David R. Kohel

Institut de Mathématiques de Marseille	Citizenships:
Université d'Aix-Marseille	American, Australian, French
163, avenue de Luminy, Case 907	
13288 Marseille cedex 9, France	DOB: 27 February 1966

David.Kohel@univ-amu.fr	Tel : +33 4 91 26 95 73
`http://iml.univ-mrs.fr/~kohel`	Mob : +33 6 77 97 52 20

Education

Academic Degrees

- Ph.D, Mathematics, U. C. Berkeley, December 1996.

  Thesis: *Endomorphism rings of elliptic curves over finite fields.*

  Advisor: Hendrik W. Lenstra, Jr.
- B.S., Mathematics, Texas A&M University (Summa Cum Laude), May 1989.
- B.S., Biochemistry, Texas A&M University (Summa Cum Laude), May 1989.

Academic Career

Université d'Aix-Marseille

- Professeur, 1ère classe, Arithmétique et Théorie de l'Information, 2011–present.
- Professeur, 2ère classe, Arithmétique et Théorie de l'Information, 2007–2011

University of Sydney

- Honorary Senior Lecturer, 2007–2013.
- Senior Lecturer, Number Theory Group, 2005–2007.
- Sesqui Lecturer in Cryptography,[1] Computational Algebra Group, 2002–2005.
- Senior Research Associate, Computational Algebra Group, 2001–2002.

Mathematical Sciences Research Institute, Berkeley

- Postdoctoral Fellow, semester on Algorithmic Number Theory, Autumn 2000.

University of Sydney

- Senior Research Associate, Computational Algebra Group, 1999–2000.

National University of Singapore

- Postdoctoral Fellow, 1997–1999.

[1] The University of Sydney created fifteen Sesqui Lecturer positions in targeted areas across the university, to commemorate the sesquicentennial of the university, founded in 1850.

International Research Invitations

- Université Henri Poincaré, Nancy, (by G. Hanrot), May–Juin 2007.
- Université de Toulouse le Mirail, (by J.-M. Couveignes), November-December 2005.
- Institut de Technologie de Tokyo, (by T. Satoh), 11–21 November 2005.
- University of Californie San Diego, (by W. Stein), September 2005.
- Università di Roma Tor Vergata, (by R. Schoof), Novembre–December 2002.
- École Polytechnique, (by F. Morain), July 2001, December 2001.
- Reed College, (by R. Crandall), June 1998.
- University of Sydney, (by J. Cannon), December 1997, May 1998.

Administrative Roles

- *Conseil du laboratoire, I2M*, 2013-present. Following the merger of three campuses of the Université d'Aix-Marseille in 2012 (split in 1970), the associated CNRS mathematics research institutes the *Institute de Mathématiques de Luminy (IML)* and the *Laboratoire d'Analyse, Topologie et Probabilité (LATP)* joined in 2013 to form the *Institute de Mathématiques de Marseille (I2M)* (see `https://www.i2m.univ-amu.fr`), which currently is composed of 295 researchers (including post-graduates and postdocs), of whom 158 are permanent, plus an additional 18 administrative staff. The majority of staff are distributed between two sites, at Château-Gombert (north Marseille) and Luminy (south Marseille).

  The *conseil du laboratoire* (management committee) includes ten elected academics, five at the professor level and five at the lecturer level. Following elections in 2013, I serve as one of the five elected professors representing the institute.

- Director of the group *Arithmétique et Théorie de l'Information (ATI)*, 2012–2015. The research of the group ATI focuses on *arithmétique* — interpreted broadly as number theory, spanning analytic to algebraic number theory and arithmetic geometry — and its applications to information theory, particularly coding theory and cryptography. There are currently nine permanent members, plus two emeritus, four post-graduates and two postdocs.

- Director of Masters, *Mathématiques Discrètes et Fondements d'Informatique*
  `http://iml.univ-mrs.fr/MDFI/`

  This masters program is devoted to discrete mathematics and its application in theoretical computer science. Since the merger of three campuses of Aix-Marseille, and of the two principal mathematics departments, after the first year masters program in Mathematics and its applications, students split into one of two specialities for the second year. This program, based at the Luminy campus, is focused on "discrete" mathematics in a broad sense, with particular strengths in logic, number theory and its applications to coding theory and cryptography, and discrete dynamical systems and combinatorics.

Conferences and Seminars

The Institut de Mathématiques de Marseille, in particular the centre in Luminy (the ex-Institut de Mathématiques de Luminy), has traditional close ties with the *Centre International de Recherche en Mathématiques* (CIRM), in Luminy.

- *Arithmetic, Geometry, Cryptography and Coding Theory (AGCT)*, co-organized with Alain Couvreur and Alp Bassa, at the CIRM in May 2015. This was the 15th in this series of international workshops in Luminy.

- Co-organizer of thematic semester in *Arithmétique* and host to the Chair Morlet Igor Shparlinski at the CIRM in Luminy.

  `http://www.chairejeanmorlet.com/`

  Specific details of this semester can be found here:

  `http://shparlinskikohel.weebly.com/`

  This semester was launched with five weeks of workshops beginning in February : *Unlikely intersections*, *Prime numbers: new perspectives*, *Frobenius distributions on curves* (doctoral school followed by a research workshop), *On the conjectures of Lang and Vojta* (doctoral school), involving coordination of four different teams of organizers. The proceedings of *Frobenius distributions* are tentatively approved to appear in the *AMS Contemporary Mathematics*, edited with Shparlinski. In addition we organized an additional smaller workshop (20 persons) and three research in pairs events. The annual *Journée de la Société de Mathématiques de France* at the *Institut Henri Poincaré* in Paris centered around the two Morlet Chairs invited to Marseille in 2013–2014. As host of the Morlet Chair Shparlinski, I presented the joint expository paper *Théorie des nombres et cryptographie* at this annual meeting in June 2014. During the course of this semester, I benefited from a *délégation* to the CNRS, in which my teaching duties as professor were replaced with a research-only position for the six month visit of Shparlinski.

- Scientific committee for *YACC 2014* and *YACC 2012*, a more informal *Yet Another Conference on Cryptography*, organized at the IGESA center on Porquerolles Island.

- Scientific committee for *Geocrypt 2013 (Tahiti)*, *Geocrypt 2011 (Corsica)*, and *Geocrypt 2009 (Pointe-à-Pitre)*. These series of workshops, focusing on algebraic geometry and cryptography have attracted high profile invited speakers in a smaller forum. The 2009 workshop received funding from Microsoft Research and the 2011 edition served as closing workshop for a large project CHIC from the French *Agence National de Recherche*.

- *Curves, Coding Theory and Cryptography*, European Science Foundation Exploratory Workshop, co-organized with G. Lachaud and C. Ritzenthaler, 15–16 juin 2009.

- *Arithmetic, Geometry, Cryptography and Coding Theory (AGCT)*, 2009, co-organized with Serge Vladuts. This was the 12th in a series of biennial international workshops at CIRM attracting 60–80 researchers in all aspects of number theory, arithmetic geometry and its applications to cryptography and coding theory. The joint proceedings of AGCT 2009 and Geocrypt 2009 were published in the *AMS Contemporary Mathematics* series, co-edited with Robert Rolland.

Recent Invited Lectures

- Sage Days 61 (Quaternion Orders and Brandt Modules), Copenhagen, Denmark, 25–29 August 2014.
- *Journée Annuelle de la Société de Mathématiques de France*, Paris, 20 June 2014.
- Discrete Logarithm Problem, Monte Verità, Ascona, Switzerland, 5–9 May 2014.
- Number Theory, Geometry and Cryptography, Warwick, UK, 1–5 July, 2013.
- International Workshop on Coding and Cryptography, Qingdao, China, 30 May to 3 June, 2011.
- Elliptic Curves and Computation, Seattle, USA, 18–22 October, 2010.

  The annual conference on Elliptic Curve Cryptography (`http://www.eccworkshop.org/`) was renamed Elliptic Curves and Computation to mark 25 years since the introduction of elliptic curves in computation, including René Schoof's elliptic curve point counting algorithm, Neal Koblitz and Victor Miller's proposals to use elliptic curve for cryptography, and Hendrik Lenstra's elliptic curve integer factoring method, among others. See `2010.eccworkshop.org` for more details. I was invited to present results of my thesis work, which has seen a resurge of interest in recent years.
- Final GTEM conference, Galois Theory and Explicit Methods, Barcelona, Spain, 6–10 September 2010.
- Workshop on Computational Number Theory and Arithmetic Geometry, Leuven, Belgium, 17–21 May 2010.
- Workshop on Counting Points: Theory, Algorithms and Practice, *Centre de Recherches Mathematiques*, Montreal, Canada, April 19–23, 2010 (flight cancelled due to the Eyjafjallajökull eruption).
- Sage Days 20 and *Journée Sage dans l'enseignement*, opening talk and expository presentation to high school teachers, CIRM, Luminy, 22–26 February 2010.
- Sage Days 16 (Computational Number Theory), Barcelona, Spain, 22-27 June 2009.
- Algebraic Geometry and Cryptography, satellite workshop of the joint meeting of the Belgian Mathematical Society and London Mathematical Society, Leuven, Belgium, 5 December 2009.
- Computational number theory, satellite workshop of Foundations of Computational Mathematics, Hong Kong, 24–26 June 2008.
- Symposium on Algebraic Geometry and its Applications (SAGA), Papeete, Tahiti, 7–11 May 2007

Research Grant Funding

I have benefited from continuous grant funding of my research activities since my first ARC Discovery grant in 2003. I detail the main grants and aid-granting agencies below.

Agence Nationale de Recherche[2]

Parameter spaces for Efficient Arithmetic and Curve security Evaluation (PEACE), with the Université de Rennes (D. Lubicz) and the Centre de recherche INRIA Bordeaux Sud-Ouest (J.-M. Couveignes), 2012–2015 (total funding of €139 000 over four years for the three centers). The PEACE project aims to better understand and analyse the security of curve-based cryptosystems, focusing on effective analysis of curves and Jacobians by means of the moduli spaces which classify them.

Courbes Hyperelliptiques, Isogénies et Comptage (CHIC), with the Université de Rennes (D. Lubicz) and INRIA Lorraine, Nancy (E. Thomé), 2009–2012 (total funding of €380 000 over four years for the three centers). The main objective of the CHIC project was to fill the gap in terms of security and performance between cryptography based on elliptic curves and that based on curves of small genus (greater than 1).

Égide (French) / Procope (German) cooperation

Explicit Methods and Algorithms in Number Theory, 2009–2010, with F. Hess, a project for exchange of researchers between our respective institutions, the Institut de Mathématiques de Luminy and Technische Universität Berlin (€6 600 from Égide for IML).

European Science Foundation

Curves, Coding Theory and Cryptography, with G. Lachaud and C. Ritzenthaler, Exploratory Workshop, 15–16 juin 2009 (€15 000 grant).

Australian Research Council

Mathematics of Elliptic Curve Cryptography, with C. Doche et I. Shparlinski (CI), 2008–2011 (total funding AU$230 000 over three years). The program of research for this project concerned the effective methods for the utilisation of elliptic curves in cryptography.

p-Adic Methods in Arithmetic Geometry, David Kohel, Chief Investigator, 2004-2006 (total funding AU$210 000 over three years). The program of research to be undertaken in this project concerned the effective determination of the orders of certain groups, the Jacobian of an algebraic curve, which can be used for cryptography.

[2]The Agence Nationale de Recherche is the French equivalent of the Australian Research Council or US National Science Foundation.

Publications

Edited Books

- *Arithmetic, Geometry, Cryptography and Coding Theory 2015*, A. Bassa, A. Couvreur, et D. Kohel, eds., *Contemporary Mathematics*, American Mathematical Society, preliminary approval 2015.
- *Frobenius Distributions: Sato-Tate and Lang-Trotter conjectures*, D. Kohel et I. Shparlinski, eds., *Contemporary Mathematics*, **663**, American Mathematical Society, 2016.
- *Arithmetic, Geometry, Cryptography and Coding Theory 2009*, D. Kohel et R. Rolland, eds., *Contemporary Mathematics*, **521**, American Mathematical Society, 2010.
- *Algorithmic number theory (Sydney, 2002)*, C. Fieker et D. Kohel, eds., *Lecture Notes in Comput. Sci.,* **2369**, Springer, Berlin, 2002.

Expository publication

- Théorie des nombres et cryptographie, with Igor Shparlinski, *Journée Annuelle de la SMF (Arithmétique et dynamique)*, **27**, Societé de Mathématiques de France, 2014.

Extended abstract

- *Sato-Tate and notions of generality* (extended abstract), *Explicit Methods in Number Theory*, Oberwolfach report, 2011. `https://www.mfo.de/document/1129/OWR_2011_35.pdf`.

Refereed publications

- *Twisted Hessian curves*, avec D. J. Bernstein, T. Lange, C. Chuengsatiansup, *Progress in Cryptology - Latincrypt 2015 (Guadalajara) Lecture Notes in Comput. Sci.*, **9230**, 269–294, 2015.
- *The geometry of efficient arithmetic on elliptic curves*, *Arithmetic, Geometry, Cryptography and Coding Theory*, AMS Contemporary Mathematics, **637**, 95–110, 2015.
- *On the quaternion l-isogeny path problem*, avec K. Lauter, C. Petit, J.-P. Tignol, LMS J. Computation and Mathematics, **17**, 418–432, 2014.
- Efficient arithmetic on elliptic curves in characteristic 2, *Progress in Cryptology — Indocrypt 2012* (Kolkata), *Lecture Notes in Computer Science*, **7668**, 378–398, 2012.
- Complete addition laws on abelian varieties, with C. Arene and C. Ritzenthaler, *LMS Journal of Computational Mathematics*, **15**, 308–316, 2012.
- Point counting on genus 2 curves with real multiplication, with P. Gaudry and B. Smith, *Advances in Cryptology — Asiacrypt 2011* (Seoul), *Lecture Notes in Computer Science*, **7073**, 504–519, 2011. **[Best paper award]**
- Addition law structure of elliptic curves, *Journal of Number Theory*, **131**, Issue 5 (special volume: Elliptic Curve Cryptography), 894–919, 2011.
- Arithmetic of split Kummer surfaces: Montgomery endomorphism of Edwards products, *International Workshop on Coding and Cryptography 2011 (Qingdao)*, *Lecture Notes in Computer Science*, **6639**, 238–245, 2011.
- Double-base number system for multi-scalar multiplications, with C. Doche and F. Sica, *Advances in Cryptology — Eurocrypt 2009* (Cologne), *Lecture Notes in Computer Science*, **5479**, 502–519, 2009.
- Complex multiplication and canonical lifts, *Algebraic geometry and its applications*, *Number Theory and its Applications*, **5**, 67–83, 2008.
- Higher dimensional 3-adic CM construction, with R. Carls and D. Lubicz, *Journal of Algebra*, **319**, no. 3, 971–1006, 2008.

- The Weierstrass subgroup of a curve has maximal rank, with M. Girard and C. Ritzenthaler, *Bulletin of the London Mathematical Society*, **38**, Issue 06, 925–931, 2006.
- The 2-adic CM method for genus 2 curves with application to cryptography, with P. Gaudry, T. Houtmann, C. Ritzenthaler, and A. Weng, *Advances in Cryptology — Asiacrypt 2006* (Shanghai), *Lecture Notes in Computer Science*, **4284**, 114–129, 2006.
- Classification of genus 3 curves in special strata of the moduli space, with M. Girard, *Algorithmic Number Theory Symposium* (Berlin, 2006), *Lecture Notes in Computer Science*, **4076**, 346–360, 2006.
- Efficiently computable endomorphisms for hyperelliptic curves, with B. Smith, *Algorithmic Number Theory Symposium* (Berlin, 2006), *Lecture Notes in Computer Science*, **4076**, 495–509, 2006.
- Efficient scalar multiplication by isogeny decompositions, with C. Doche and T. Icart, *Public Key Cryptography 2006* (New York), *Lecture Notes in Computer Science*, **3958**, 191–206, 2006.
- The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting, in *Advances in Cryptology – Asiacrypt 2003* (Taipei), 124–136, *Lecture Notes in Computer Science*, **2894**, Springer, Berlin, 2003.
- Fundamental domains for Shimura curves, with H. Verrill, *Journal de Théorie de Nombres Bordeaux*, **15**, no. 1, 205–222, 2003.
- Hecke module structure of quaternions, *Class Field Theory—Its Centenary and Prospect (Tokyo, 1998)*, 177–195, *Advanced Studies in Pure Math.*, **30**, 2001.
- Rational groups of elliptic curves suitable for cryptography, *Cryptography and Computational Number Theory (Singapore, 1999)*, 69–80, *Progress in Computer Science and Applied Logic*, **20**, Birkhäuser, 2001.
- Counting the number of points on affine diagonal curves, with C. Ding and S. Ling, *Cryptography and Computational Number Theory (Singapore, 1999)*, 15–24, *Progress in Computer Science and Applied Logic*, **20**, Birkhäuser, 2001.
- On exponential sums and group generators for elliptic curves over finite fields, with I. Shparlinski, *Algorithmic number theory (Leiden, 2000)*, 395–404, *Lecture Notes in Computer Science* **1838**, Springer, Berlin, 2000.
- Component groups of quotients of $J_0(N)$, with W. Stein, *Algorithmic number theory (Leiden, 2000)*, 405–412, *Lecture Notes in Computer Science* **1838**, Springer, 2000.
- Split group codes, with S. Ling and C. Ding, *IEEE Transactions on Information Theory* **46**, no. 2, 280–284, 2000.
- Elementary 2-group character codes, with S. Ling and C. Ding, *IEEE Transactions on Information Theory* **46**, no. 1, 485–496, 2000.
- Secret-sharing with a class of ternary codes, with S. Ling and C. Ding, *Theoretical Computer Science* **246**, no. 1–2, 285–298, 2000.
- Explicit sequence expansions, with S. Ling and C. Xing, *Sequences and their applications (Singapore 1998)*, 308–317, C. Ding, T. Helleseth, and H. Niederreiter, eds., *Discrete Mathematics and Theoretical Computer Science* Springer-Verlag, 1999.

Thesis

- *Endomorphism rings of elliptic curves over finite fields.* Ph.D. Thesis, University of California, Berkeley, 1996. (*One of my most cited works, yet to be published elsewhere.*)

Computational Algebra Development

Beyond traditional mathematical research publications, I am interested in the representation of mathematical objects in a computer, and the algorithms (both theoretical and in practice) which operate on them.

Magma. From 1999-2002 I contributed to computational algebra design, code, and documentation in the Magma computational algebra system (managed at the U. of Sydney by John Cannon). This included a computational model for schemes (with G. Brown); algorithms for curves of low genus, particularly conics, elliptic and hyperelliptic curves; isogeny structures for elliptic curves, modular curves and parametrized isogenies; SEA and p-adic point counting algorithms; binary quadratic forms and class groups of quadratic orders; spinor genera and genera of integral lattices; quaternion algebras and associated Brandt modules; modules of supersingular points (with W. Stein); congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$ and quaternion unit groups, their actions on uppper half complex plane, and invariants of Shimura curves (with H. Verrill); Witt rings.

Sage. Beginning in 2005, I was involved with William Stein in the initial phases of development of a new computer algebra system, Sage. This system has matured considerably since to be an extremely useful tool for teaching and research, and has attracted developers (research mathematicians and computer scientists) from around the world.

ECHIDNA is a repository of open source Magma code and associated databases which I manage, conceived for research in number theory and arithmetic geometry. This code includes contributions from numerous authors and collaborators, *cf.*

`http://echidna.maths.usyd.edu.au/kohel/alg/index.html`
`http://echidna.maths.usyd.edu.au/kohel/dbs/index.html`

Research Supervision

I attach a great importance to the supervision of students, and have been fortunate to work with a number of talented young researchers. After moving to Marseille in 2007 as professor, I continued supervision of my students David Gruenewald, Steven Enright-Ward, Ley Wilson, and Hamish Ivey-Law until successful completion. Ley visited France on two occasions during this period and Hamish, who took up residence in Marseille, completed a double diploma between Sydney and Aix-Marseille in 2012. As of December 2015, four new students will have completed a thesis with me in Aix-Marseille.

Ph.D. Students

- Ben Smith (2002–2005), *Explicit Endomorphisms and Correspondences*, University of Sydney, 2006. After a postdoc at Royal Holloway, London, Ben has held a permanent position as *Chargé de recherche* with INRIA, at the *École Polytechnique* in Paris since 2007.
- David Gruenewald (2004–2008), *Explicit Algorithms for Humbert Surfaces*, University of Sydney, 2009. After an internship at Microsoft Research, postdocs at Aix-Marseille, University of Nijmegen, and Université de Caen Basse-Normandie, he is currently between postdocs.

- Stephen Enright-Ward (2005–2008), *CM Proofs for Elliptic Curves over Number Fields* (masters thesis), University of Sydney, 2009. Enrolled for doctoral studies, for personal reasons Stephen preferred to seek out doctoral studies in Germany (rather than completing a PhD thesis in Australia or France). Consequently, his masters thesis represents a significantly more substantial effort than typical for a masters project. He completed doctoral studies in number theory in Freiburg.
- Ley Wilson (2006–2009), $\mathbb{Q}$-*Curves with Complex Multiplication*, University of Sydney, 2010. After her thesis, Ley decided not to continue an international academic career.
- Christophe Arene (2008–2011), *Géométrie et arithmétique explicites des variétés abéliennes et applications à la cryptographie*, Université d'Aix-Marseille (co-supervised with Christophe Ritzenthaler), 2011. Christophe is a permanent high school teacher, having passed the competetive certification exam during the course of his doctoral studies.
- Hamish Ivey-Law (2007–2012), *Algorithmic Aspects of Hyperelliptic Curves and their Jacobians*, Université d'Aix-Marseille and University of Sydney (co-supervised with Claus Fieker), 2012. Hamish is currently a postdoc at the Université de Bordeaux.
- Virgile Ducet (2009–2013), *Construction of algebraic curves with many rational points over finite fields*, Université d'Aix-Marseille, 2013. Virgile completed a first postdoc in Turkey, and is currently a postdoc at the École Polythechnique in Paris.
- Florent Ulpat Rovetta (2011–2015) *Étude arithmétique et algorithmique de courbes de petit genre*, (co-supervised with Christophe Ritzenthaler), Université d'Aix-Marseille, 2015.
- Yih-Dar Shieh (2009–2015), *Arithmetic aspects of point counting and Frobenius distributions*, (co-supervised with Gilles Lachaud), Université d'Aix-Marseille, 2015.
- Thomas Houtman (2014–present), Université de Caen Basse-Normandie (co-supervised with John Boxall).

Masters Students

- Virgile Ducet, *The arithmetic of CM elliptic curves*, École Normale Supériere, Lyon, 2009.
- Yih-Dar Shieh, *Algebraic curves over finite fields*, Univerité Paris-Sud (Orsay), 2009.
- Thomas Icart, *Cryptologie: multiplication scalaire sur les courbes elliptiques*, École Polytechnique, 2005.

  This project resulted in a publication *Efficient scalar multiplication by isogeny decompositions*, with C. Doche and T. Icart, in *Public Key Cryptography 2006 (New York)*.
- Alex Unger, *Courbes elliptiques et variétés abéliennes*, Leipzig, 2005.

Honours Students

The honours year (fourth year undergraduate) is analogous to a masters program in the European context, culminates in a supervised research and honours thesis.

- Graeme Pope, *Efficient arithmetic on elliptic and hyperelliptic curves*, 2006.
- Gareth White, *Heights on elliptic curves*, 2006.
- Zhuo Jia Dia, *Algebraic geometric coding theory*, 2006.
- Hamish Ivey-Law, *Rational points on higher genus curves*, (with M. Girard), 2006.
- David Gruenewald, *An introduction to modular forms*, 2003.
- Gordon Childs, *Counting points on hyperelliptic curves over finite fields*, 2001.
- Quy Tuan Nguyen, *Binary quadratic forms*, 2000.

Thesis Committees

- Ph.D. Thesis Committee (referee), Christophe Tran, *Formules d'addition sur les jacobiennes de courbes hyperelliptiques : applications à la cryptographie*, 1 December 2014.
- Ph.D. Thesis referee, Peng Tian, Computations on Fourier coefficients of modular forms, Università di Roma Tor Vergata, October 2013
- Ph.D. Thesis Committee (referee), Kisoon Yoon, *Construction de courbes elliptiques et de surfaces abéliennes adaptées à la cryptographie à couplage*, Université de Caen, Basse-Normandie, 20 September 2013
- Ph.D. Thesis Committee (referee), Jean-Gabriel Kammerer, *Analyse de nouvelles primitives cryptographiques pour les schémas Diffie-Hellman*, Université de Rennes I, 23 May, 2013.
- HDR Thesis Committee (referee), Emmanuel Hallouin, *Courbes très spéciales mais en aucun cas génériques*, 12 November 2013.
- Ph.D. Thesis Committee (referee), Aurélien Bajolet, *Aspects numériques de l'analyse diophantienne*, Université Bordeaux I, 7 December 2012.
- Ph.D. Thesis Committee (referee), Gaëtan Bisson, *Endomorphism Rings in Cryptography*, Technische Universiteit Eindhoven, 14 July 2011.
- Ph.D. Thesis Committee (referee), Marco Streng, *Complex Multiplication of Abelian Surfaces*, Universiteit Leiden, 1 June 2010.
- Ph.D. Thesis Committee (referee), Sorina Ionica, *Algorithmique des couplages et cryptographie*, Université de Versailles, Saint Quentin-en-Yvelines, 14 May 2010.
- Ph.D. Thesis Committee, Marie Virat, *Courbes elliptiques sur un anneau et applications cryptographiques*, Université de Sciences de Nice Sophia-Antipolis, 17 April 2009.
- Ph.D. Thesis Committee (referee), Stephen Meagher, *Twists of genus 3 curves and their Jacobians*, University of Groningen, 8 April 2008.

Refereeing and Consultations

I have served as referee for numerous journals and conferences spanning pure to computational or applied mathematics (from *Crelle*, *Compositio*, and *J. Algebra* to *Mathematics of Computation* and *Designs, Codes and Cryptography*).

I have been expert referee for grant agencies of various countries, the Australia Research Council, since 2003; Royal Grant Council, Hong Kong, in 2004; the French Agence National de Recherche, since 2006; the European Science Foundation in 2008–2009; and the Belgian Fonds Wetenschappelijk Onderzoek, in 2014.

On the basis of my application and organization of a European Science Foundation "Exploratory Workshop", I was invited to participate in two meetings of the Physical & Engineering Sciences Standing Committee (PESC):

- European Science Foundation, PESC Round Table, Berlin, 15-16 June 2009.
- European Science Foundation, PESC Core Group, Egelsbach, 1 September 2010.

I have served on the selection committees for lecturer positions in Besançon 2010 and Caen in 2010, and locally in Aix-Marseille in 2014 and 2015 (as president of the committee), as well as for a professor position in Bordeaux in 2011.

International Teaching Experience

University of Copenhagen

Algebraic and Geometric Constructions of Brandt Modules, Sage Days 61 *Quaternion Orders and Brandt Modules*. 25–29 August 2014. In my article *Hecke module structure of quaterions*, I put the emphasis on the module underlying the classical presentation of Brandt matrices (developed by Eichler, following Brandt). In the article, I present the theoretical importance of this Hecke module (as a Galois representation in isomorphisms with a module of modular forms), for which I introduced the term *Brandt module* in its Magma implementation. In two lectures, I presented an overview of algebraic and geometric constructions of Brandt modules. The complete series of lectures and computer tutorials (by five invited lecturers) were validated as a European masters course at the University of Copenhagen. For details, see:

`http://www.math.ku.dk/english/calendar/events/sagedays61/`
`https://sites.google.com/site/sagedays61/`
`http://wiki.sagemath.org/days61`

University of Sydney

Cryptography, at the *ICE-EM/AMSI Summer School*, 15 January – 9 February 2007. This was an intensive course, sponsored by the Australian Mathematical Sciences Institute, destined for masters and doctoral students (24 hours of lectures and 4 hours of computer tutorials). For details, see:

`http://www.maths.usyd.edu.au/u/amsiss07`
`http://echidna.maths.usyd.edu.au/~kohel/tch/Crypto`

Mathematical Sciences Research Institute, Berkeley

Modular forms and quaternion algebras, course at the *Summer Graduate Workshop in Computational Number Theory:*, *Computing with Modular Forms* 31 July – 11 August 2006. This series of lectures focused on computational approaches to modular forms based on the arithmetic of quaternion algebras. For details, see:

`http://modular.math.washington.edu/msri06`
`http://www.msri.org/summer_schools/392`

Finally I mention some expository talks aimed at a broader audience:

Centre International de Recherche en Mathématiques, Luminy

Sage dans l'éducation: cryptographie, at the *Journée Sage dans l'enseignement* organized for an audience consisting mostly of high school teachers, 24 February 2010.

Institut Henri Poincaré, Paris

Théorie des nombres en cryptographie at the annual *Journée annuelle de la Société de Mathématiques de France*, was based on the work of the Morlet Chairs I. Shparlinski (on which my presentation was based) and B. Hasselblatt in Luminy, again to an audience of mathematicians ranging from high school teachers to active researchers, 20 June 2014.

African Institute for the Mathematical Sciences, Capetown

Introduction to Magma and applications, a public talk aimed at a general audience of mathematics students, on the occasion of a conference on arithmetic geometry in nearby Stellenbosch University, South Africa, 2 February 2005.

Teaching History

Here I give a brief summary of the lecture courses for which I was responsible (or co-responsible for certain split courses in Sydney).

University of Sydney

My teaching at the University of Sydney spanned all years (1st to 3rd plus honours), plus exceptional mini-courses for the Talented Student Program.

- *Elliptic Curves and Cryptography*, Talented Student Program, 2003, 2004.
- *Mathematics of Cryptography*, Talented Student Program, 2007.
- *Integral Calculus and Modelling* [MATH 1003], 2003, 2004, 2006, 2007.
- *Linear Mathematics and Vector Calculus* [MATH 2061], 2007.
- *Information and Coding Theory* [MATH 3067], 2006, 2007.
- *Elementary Cryptography and Protocols* [MATH 3024], 2001, 2002, 2003, 2004.
- *Public Key Cryptography* [MATH 3925], 2002, 2003, 2004.
- *Commutative Algebra* [Honours], 2005, 2006.

Université de Toulouse 2

As invited professor, I took responsibility for lectures in a cours on analysis (*Analyse*), in November 2005.

Université d'Aix-Marseille

At the Université d'Aix-Marseille, my lectures have been from third year undergraduate (L3) to first and second year masters (M1 and M2), in addition to various tutorials.

- *Échange des données* and *Pratique de la cryptographie* (L3), covering information theory and cryptography, taught in 2008, 2009, 2010, and 2013.
- *Cryptographie* [Cryptography] (M1 & M2), covering the foundations of cryptography and applications for a professional masters program (centered on Networks and telecommunications) aimed at an engineering background. I have taught this course regularly from the academic year 2007-2008 to the present.
- *Courbes elliptiques* [Elliptic curves] (M2), a research masters course introducing elliptic curves and their applications, taught in 2008, 2009, 2010 and 2013.
- *Algèbre et calcul formel* [Algebra and symbolic computation] (M2), a masters course in the teaching masters *Préparation à l'agrégation*. I have taught this course every academic year since 2011–2012.

I note that the last course in 'Algebra and symbolic computation' is destined for students seeking to pass the competitive examination for the *agrégation*, which permits entry into the corps of teachers for the Ministry of Education, employed from the middle and high school level to the prestigious *classes préparatoires*. The course title refers to one of four options for an oral exam in for which candidates have 3 hours to prepare a 40 minute (pedagogically sound) teaching presentation, integrating computer modelling, examples, and/or graphical illustrations, built around a choice of two randomly selected texts in the area of the option.

In particular, my masters teaching has spanned courses aimed at training students for professional, teaching and research careers.

Course Development

As Sesqui *Lecturer en Cryptography*, I introduced two new courses: *Elementary cryptography and protocoles* [MATH3024] at the ordinary level, and *Public key cryptography* [MATH3925] at the advanced level. These covered the basis of cryptography and cryptanalysis from the classical to the modern age. Notes and tutorial sheets are still available:

`http://echidna.maths.usyd.edu.au/~kohel/tch/USyd/MATH3024`
`http://echidna.maths.usyd.edu.au/~kohel/tch/USyd/MATH3925`

These courses are no longer taught in the present form since a revision of the curriculum in 2005, but the course *Number theory and cryptography* [MATH2068] is largely based on *Public key cryptography*. In addition my cryptography textbook and and AMSI cryptography course developed out of these courses:

`http://echidna.maths.usyd.edu.au/~kohel/tch/USyd/Crypto/crypto.pdf`
`http://echidna.maths.usyd.edu.au/~kohel/tch/USyd/Crypto`

At the Université d'Aix-Marseille, I similarly developed courses, covering aspects of information theory and cryptography (*Échange des données* and *Pratique de la cryptographie*) at the third year undergraduate to various masters level courses (professional and research) in cryptography.