Dr Christophe DOCHE

I Personal details

1. Bio

- Date of birth: 25 June 1971.
- Citizenship: French.
- Visa: Australian Permanent Resident (since 2003).

2. Contact

- Address: Building E6A, Office 360
  Computing Department, Macquarie University
  North Ryde, NSW 2109, Australia.
- Tel: (+61) 2 9850 9576.
- Fax: (+61) 2 9850 9551.
- Email: `christophe.doche@mq.edu.au`
- Home page: `http://www.comp.mq.edu.au/~doche`

II Education

1. Theoretical Computer Science/Mathematics

- **PhD in Algorithmic Number Theory, University of Bordeaux (2000).**
  Title: *Mahler measure and real roots of certain family of polynomials.*
  Advisors: L. Habsieger and M. Langevin.
  cf. `http://www.comp.mq.edu.au/~doche/these.pdf`
- Master of Research in Mathematics, University of Bordeaux (1996).
  Specialisation: Number Theory.
- Knowldege of mathematical softwares: `GP-PARI`, `Maple`, `Magma`, and `Mathematica`.
- Programming in `Java` and `C/C++`.
- Expertise in TeX and LaTeX.

2. General

- Bachelor Degree in Science, University of Bordeaux (1994).
  Specialisations: Mathematics, Physics, and Computer Science.
- Associate Degree in Law, University of Bordeaux (1992).

III Employment

1. Academia

- **In Computing at Macquarie University (since 2003)**:
  - **Head of Department (since 2014)**.
  - Senior Lecturer (since 2007).
  - Lecturer (2003–2007).
- Postdoctoral fellow at the University of Bordeaux (2000–2001).
- PhD fellow at the University of Bordeaux (1998–2000).

2. Industry

- **Cryptographer for the AREHCC project (2001–2003)**.
  AREHCC stands for Advanced Research in Elliptic and Hyperelliptic Curve Cryptography. This consortium, partially funded by the European Community, gathered a network of Belgian, French, and German Universities as well as industrial partners such as Philips and Oberthur. Its goal was to assess the suitability of elliptic and hyperelliptic curves for cryptographic applications on smart cards.

IV Teaching

1. **Recent activity (convening in bold)**
   - ○ COMP125 – Fundamentals of Computer Science in **2011**, 2012, **2013**, and **2014**.
   - ○ COMP333 – Algorithm Theory and Design 2006, **2008**, **2009**, and 2015.
   - ○ COMP343 – Cryptography and Information Security in 2010, **2011**, 2012, and **2014**.
   - ○ COMP777 – Computing Methods for Research (MRes unit) in **2013**.

2. **Past activity**
   - ○ At Macquarie:
     - COMP115 – Introduction to Computer Science.
     - COMP238 – Numerical Computing.
     - COMP445 – Advanced Information Security (Honours unit).
   - ○ Undergraduate lectures in Mathematics at the University of Bordeaux (1998–2001).
     Topics: logic, basic algebra, linear algebra, group theory, probability, and statistics.

V Curriculum Development

1. **Programs**
   - • Instrumental in the creation of the *Cyber Security* Major to be offered in 2017 and the *Data Science* Major developed with Statistics and offered since 2016.
   - ○ Involved in the creation of the *Web Design and Development* Major developed with Media and offered since 2014 as well as the *Business Information Systems* Major co-owned by FBE and Science and offered since 2012.
   - • Led the transition to the new Curriculum in Computing implemented in 2010.

2. **Units**
   - ○ Involved in the creation of ISYS200 – IT & the Future of Society, offered since 2014.
   - ○ Instrumental in the creation of MRes unit COMP777 – Computing Methods for Research offered since 2013.

VI Reasearch Funding

1. **External**
   - ○ CNRS Project CANTaL (Cryptography Algorithmic Number Theory and Lattices), with Chief Investigators I. Shparlinski, and R. Steinfeld.
     Amount awarded: 30,000 € (approx. $45,000) over three years (2012–2014).
   - • ARC Discovery DP110100628, *Lattices as a Constructive and Destructive Cryptographic Tool*, with Chief Investigator I. Shparlinski, and Partner Investigators R. Steinfeld and D. Stehlé.
     Amount awarded: $330,000 over three years (2011–2013).
   - • ARC Discovery DP0881473, *Mathematics of Elliptic Curve Cryptography*, with Chief Investigator I. Shparlinski, and Partner Investigator D. Kohel.
     Amount awarded: $230,000 over three years (2008–2010).

2. **Internal**
   - ○ MQRDG with Y. Kong from the Department of Engineering.
     Title: *Digital Arithmetic for Elliptic Curve Cryptography.*
     Amount awarded: $44,456 over three years (2010–2012).
   - ○ Emerging Technologies Grant Scheme with S. Cassidy.
     Title: *Evaluating Moodle in the Computing Curriculum.*
     Amount awarded: $39,721 over two years (2008–2009).
     Paved the way to the deployment of iLearn.
   - ○ New Staff Grant.
     Title: *Fast arithmetic for cryptographic purposes through alternative representations.*
     Amount awarded: $19,827 over two years (2006–2007).
   - ○ Start-up grant.
     Title: *Development of algorithms to improve the arithmetic of hyperelliptic curves.*
     Amount awarded: $5,550 over two years (2003–2004).

VII Publications

1. Book

• *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press.
30 chapters, 848 pages, 2005 (ISBN: 978-1584885184). R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren.
Cited more than 950 times in Google Scholar. As Executive Editor, led a team of 15 researchers from Academia and the Industry. Directly authored six chapters representing more than 200 pages.

2. Chapters in Book

○ *Handbook of Finite Fields*, CRC Press.
17 chapters, 1068 pages, 2013 (ISBN: 978-1439873786). G. L. Mullen and D. Panario. More than 60 internationally recognised experts collaborated to this ultimate reference on finite fields. Contributed to the Section *Algorithms – Computational techniques*, 18 pages.

○ *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press.
Author of the chapters:
– *Algebraic Background*, with D. Lubicz, 20 pages.
– *Exponentiation*, 24 pages.
– *Integer Arithmetic*, 30 pages.
– *Finite Field Arithmetic*, 38 pages.
– *Arithmetic of Elliptic Curves*, with T. Lange, 36 pages.
– *Arithmetic of Special Curves*, with T. Lange, 34 pages.

3. Recent Journal Articles

• *New and Improved Methods to Analyze and Compute Double-Scalar Multiplications*, with D. Sutantyo, IEEE Transactions on Computers, 63(1), 230-242, (2014). Journal ranked A*.

○ *Equidistribution modulo 1 and Salem numbers*, with M. Mendès France and J.-J. Ruch, in honour of W. Narkiewicz for his 70th birthday, Funct. Approx. Comment. Math. 39 (2008), part 2, 261–271, (2008).

4. Selected Refereed Conference Proceedings

• *On the Enumeration of Double-Base Chains with Applications to Elliptic Curve Cryptography.* Proceedings of AsiaCrypt 14 Advances in Cryptology — AsiaCrypt 2014, Kaohsiung. Lecture Notes in Computer Science **8873** 297–316 (2014). Springer. Conference ranked A.

• *Double-Base Number System for Multi-Scalar Multiplications*, with D. Kohel and F. Sica, Advances in Cryptography — EuroCrypt 2009, Köln. Lecture Notes in Computer Science **5479** 502–517 (2009). Springer. Conference ranked A*.

○ *A Tree-Base Approach for Computing Double-Base Chains*, with L. Habsieger, Australasian Conference on Information Security and Privacy — ACISP 2008, Wollongong. Lecture Notes in Computer Science **5107** 433–446 (2008). Springer.

○ *Extended Double-Base Number System with applications to Elliptic Curve Cryptography*, with L. Imbert, Progress in Cryptology — IndoCrypt 2006, Kolkata. Lecture Notes in Computer Science **4329** 335–348 (2006). Springer.

• *Extending Scalar Multiplication using Double Bases*, with R. Avanzi, V. Dimitrov, and F. Sica, Advances in Cryptology — AsiaCrypt 2006, Shangai. Lecture Notes in Computer Science **4284** 130–144 (2006). Springer. Conference ranked A.

○ *Efficient Scalar Multiplication by Isogeny Decompositions*, with T. Icart and D. Kohel, Public Key Cryptography — PKC 2006, New-York. Lecture Notes in Computer Science **3958** 191–206 (2006). Springer.

5. Impact

○ Over 30 publications cited more than 1,400 times according to Google Scholar
cf. http://scholar.google.com.au/citations?user=NjSMsnUAAAAJ&hl=en&oi=ao

VIII Softwares

1. C++ Library

○ Arithmetic on elliptic curves defined over prime fields and extension fields of characteristic 2, with S. Duquesne (2002–2003). Open source.

2. GP-PARI Libraries

○ Redundant trinomials for finite fields of characteristic 2 (2004).
cf. http://www.comp.mq.edu.au/~doche/redundant.gp.gz

● Cardinality of an elliptic curve defined over a prime field using the SEA algorithm, with S. Duquesne (2003). This is the first public implementation competing with governmental and commercial versions in terms of efficiency.
Available with the GP-PARI distribution.
cf. http://pari.math.u-bordeaux.fr/packages.html

○ Mahler measure of polynomials in one and two variables (2001).
cf. http://www.comp.mq.edu.au/~doche/mahler.gp

IX HDR Supervision

1. PhD Students

● Principal supervisor of D. Sutantyo. Completed in 2013.

○ Co-supervisor of H. N. Vo. Completed in 2012.

○ Co-supervisor of C. McDonald. Completed in 2010.

2. Master Student

● Supervisor of B. Evans in 2010.
Title of the project: *Randomised Quiz System for Assisted Learning.*

X Service

1. Department and University

● **Head of Department since 2014.**

● **Director of Teaching (2008–2013).**

○ Member of the Individual Cases Committee (2011–2014).

○ Exemption Officer since 2005.

2. Professional Activities

● Assessor for the ARC since 2007.

○ Referee for more than 20 different journals such as IEEE Transactions on Computers, IEEE Transactions on Information Theory, London Mathematical Society, Finite Fields and their Applications, Journal of Mathematical Cryptology, etc.

○ Reviewer for more than 20 conferences, including all the major conferences in Cryptography: EuroCrypt, AsiaCrypt, IndoCrypt, PKC, SAC, and CT-RSA.

○ Program Committee member of 11 conferences, including AsiaCrypt, SAC, ACISP, CT-RSA, AfricaCrypt, and GeoCrypt.