

David R. Kohel

School of Mathematics and Statistics
University of Sydney, F07
NSW 2006 Australie

né le 27 février 1966
Résidence : Australie
Nationalité : Américaine.

kohel@maths.usyd.edu.au
<http://echidna.maths.usyd.edu.au/~kohel>

Tel : 61-2-9351-3279
Fax : 61-2-9351-4534

Éducation

Diplômes universitaires

- Thèse de Mathématiques, Université de Californie à Berkeley, décembre 1996. *Endomorphism rings of elliptic curves over finite fields*. Membres du jury : Hendrik W. Lenstra, Jr. (directeur de thèse), Paul Vojta, John Canny (informatique).
- Licence (Bachelor of Science) en Mathématiques et Licence (Bachelor of Science) en Biochimie, Université de Texas A&M (*Summa cum laude*), mai 1989.

Carrière universitaire

Université de Sydney

- Senior Lecturer (professeur/maître de conférences), Équipe de Théorie des Nombres, depuis janvier 2005.
- Sesqui Lecturer in Cryptography (maître de conférences en cryptographie), Équipe d'Algèbre Computationnelle, 2002–2004.
En 2001, l'Université de Sydney a créé 15 postes permanents, dans des disciplines ciblées, pour la commémoration du 150ième anniversaire de l'université (le sesquicentenniel). Dans ce poste en cryptographie, j'avais la responsabilité de créer un programme d'enseignement en cryptographie dans le département de mathématiques.

Mathematical Sciences Research Institute

- Postdoctorant, août–décembre 2000.

Université de Sydney

- Senior Research Associate (associé de recherche), Équipe d'Algèbre Computationnelle, 1999–2000 et 2001.

Université nationale de Singapour

- Postdoctorant, 1997–1999.

Invitations à l'étranger

- Université Henri Poincaré, Nancy, (Professeur invité) fin avril–juin 2007.
- Université Toulouse le Mirail, GRIMM (Professeur invité) fin novembre–décembre 2005.
- Institut de Technologie de Tokyo (invité par T. Satoh), 11–21 novembre 2005.
- Université de Californie à San Diego (invité par W. Stein), septembre 2005.
- Université de Rome 2, Tor Vergata (invité par R. Schoof), fin novembre–décembre 2002.
- École Polytechnique (invité par F. Morain, LIX), juillet 2001, décembre 2001.
- Reed College (invité par R. Crandall), juin 1998.
- Université de Sydney, (invité par J. Cannon), mai 1998, décembre 1997.

Résumé des Publications

Les thèmes de ma recherche sont l'arithmétique des courbes (elliptiques, hyperelliptiques et modulaires), les algèbres de quaternions (et leurs relations avec les courbes modulaire et courbes de Shimura), le calcul formel en théorie des nombres et en géométrie arithmétique, et les applications en cryptographie et en théorie des codes.

En cours de rédaction

1. *Efficient computation of modular forms using quaternion algebras*, avec L. Dembélé et W. Stein, en cours de rédaction.

Résumé : Nous décrivons un algorithme efficace pour calculer des formes modulaires en utilisant des algèbres de quaternions.

2. *Galois module structure of Weierstrass subgroups*, avec M. Girard, en cours de rédaction.

Résumé : Nous déterminons la structure de module galoisien du sous-groupe de Weierstrass pour chaque strate de la stratification de Vermeulen de l'espace de modules des courbes de genre 3.

3. *An ℓ -adic CM method for genus 2*, en cours de rédaction.

Résumé : J'étends la théorie explicite du relèvement canonique en caractéristique $\ell \neq p$, en utilisant les correspondances qui viennent des (p, p) -isogénies de Richelot ($p = 2$) et décrites dans Carls, Kohel et Lubicz ($p = 3$).

Pré-publications

4. *Cryptography*, 2007.

Résumé : Livre d'introduction basé sur les cours de cryptographie développés à Sydney, avec exercices utilisant le logiciel SAGE.

5. *Higher dimensional 3-adic canonical lifting*, avec R. Carls et D. Lubicz, <http://arxiv.org/abs/math.NT/0607583>, 2006.

Résumé : Nous développons une théorie explicite du relèvement canonique de caractéristique résiduelle 3, au moyen d'une correspondance des valeurs nulles des fonctions thêta qui proviennent des $(3, 3)$ -isogénies.

6. *The p -adic CM method in genus 2*, avec P. Gaudry, T. Houtmann, C. Ritzenthaler, et A. Weng, <http://arxiv.org/abs/math.NT/0503148>, 2005.

Résumé : Nous trouvons une méthode efficace pour la construction p -adique (pour $p = 2$) des invariants des courbes CM, au moyen de la théorie du relèvement canonique des courbes ordinaires en caractéristique 2. La construction utilise une description intégrale de la $(2, 2)$ -isogénie de Richelot entre deux jacobiniennes (suivant le travail de Mestre).

7. *Constructive and destructive facets of torus-based cryptography*, <http://echidna.maths.usyd.edu.au/~kohel/res/index.html>, 2004.

Résumé : Suivant des idées de Rubin et Silverberg pour les tores en cryptographie, je trouve des représentations explicites des tores efficaces au moyen des jacobiniennes généralisées de courbes hyperelliptiques singulières. Je trouve alors des équivalences entre les logarithmes discrets dans certains groupes de Picard et dans les corps finis.

Publications

- ★ 8. *The Weierstrass subgroup of a curve has maximal rank*, avec M. Girard et C. Ritzenthaler, *Bulletin of the London Mathematical Society*, 38, Issue 06, 925-931, 2006.

Résumé : Nous montrons que le groupe engendré par les points de Weierstrass de la courbe générique de genre $g \geq 3$ est maximal, c'est-à-dire $\mathbf{Z}^{g(g^2-1)-1}$.

- ★ 9. *The 2-adic CM method for genus 2 with application to cryptography*, avec P. Gaudry, T. Houtmann, C. Ritzenthaler, et A. Weng, *Asiacrypt 2006 (Shanghai, 2006)*, *Lecture Notes in Comput. Sci.*, **4284**, 114-129, 2006.

Résumé : Nous expliquons comment appliquer notre méthode 2-adique dans le contexte de la cryptographie. En particulier, nous construisons une base de données des invariants CM pour utilisation dans la méthode CM en cryptographie (cf. <http://echidna.maths.usyd.edu.au/~kohel/dbs>).

- ★ 10. *Classification of genus 3 curves in special strata of the moduli space*, avec M. Girard, *Algorithmic Number Theory Symposium (Berlin, 2006)*, *Lecture Notes in Comput. Sci.*, **4076**, 346-360, 2006.

Résumé : Nous décrivons les invariants des courbes de genre 3, de Dixmier et Ohno, et les appliquons à la classification de quelques familles de dimension 1 de courbes spéciales.

- ★ 11. *Efficiently computable endomorphisms for hyperelliptic curves*, avec B. Smith, <http://arxiv.org/abs/math.NT/0603505>, *Algorithmic Number Theory Symposium (Berlin, 2006)*, *Lecture Notes in Comput. Sci.*, **4076**, 495-509, 2006.

Résumé : Dans ce travail nous trouvons des équations explicites pour l'application d'un endomorphisme réel de la jacobienne d'une courbe hyperelliptique dans des familles à multiplication réelle.

- ★ 12. *Efficient scalar multiplication by isogeny decompositions*, avec C. Doche et T. Icart, *Public Key Cryptography (New York, 2006)*, *Lecture Notes in Comput. Sci.*, **3958**, 191-206, 2006.

Résumé : Nous utilisons les décompositions multiplicatives $[\ell] = \hat{\varphi}\varphi$ pour la multiplication scalaire $[\ell]$ ($= 2, 3$) dans quelques familles universelles de courbes elliptiques. En les combinant avec des généralisations du NAF (*non-adjacent form*) pour les représentations éparses des entiers n en sommes additives (avec coefficients ± 1), nous trouvons des formules efficaces pour l'addition sur les courbes elliptiques.

- ★ 13. *The AGM- $X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting*, *Advances in Cryptology – Asiacrypt 2003*, 124-136, *Lecture Notes in Comput. Sci.*, **2894**, Springer, 2003.

Résumé : Dans ce travail, je donne de nouveaux algorithmes pour le comptage de points sur les courbes elliptiques en petites caractéristiques. Ces algorithmes généralisent les algorithmes de Satoh, Mestre, *et al.*, et aussi donnent une construction p -adique pour les invariants de la multiplication complexe sur les courbes $X_0(N)$.

- ★ 14. *Fundamental domains for Shimura curves*, avec H. Verrill, *J. Théorie des Nombres Bordeaux*, **15** (2003), no. 1, 205-222.

Résumé : Nous étudions les groupes d'unités des algèbres de quaternions et leurs actions sur le demi-plan de Poincaré. Nous décrivons un algorithme pour trouver leurs générateurs, leurs domaines fondamentaux, et leurs invariants, avec des exemples explicites.

- ★ 15. *Rational groups of elliptic curves suitable for cryptography*, dans *Proceedings of the Workshop on Cryptography and Computational Number Theory (CCNT'99)*, National University of Singapore, 1999, K.-Y. Lam, I. E. Shparlinski, H. Wang, and C. Xing, eds. Birkhäuser, 2001.

Résumé : Cet article décrit diverses méthodes pour construire des groupes d'ordre premier utilisables en cryptographie. En particulier, on donne plusieurs variantes efficaces des protocoles standard en cryptographie sur les courbes elliptiques.

- ★ 16. *Hecke module structure of quaternions*, dans *Class Field Theory – Its Centenary and Prospect*, K. Miyake, ed., Advanced Studies in Pure Mathematics Series, Mathematical Society of Japan, Kinokuniya Press, Tokyo, Japan 2001.

Résumé : Nous utilisons la théorie des idéaux dans les ordres d'une algèbre de quaternions pour associer un module de Hecke aux courbes de Shimura $X_0^D(N)$ (qui généralisent les courbes modulaires classiques $X_0(N)$). Cet article fournit la première description d'une méthode effective pour déterminer les invariants de ces courbes comme par exemple le groupe des composantes des fibres spéciales ou encore la dimension des facteurs simples des jacobiniennes de ces courbes.

- 17. *On exponential sums and group generators for elliptic curves over finite fields*, avec Igor Shparlinski. dans *Algorithmic Number Theory, Proceedings of ANTS IV*, W. Bosma, ed. *Lecture Notes in Comput. Sci.*, **1838**, Springer, Berlin, 2000.

Résumé : Nous établissons une borne supérieure pour les sommes exponentielles sur les courbes elliptiques. Cela nous permet de prouver l'existence de générateurs dans certains ensembles bornés de points d'une courbe elliptique sur un corps fini. Ce travail borne la complexité d'un algorithme déterministe pour trouver la structure de groupe d'un ensemble de points d'une courbe elliptique.

- ★ 18. *Component groups of quotients of $J_0(N)$* , avec William Stein. dans *Algorithmic Number Theory, Proceedings of ANTS IV*, W. Bosma, ed. *Lecture Notes in Comput. Sci.*, **1838**, Springer, Berlin, 2000.

Résumé : Nous combinons des techniques de mon article *Hecke module structure of quaternions* et de la thèse de Stein pour déterminer les groupes des composantes des fibres spéciales du modèle de Néron des quotients simples de jacobiniennes modulaires $J_0(N)$. L'ordre de ces groupes finis est un des invariants qui apparaissent dans les formules conjecturelles de Birch et Swinnerton–Dyer.

- 19. *Split group codes*, avec San Ling et Cunsheng Ding. *IEEE Transactions on Information Theory*, **46**, no. 2, (2000), pp. 280–284.

Résumé : Nous généralisons la structure implicite d'algèbre de groupe des codes de Reed–Solomon et la construction spécifique des codes duadiques de Pless, pour identifier une classe de codes à étudier. L'analyse de la théorie des idéaux des anneaux artiniens que l'on obtient – élémentaire du point de vue de la théorie des anneaux – nous donne une description explicite et détaillée des codes obtenus. En sélectionnant certaines sous-classes ayant des propriétés optimales, nous pouvons construire des codes avec des paramètres qui améliorent ceux connus dans de nombreux cas (voir, par exemple, la librairie en ligne d'Andries Brouwer).

- 20. *Secret-sharing with a class of ternary codes*, with Cunsheng Ding and San Ling. *Theoretical Computer Science* **246** (2000), no. 1-2, pp. 285–298.

Résumé : L'échange de secret en cryptographie pose le problème de partitionner une information entre plusieurs parties de manière à ce que seules les parties d'une taille critique (et non celles d'une plus petite taille) puisse reconstruire cette information. Nous décrivons un tel protocole utilisant une classe de codes définie sur \mathbf{F}_3 .

21. *Elementary 2-group character codes*, avec San Ling et Cunsheng Ding. *IEEE Trans. Inform. Theory*, **46**, no. 1, (2000), pp. 485–496.

Résumé : Nous déterminons la structure et les invariants d'une classe de codes définie dans l'algèbre d'un groupe 2-abélien élémentaire.

22. *Explicit sequence expansions*, avec San Ling et Chaoping Xing. Proceedings of the International Conference on Sequences and their Applications. National University of Singapore. 14–17 December, 1998.

Résumé : Un outil important pour l'analyse des chiffrements par flot (*stream cipher*) est l'analyse du profil de complexité linéaire de la suite chiffrante. Nous décrivons un algorithme, basé sur une construction de Xing, pour calculer des suites avec des bornes connues sur le profil de complexité linéaire à partir des développements en série entière de certaines fonctions sur une courbe sur un corps fini. Nous déterminons de nombreux exemples, dont une grande partie a été incorporée à la librairie en ligne de suites chiffrantes de Neil Sloane.

23. *Endomorphism rings of elliptic curves over finite fields*, Thesis, University of California Berkeley, 1996.

Résumé : Je traite le problème de déterminer l'anneau d'endomorphismes d'une courbe elliptique sur un corps fini en tant qu'anneau abstrait. Ce problème est naturellement une généralisation du problème de comptage de points sur une courbe elliptique. En effet, l'anneau d'endomorphismes, avec un élément Frobenius distingué détermine le nombre de points. Ce problème se partitionne de manière naturelle en deux cas, le cas ordinaire et le cas super-singulier, avec la théorie de la multiplication complexe servant de thème commun. Ce travail est régulièrement cité comme référence dans le domaine des courbes elliptiques sur les corps finis et dans diverses applications cryptographiques.

Livre édité :

24. *Algorithmic number theory (Sydney, 2002)*, C. Fieker and D. Kohel, eds., *Lecture Notes in Comput. Sci.*, **2369**, Springer, Berlin, 2002.

N.B. En dehors des publications traditionnelles ci-dessus, j'ai écrit des chapitres entiers du *Magma Handbook*, qui incluent *Quaternion Algebras*, *Binary Quadratic Forms*, *Brandt Modules*, *Modular Curves*, *Rational Curves and Conics* (avec P. Leiby), *Module of Supersingular Points* (avec W. Stein), et contribué au chapitres *Lattices*, *Elliptic Curves*, et *Hyperelliptic Curves*. Cela correspond à plusieurs centaines de pages.

★ Exemplaies inclus.

Recherche

N.B. *Dans ce qui suit, les références renvoient à ma liste de publications.*

Depuis ma thèse sur l'arithmétique des courbes elliptiques, je me suis intéressé à de nombreux problèmes concernant les aspects computationnels de la théorie des nombres et de la géométrie arithmétique, et à leurs applications en théorie des codes et en cryptographie. En tant que postdoctorant à l'Université Nationale de Singapour (1997–1999), j'ai étudié diverses applications élémentaires de la théorie des nombres en théorie des codes. En même temps, j'ai continué à m'intéresser aux courbes elliptiques, modulaires et de Shimura. Après plusieurs visites à l'Université de Sydney, j'ai rejoint l'Équipe d'Algèbre Computationnelle en tant que chercheur associé. J'ai implémenté de nombreux algorithmes de haut niveau en théorie des nombres et géométrie arithmétique, en particulier avec G. Brown, nous avons créé l'ossature dans laquelle la géométrie algébrique est développée dans `Magma`. Depuis 2002, j'ai un poste permanent d'enseignant-chercheur. J'ai néanmoins commencé à enseigner un cours de cryptographie dès 2001.

Depuis 2001, j'encadre des étudiants de thèse. Le premier de ces étudiants, Paul Hunter, a commencé un projet sur les surfaces de Humbert et leurs relations aux courbes de Shimura avant d'obtenir une bourse de thèse au sein du département d'informatique de Cambridge. Ben Smith (2002–2005) a récemment terminé sa thèse *Explicit endomorphisms and correspondences* (Endomorphismes explicites et correspondances) dans laquelle il construit un cadre pour représenter les endomorphismes de courbes arbitraires et calculer à l'aide de ces endomorphismes. Dans notre article en commun [11], nous déterminons des expressions efficaces pour représenter les endomorphismes des jacobiniennes de courbes dans des familles à multiplication réelle dues à Mestre, dans une dégénérescence de cette famille apparaissant dans Tautz, Top et Verberkmoes, et dans une famille analogue de Artin et Schreier. L'existence d'endomorphisme efficace est intéressante car elle permet d'accélérer les algorithmes pour la multiplication scalaire dans des applications cryptographiques, tandis que la construction mathématique sous-jacente est indépendamment intéressante.

En ce moment, j'encadre quatre autres étudiants de thèse sur des sujets ayant trait aux formes modulaires, aux variétés abéliennes et à la multiplication complexe, et l'arithmétique des courbes (sur des corps finis, locaux, et globaux). De manière générale, j'essaie d'encourager mes étudiants à travailler sur des sujets ayant un problème computationnel sous-jacent (avec des applications en théorie des codes ou en cryptographie) tout en leur fournissant un prétexte pour étudier des objets fondamentaux en mathématiques. Finalement, j'encadre de nombreux mémoires de fin d'études (voir détails plus loin).

De 2004 à 2006, j'ai bénéficié du recherche du Australian Research Council *p-Adic Methods in Arithmetic Geometry* (*Méthodes p -adiques en géométrie arithmétiques*) pour rechercher des algorithmes p -adiques pour déterminer les fonctions zêta. Le but de ce projet était d'étendre les méthodes de Satoh, de Mestre, de Kedlaya et de Lauter pour le comptage p -adique de points et pour les constructions CM explicites, avec application à la cryptographie (en commençant par ma contribution [13] en la matière). Robert Carls (Ph.D. Leiden) est employé en tant que postdoctorant au sein de ce projet et recherche les fonctions thêta algébriques et leurs applications aux relèvements canoniques. Cette bourse de recherche a financé les séjours à Sydney des chercheurs suivants : Ralf Gerkmann (Mainz), Nicolas Gürel (LIX), Christophe Ritzenthaler (Luminy), David Lubicz (CELAR), Jean-Marc Couveignes (Toulouse), Thierry Henocq (Toulouse) et Peter Stevenhagen (Leiden). Parmi les résultats de ces visites figurent les (pré-)publications [6], [9] avec Gaudry, Houtmann, Ritzenthaler et Weng, et [11] avec

Ritzenthaler et Girard, ainsi que le pré-publication [5] avec Carls et Lubicz. De manière similaire, le problème de recherche posé à Thomas Icart (École Polytechnique) lors de son stage d’“Internship” à Sydney a évolué en la publication [12] en collaboration avec C. Doche de l’Université Macquarie.

L’adoption par la NSA, en 2005, des courbes elliptiques comme standard de cryptage (cf. http://www.nsa.gov/ia/industry/crypto_suite_b.cfm) donne plus de poids aux investigations mathématiques du rôle des courbes et variétés abéliennes en cryptographie. En collaboration avec Christophe Doche et Igor Schparlinski de l’Université Macquarie, nous avons candidaté sur une bourse de recherche *Mathematics of Elliptic Curve Cryptography* (*Les mathématiques de cryptographie à courbes elliptiques*). Ce projet de recherche a des applications cryptographiques bien plus directes.

Thèmes de Recherche

Dans ce qui suit, je décris certains de mes thèmes de recherches en théorie des nombres et géométrie arithmétique, ainsi que des liens éventuels avec la cryptographie.

Arithmétique explicite des courbes et des variétés abéliennes.

Pour utiliser les variétés abéliennes en cryptographie, il faut un modèle explicite pour représenter leurs points et l’arithmétique de leur loi de groupe. En outre, une approche complète de ces objets (leur robustesse et leur vulnérabilité) nécessite une théorie explicite des morphismes de courbes, des jacobiniennes et des variétés abéliennes. Finalement, je m’intéresse aux constructions explicites pour les courbes ou les variétés abéliennes ayant des structures particulières. La théorie et les algorithmes pour de telles constructions sont essentiels en cryptographie, mais fournissent aussi des outils pour l’étude du comportement arithmétique sur les corps globaux.

Arithmétique des courbes modulaires.

Les courbes modulaires $X_0(N)$ (et leurs analogues, les courbes de Shimura $X_0^D(N)$) jouent un rôle fondamental en théorie des nombres, que ce soit dans l’étude des conjectures de Birch et Swinnerton-Dyer ou dans la preuve du théorème de Fermat (au moyen des représentations galoisiennes). En tant qu’espaces de paramétrisation pour les courbes elliptiques ayant une isogénie cyclique d’ordre N , elles jouent un rôle important dans les algorithmes explicites pour construire des isogénies et pour la décomposition des structures de torsion de $E[N]$ dans l’algorithme de Schoof-Elkies-Atkin.

Afin d’étudier les invariants des courbes modulaires comme $X_0(N)$, il est nécessaire d’avoir une théorie explicite pour calculer avec des formes modulaires. Dans ce but, je m’intéresse aux algorithmes pour les symboles modulaires, à la méthode des graphes (de Mestre et Oesterlé, et les algorithmes mathématiquement équivalents de Pizer) et aux constructions analogues utilisant les classes d’isométrie de réseaux de genre donné (ainsi qu’étudiées par Birch, Kneser, Schultze-Pillot).

Une application de ces algorithmes apparaît dans mon article avec Stein [18]; de plus amples développements du côté algorithmique est en cours d’investigation avec Dembélé et Stein [1]. Aussi avec Dembélé et Stein (entre autres), nous avons organisé une école d’été à Berkeley pour les étudiants de thèse (au Mathematical Sciences Research Institute) dont le sujet était précisément les méthodes computationnelles pour les formes modulaires.

Espaces de modules des courbes et variétés abéliennes explicites.

Comme préliminaire à l'étude des propriétés arithmétiques des courbes et des variétés abéliennes, les méthodes classiques de la théorie des invariants et des fonctions thêta fournissent un moyen de déterminer des invariants géométriques. Pour les courbes de genre 1 et 2, l'invariant j et les invariants de Igusa et Clebsch fournissent un moyen de classifier ces courbes. Dans un travail en commun avec R. Carls et D. Lubicz [5] sur les méthodes de relèvement p -adique, nous utilisons la théorie des fonctions thêta pour décrire l'espace de modules des invariants des variétés abéliennes, analogue des courbes $X_0(N)$ en dimension 1. Pour les courbes de genre 3, un ensemble complet d'invariants pour la partie non-hyperelliptique de l'espace de modules des courbes de genre 3 (espace de dimension 6) n'a été que récemment déterminé par Ohno, en complétant les résultats de Dixmier (en combinant la théorie des invariants du 19ième siècle et les outils de calcul formel). Cela fournit un outil pour la classification des courbes de genre 3; en collaboration avec M. Girard [8], nous l'utilisons pour déterminer les invariants de strates de petites dimensions dans cet espace de modules (décrites de manière canonique en fonction de leur points de Weierstrass). Cela sert de base à l'étude de l'aspect arithmétique des structures associées de modules galoisiens engendrées par les points de Weierstrass [2].

Nouvelles constructions cryptographiques.

Les variétés abéliennes de petite dimension sont choisies en cryptographie car il n'existe pas d'attaque sub-exponentielle (connue) du problème du log discret. D'autre part, elles admettent de nouvelles constructions comme la cryptographie basée sur les accouplements.

Afin de trouver de nouvelles constructions et de comprendre leurs vulnérabilités, il est important de développer des algorithmes ainsi que la théorie pour calculer dans (1) les variétés sub-abéliennes d'une jacobienne (appelées "sous-groupes de trace zéro" dans le travail de T. Lange), (2) les quotients de variétés abéliennes (par exemple, les variétés de Kummer qui ont une multiplication scalaire, mais pas de loi de groupe, exploitée dans l'addition de Montgomery), (3) les variétés abéliennes ayant des structures d'automorphismes ou d'endomorphismes particulières et (4) les variétés abéliennes dégénérées (comme le tore algébrique décrit dans les jacobiniennes généralisées de [7]).

Le développement d'algorithmes constructifs pour représenter les variétés abéliennes et pour travailler avec celles-ci est au centre de l'investigation de leurs structures quel que soit le corps, mais pour les applications cryptographiques, je m'attends à ce qu'un tel cadre soit essentiel pour comprendre les problèmes d'ordre sécuritaires et pour les aborder, ainsi que pour trouver de nouvelles applications.

Autres Activités de Recherche

Bourse de recherche du Australia Research Council

- *p-Adic Methods in Arithmetic Geometry (Méthodes p-adiques en géométrie algébrique)*, 2004–2006 (montant 210 000 AU\$). Le programme de recherche de ce projet concerne les méthodes p -adiques effectives pour la détermination des ordres de jacobiniennes de courbes algébriques, dans le but d'une application cryptographique.

Recherche en Algèbre Computationnelle

MAGMA. Depuis 1997, comme postdoctorant à Singapour, j'ai contribué au logiciel **Magma** avec du code pour les isogénies des courbes elliptiques. De 1999 à 2002, j'ai participé au développement de code et de documentation pour le système d'algèbre computationnelle **Magma**, ainsi qu'à la conception et à l'intégration de modules de géométrie algébrique et de théorie des nombres. En particulier, cela inclut un modèle computationnel pour les schémas (avec G. Brown) ; des algorithmes pour les courbes de petit genre, en particulier, les coniques, les courbes elliptiques et hyperelliptiques ; les structures d'isogénies pour les courbes elliptiques, les courbes modulaires et les isogénies paramétrées ; SEA et l'algorithme p -adique de comptage de points $AGM-X_0(N)$; les formes quadratiques binaires et les groupes de classes des ordres quadratiques non-maximaux ; théorie locale-globale des réseaux ; les algèbres de quaternion et les modules de Brandt associés ; les modules des points supersinguliers (avec W. Stein) ; les sous-groupes de congruence de $SL_2(\mathbf{Z})$ et groupes des unités des quaternions ; actions sur le demi-plan complexe supérieur et les invariants des courbes de Shimura (avec H. Verrill) ; les anneaux de Witt.

Références :

<http://echidna.maths.usyd.edu.au/~kohel/alg/>
<http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm>

SAGE. Depuis 2005 j'ai participé au développement du logiciel **SAGE**, créé par W. Stein, un système moderne et orienté objet (écrit dans python), avec des interfaces vers d'autres logiciels comme GAP, Maxima, PARI, et Singular. En particulier, avec Stein, j'ai développé les concepts de catégories et de morphismes entre objets, et écrit du code pour les monoïdes, algèbres, et schémas.

Références :

<http://echidna.maths.usyd.edu.au/sage>
<http://www.sagemath.org/sage>

Encadrement d'étudiants (Université de Sydney)

Encadrement de thèses

- Ben Smith, 2002–2005, *Explicit endomorphisms and correspondences (Endomorphismes explicites et correspondances)*, 2006.
- David Gruenewald, thème de recherche : aspects computationnels des formes modulaires, commencée en 2004.
- Steve Ward, thème de recherche : algorithmes de preuve de multiplication complexe des variétés abéliennes, commencée en 2005.
- Ley Wilson, thème de recherche provisoire : théorie du corps de classes et variétés abéliennes ayant partout bonne réduction, commencée en 2006.
- Hamish Ivey-Law, commencée en 2007.

Encadrement d'étudiants étrangers

- Thomas Icart (École Polytechnique), *Cryptologie : multiplication scalaire sur les courbes elliptiques*, stage d'informatique, 2005.
- Alex Unger (Leipzig), étude des courbes elliptiques et des variétés abéliennes, 2005.

Encadrement de mémoires de fin d'études (Honours thesis)

La quatrième année d'université permet aux étudiants d'obtenir leur diplôme avec mention. Pour cela, ils doivent suivre des cours généraux et rédiger un mémoire d'une soixantaine de pages.

- Graeme Pope, *Efficient arithmetic on elliptic and hyperelliptic curves (Arithmétique des courbes elliptiques et hyperelliptiques)*, 2006.
- Gareth White, *Heights on elliptic curves (Hauteurs sur les courbes elliptiques)*, 2006.
- Zhuo Jia Dia, *Algebraic geometric coding theory (Codes géométriques)*, 2006.
- Hamish Ivey-Law, *Rational points on higher genus curves (Points rationnels sur les courbes de genre supérieur)*, (co-encadré avec M. Girard), 2006.
- David Gruenewald, *An introduction to modular forms (Une introduction aux formes modulaires)*, 2003.
- Gordon Childs, *Counting points on hyperelliptic curves over finite fields (Comptage de points des courbes hyperelliptiques sur des corps finis)*, 2001.
- Quy Tuan Nguyen, *Binary quadratic forms (Formes quadratiques binaires)*, 2000.

Vacation Scholars

L'Université de Sydney donne la possibilité (sur dossier) aux étudiants inscrits en quatrième année de travailler sur un projet de recherche pendant six semaines l'été.

- Jacky Chow (Fonctions elliptiques et fonctions abéliennes), 2005.
- Graeme Pope (Courbes elliptiques et cryptographie), 2005.
- Gareth White (Groupes de Mordell-Weil des courbes elliptiques), 2005.
- Peter McNamara (Courbes elliptiques), 2004.
- Quy Tuan Nguyen (Formes quadratiques), 2000.

Enseignement

Développement de cours et expérience d'enseignement

Les cours à l'Université de Sydney existent à deux niveaux de difficulté : “ordinaire” pour la plupart des étudiants et “avancé” pour les bons étudiants. Ci-dessous ne figurent que les cours pour lesquels j'ai donné des cours magistraux. À ceux-ci s'ajoutent des travaux dirigés dans des sujets variés. Les deux cours de cryptographie (MATH3024 et MATH3925) créés lors de mon emploi *Lecturer in Cryptography* sont détaillés à la page suivante, ainsi qu'un cours intensif dérivé de ces deux cours pour l'école d'été australienne.

Enseignement à l'Université de Sydney

- *Cryptographie*, AMSI/ICE-EM Summer School, Un cours intensif à l'école d'été de l'Australian Mathematical Sciences Institute, pour les étudiants de master et étudiants de thèse (24 heures + 4 heures de TD).
- *Algèbre commutative*, 1er semestre 2005, 2006, Cours de quatrième année en algèbre commutative, traitant les quatre premiers chapitres de Atiyah–Macdonald (26 heures).
- MATH 3067 *Information and Coding Theory (Théorie de l'information et des codes)*; niveau ordinaire, 2ième semestre, 2006 et 2007 (prévu). Un cours magistral de 3ième année en deux parties; je suis responsable pour la deuxième partie sur la théorie des codes (13 heures).
- MATH 3024, *Elementary Cryptography and Protocols (Cryptographie élémentaire et protocoles)*; niveau ordinaire, 1er semestre, 2001, 2002, 2003, 2004. Ce cours présente aux étudiants les principes de base de la cryptographie et de la crypto-analyse. J'ai développé le cours, ainsi que le matériel de travaux dirigés (en partie sur ordinateur). J'ai aussi créé un module de cryptographie (pour Magma) pour que les étudiants puissent mettre en pratique les méthodes étudiées en cours (26 heures de cours + 12 heures de TD).
- MATH 3925, *Public Key Cryptography (Cryptographie à clef publique)*; niveau avancé, 2ième semestre, 2002, 2003, 2004. Ce cours traite des fondements mathématiques pour la construction et l'analyse des systèmes cryptographiques à clef publique : RSA, ElGamal, et cryptographie sur les courbes elliptiques (26 heures de cours + 12 heures de TD).
- MATH 2061, *Linear Mathematics (Algèbre linéaire)*; niveau ordinaire, 1er semestre, 2007. Ce cours introduit la théorie des espaces vectoriels et les bases de l'algèbre linéaire aux étudiants de deuxième année, suivi par environ 400 étudiants, répartis entre deux salles d'exposés (18 heures).
- MATH 1003, *Integral Calculus and Modelling (Calcul intégral et modélisation)*; niveau ordinaire, 2ième semestre, 2003, 2004, 2006, 2007 (prévu). Il s'agit d'un cours magistral de première année, suivi par environ 1200 étudiants, répartis entre quatre salles d'exposés (26 heures).
- *Elliptic Curves and Cryptography (Courbes elliptiques et cryptographie)*, 2003 et 2004; et *Mathematics of Cryptography (Les mathématiques de la cryptographie)*, 2007. Série d'exposés dans le cadre du programme destiné aux étudiants talentueux (Talented Student Programme) (6 heures).

Enseignement en France (en français)

- *Analyse*, (Université de Toulouse II), 2005, Notions d'analyse : étude des suites, séries, et suites de fonctions (six heures d'exposés aux étudiants de deuxième année en tant que professeur invité).

Enseignement aux États Unis

- *Summer Graduate Workshop in Computational Number Theory*, Mathematical Sciences Research Institute, Berkeley (organisé par W. Stein), du 31 juillet au 11 août 2006. Exposés sur les aspects computationnels des formes modulaires, avec L. Dembélé, P. Gunnels, W. Stein, G. Weise.

Développement de Cours en Cryptographie

J'ai commencé le poste de *Lecturer en Cryptographie* en 2002, mais j'ai créé le premier de ces deux cours en cryptographie en 2001. Chaque cours représente 26 heures de cours et 12 heures de TD.

MATH3024 *Cryptographie élémentaire et protocoles*. Ce cours présente aux étudiants les principes de base de la cryptographie et de la crypto-analyse. Des notes d'exposés et de TD se trouvent sur ma page web :

<http://echidna.maths.usyd.edu.au/~kohel/tch/MATH3024>

Les concepts principaux sont :

- Cryptographie élémentaire : définitions et concepts élémentaires de la cryptographie, les schémas de cryptographie classiques : substitution, transposition, chiffrements de Vernam et de Vigenère, et machines de chiffrement.
- Cryptanalyse élémentaire : méthodes pour rendre vulnérables les chiffrements classiques.
- Théorie de l'information : théorie de Shannon.
- Les schémas de chiffrement par blocs : les schémas de Feistel, DES, 3DES, AES, et leurs modes d'opération : ECB, CBC, CFB, OFB.
- Les schémas de chiffrement par flot : concepts de chiffrements synchrone et asynchrone, LFSR, complexité linéaire, l'algorithme de Berlekamp–Massey.
- Arithmétique de $\mathbf{Z}/n\mathbf{Z}$ et \mathbf{F}_q .
- Protocoles de chiffrement symétriques et asymétriques, et les principaux chiffrements à clef publique : RSA et ElGamal.
- Autres protocoles : partage de secret (protocole de Shamir), les fonctions hash, les MAC, signatures électroniques, et l'argent électronique.

Pour les TD, j'ai développé un module pour Magma autour d'une implémentation d'un schéma de chiffrement $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$, où \mathcal{K} , \mathcal{M} , et \mathcal{C} représentent les espaces de clefs, de messages clairs, et de messages chiffrés. Ce module est accessible à la page web ci-dessus.

MATH3925 *Cryptographie à clef publique*. Ce cours traite des fondements mathématiques pour la construction et l'analyse des systèmes cryptographiques à clef publique. Je traite les algorithmes pour la primalité, la factorisation, les logarithmes discrets ; les relations entre ces problèmes et les chiffres RSA, ElGamal ; la cryptographie sur les courbes elliptiques. Des notes de TD se trouvent sur ma page web :

<http://echidna.maths.usyd.edu.au/~kohel/tch/MATH3925>

N.B. Depuis 2005, suite à des réformes du curriculum, nous n’enseignons plus ces cours dans leur forme originelle (e.g. théorie de nombres élémentaire et cryptographie se trouvent dans un nouveau cours MATH2068).

Cryptographie. Un cours intensif à l’école d’été de l’Australian Mathematical Sciences Institute, pour les étudiants de master et étudiants de thèse.

<http://echidna.maths.usyd.edu.au/~kohel/tch/Crypto>

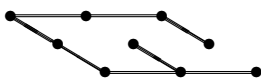
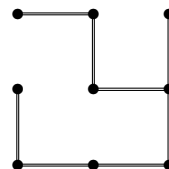
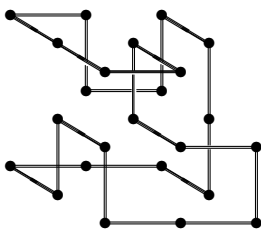
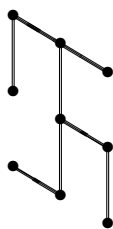
Administration

Université de Sydney

- Création de l’Équipe de Théorie des Nombres, 2005.
- Vice-président de la *Commission informatique*, 2003–2005 et président depuis 2006 ; membre du *Conseil d’administration*, 2002–2006.
- Organisateur, *Elliptic Curves and Higher Dimensional Analogues (ECHIDNA)*, Université de Sydney, 2002, et *ECHIDNA II*, Université de Sydney, 2005.
- Organisateur, *Algorithmic Number Theory Symposium V*, avec J. Cannon et C. Fieker, Université de Sydney, 7–12 juillet 2002,
- Editeur, *Algorithmic number theory (Sydney, 2002)*, Proceedings of Algorithmic Number Theory Symposium V, avec C. Fieker, *Lecture Notes in Comput. Sci.*, **2369**, Springer, Berlin, 2002.
- Organisateur, *Séminaire d’algèbre computationnelle*, 2001–2002, et *Séminaire de théorie des nombres*, 2003–2005.
- Supervision de programmeurs en théorie des nombres et géométrie arithmétique, Équipe d’Algèbre Computationnelle, Université de Sydney, 1999–2002.

Referee pour les bourses de recherches et publications

- Australia Research Council depuis 2003 et Royal Grant Council, Hong Kong, 2004.
- Jury de thèse, Mireille Fouquet, École Polytechnique (LIX), 2001.
- Referee pour les journaux and conférences *Algorithmic Number Theory Symposium*, *Experimental Mathematics*, *Finite Fields and Applications*, *IEEE Transactions on Information Theory*, *Journal of Complexity*, *Mathematics of Computation*, etc.



Conférences et Exposés

- *Summer Graduate Workshop in Computational Number Theory*, Mathematical Sciences Research Institute, (organisé par W. Stein). Exposés sur les aspects computationnels des formes modulaires, avec L. Dembélé, P. Gunnels, W. Stein, G. Weise, du 31 juillet au 11 août 2006.
- *Classification of genus 3 curves in special strata of the moduli space* (avec M. Girard) et *Efficiently computable endomorphisms for hyperelliptic curves* (avec B. Smith), Algorithmic Number Theory Symposium VII (Berlin), 23–28 juillet 2006.
- *On invariants of plane quartics, MAGMA Workshop on Computational Number Theory*, Université de Sydney, 22 mars 2006.
- *SAGE notions of computing with schemes*, SAGE Days, U.C. San Diego, 5 février 2006.
- *Construction p -adique des invariants CM des courbes de genre 2*, Université de Bordeaux, 16 décembre 2005.
- *Construction p -adique des invariants CM des courbes de genre 2*, Université de Toulouse Le Mirail, 12 décembre 2005.
- *Tores algébriques et jacobiniennes généralisées en cryptographie*, Institut de Mathématiques de Luminy, 8 décembre 2005.
- *Constructive p -adic CM for genus 2 curves*, Université Chuo, Tokyo, 19 novembre 2005.
- *Constructive p -adic CM for genus 2 curves*, Institut de Technologie de Tokyo, 15 novembre 2005.
- *Explicit methods in number theory*, Oberwolfach, 17–23 juillet 2005.
- *An ℓ -adic CM method for genus 2*, XXIVièmes Journées Arithmétiques, Marseille, 4–8 juillet 2005.
- *Introduction to Magma and Applications*, Institut africain pour les sciences mathématiques, Afrique du Sud, 2 février 2005.
- *Constructing CM invariants of genus 2 curves, Workshop on Arithmetic Geometry, Related Areas, and Applications*, Université de Stellenbosch, 1 février 2005.
- *Igusa class invariants via p -adic lifting*, ECHIDNA II, 12–14 janvier 2005.
- *Igusa class invariants and the AGM, Magma Workshop*, Université Georg-August, Göttingen, 11–15 décembre 2004.
- *Constructive CM by p -adic lifting, Effective Methods in Arithmetic Geometry*, Institut Henri Poincaré, 6–10 décembre 2004.
- *Weierstrass points and the groups they generate*, Université Texas A&M, 19 novembre 2004.
- *Constructing CM invariants of genus 2 curves*, Banff, 13–18 novembre 2004.
- *The AGM- $X_0(N)$ algorithm : Heegner point lifting with applications*, Schloss Dagstuhl, Algorithms and Number Theory, 16–21 mai 2004.
- *The AGM- $X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting*, Asiacrypt 2003 (Taipei), 1 décembre 2003.
- *The AGM- $X_0(N)$ point counting algorithm*, Université des sciences et technologies de Hong Kong, 28 novembre 2003.
- *Elliptic curve point counting using $X_0(N)$* , Explicit methods in number theory, Oberwolfach, 20–26 juillet 2003.
- *Effective Brauer group computations over global fields*, XXIIIièmes Journées Arithmétiques, Graz, 6–12 juillet 2003.
- *Galois module structure and ranks for Weierstrass subgroups*, Workshop on Computa-

- tional Arithmetic Geometry, Université de Sydney, 18–20 juin 2003.
- *p-Adic lifts of Heegner points on $X_0(N)$* , Université de Leiden, 13 janvier 2003.
 - *p-Adic lifts of Heegner points on $X_0(N)$* , Séminaire de Théorie des Nombres, Algorithmique et Cryptographie, Université de Toulouse II, 18 décembre 2002.
 - *Canonical p-adic lifts on $X_0(N)$* , Université de Rome 2, 13 décembre 2002.
 - *p-Adic point counting algorithms for elliptic curves*, Algebraic Geometry Seminar, Université de Sydney, 22 novembre 2002.
 - *CM points on $X_0(N)$ via p-adic lifts*, Elliptic Curves and Higher Dimensional Analogues (ECHIDNA, Workshop in Arithmetic Geometry and Applications), 15–19 juillet 2002.
 - *Applications of class invariants on modular curves*, Computational Algebra Seminar, Université de Sydney, 24 janvier 2002.
 - *Fundamental domains for Shimura curves*, Computational Algebra Seminar, Université de Sydney, 29 novembre 2001.
 - *Computational aspects of Shimura curves*, Explicit methods in number theory, Oberwolfach, 23–27 juillet 2001.
 - *Fundamental domains for Shimura curves*, XXIIIèmes Journées Arithmétiques, Lille, 2–6 juillet 2001.
 - *Shimura curve invariants*, Workshop on Arithmetic Geometry, Mathematical Sciences Research Institute, 11–15 décembre 2000.
 - *On Satoh’s algorithm*, Computer algebra seminar, Université de Nijmegen, 30 novembre 2000.
 - *Endomorphism ring structure of elliptic curves*, Number theory seminar, Université du Texas, 20 novembre 2000.
 - *Endomorphism ring structure of elliptic curves*, Number theory seminar, Mathematical Sciences Research Institute, 8 novembre 2000.
 - *The Magma Language and Vistas*, Mathematical Sciences Research Institute, Computer Education Seminar, 6 octobre 2000.
 - *On exponential sums and group generators for elliptic curves over finite fields*, avec Igor Shparlinski. Algorithmic Number Theory Symposium IV (Leiden), 2–7 juillet 2000.
 - *Component groups of quotients of $J_0(N)$* , avec William Stein (conférencier). Algorithmic Number Theory Symposium IV (Leiden), 2–7 juillet 2000.
 - *Component groups of Shimura curves*, Workshop on Number Theory, Lorentz Center, Leiden, 26–30 juin 2000.
 - *Rational groups of elliptic curves suitable for cryptography*, Number Theory and Cryptography Conference. Université nationale de Singapour, 22–26 novembre 1999.
 - *Quaternion algebras and invariants of Shimura curves*, Algebra seminar, University of Sydney, 1 octobre 1999.
 - *Elliptic Curves, Modular Forms, and Galois Representations Workshop*, Université de Rome 3, 19–23 juillet 1999.
 - *XXIèmes Journées Arithmétiques Università Lateranense*, Vatican City, 12–16 juillet 1999.
 - *An overview of algebraic geometric coding theory*, Colloquium, Université des Philippines, 11 mars 1999.
 - *On representation numbers of certain ternary quadratic forms*, 2nd KIAS Number Theory Conference. Korean Institute for Advanced Studies, 16–18 décembre 1998.
 - *Explicit sequence expansions*, avec S. Ling (conférencier) et C. Xing. International Conference on Sequences and their Applications. Université nationale de Singapour. 14–17

décembre 1998.

- Algorithmic Number Theory Symposium (ANTS III), Reed College, Portland, 21–25 juin 1998.
- *Hecke module structure of quaternions*, Class Field Theory Conference – its Centenary and Prospect, Université Waseda, Tokyo, 3–12 juin 1998.
- Number Theory and Topology, In honor of Barry Mazur’s 60th birthday, Harvard University, Boston, 27–30 mai 1998.
- *Computing the zeta function of diagonal varieties over finite fields*, Algebra seminar, Université de Sydney, 22 mai 1998.
- *Computing modular curves via quaternions*, Fourth CANT Conference : Number Theory and Cryptography, Université de Sydney, 3–5 décembre 1997.
- *Coding theory : algebraic geometry of linear algebra*, Université nationale de Singapour, 16 avril 1997.
- *Sumas de tres cuadrados y otras formas cuadráticas*, Instituto de Matemáticas, UNAM, Morelia, 20 février 1997.
- *On sums of squares*, Number theory seminar, Université de Californie à Berkeley, 12 février 1997.
- Elliptic curves and modular forms, National Academy of Sciences Washington, D.C., 15–17 mars 1996.
- *Computation of the endomorphism ring of elliptic curves over finite fields*, Université de Santa Clara, 3 octobre 1995.
- Computational perspectives on number theory, in honor of A. O. L. Atkin, Université de l’Illinois à Chicago, 14–16 septembre 1995.
- XIXièmes Journées Arithmétiques, Barcelona, Spain, 16–20 juillet 1995.
- Arithmetic and geometry of abelian varieties, conference in honor of Frans Oort, Université d’Utrecht, 5–9 juin 1995.
- *On the category of supersingular elliptic curves : computational aspects*, Computational number theory, Oberwolfach, 28 mai–3 juin 1995.
- *On the category of supersingular elliptic curves*, Algebra seminar, Université de Leiden, 19 mai 1995.
- Séminaire de théorie des nombres des doctorants de Berkeley, Co-organisateur (avec Steven Hillion), Printemps–Automne 1995. Exposés :
 - *The arithmetic of quaternion algebras.*
 - *Calculating the endomorphism ring of an ordinary elliptic curve.*
- Joint mathematics meetings of the AMS & MAA, San Francisco, Californie, 4–7 janvier 1995.
- “Dessins d’Enfants” Workshop : Moduli spaces and aspects of Galois theory, Université de Californie à Berkeley et MSRI, 23–25 avril 1994.
- Arithmetic geometry with an emphasis in Iwasawa theory, Arizona State University, 15–18 mars 1993.