. Bases du formalisme algébrique pour l’analyse des systèmes dynamiques. Liens entre modèles formels et solutions analytiques.

- Bases algébriques
- Points de vue formel et analytique.
- Dualité.
- Propriétés structurale : commandabilité et observabilité.

Références bibliographiques :

- H. Bourlès, “Structural Properties of Discrete and Continuous Linear Time-Varying Systems : A Unified Approach”, in : *Advanced Topics in Control Systems Theory*, Lamnabhi-Lagarrigue F., Loría A., Panteley E. (eds.), Chap. 6, pp. 225-280, Springer 2005.
- H. Bourlès, “Structural Properties of Linear Systems-Part II : Structure at Infinity”, in : *Advanced Topics in Control Systems Theory*, Lamnabhi-Lagarrigue F., Loría A., Panteley E. (eds.), Chap. 7, pp. 259-283, Springer 2006.
- M. Fliess, “Some basic structural properties of generalized linear systems”, *Systems and Control Letters*, vol. 15, pp. 391-396, 1990.
- M. Fliess and S.T. Glad, “An Algebraic Approach to Linear and Nonlinear Control”, in *Essays on Control : Perspectives in the Theory and its Applications*, H.L. Trentelman, J.C. Willems eds., Birkhäuser, 1993, pp. 223-267.
- J.-F. Pommaret, “Partial Differential Control Theory”, Vol 1, 2, Kluwer 2001.

- U. Oberst, “Multidimensional Constant Linear Systems”, Acta Applicandae Mathematicae, 20, pp. 1-175, 1990.

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

Prérequis : Algèbre I et II, géométrie différentielle et algébrique, calcul formel

Enseignant : H. Bourlès.

ANALYSE ET COMMANDE DES SYSTÈMES LINÉAIRES GÉNÉRALISÉS

6 ECTS

Objectifs. Mettre en évidence les avantages du formalisme algébrique présenté au premier module pour certains problèmes rencontrés en pratique. Donner des solutions dans les cas non stationnaires et non linéaires.

- Modélisation : choix des entrées
- Poursuite de modèle et découplage
- pôles et zéros
- stabilité et placement de pôles
- systèmes non linéaires : platitude et commande autour d'une trajectoire

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

Prérequis : Algèbre I et II, géométrie différentielle et algébrique, calcul formel, modèles et solutions des systèmes linéaires.

Enseignant : B. Marinescu.