

A/Prof Christophe DOCHE

I Personal details

- Bio**
 - Date of birth: 25 June 1971.
 - Citizenship: French.
 - Visa: Australian Permanent Resident (since 2003).
- Contact**
 - Address: EMC Building, Level 1 – Suite 11
3 Innovation Road, Macquarie University
North Ryde, NSW 2109, Australia.
 - Tel: (+61) 2 9850 9576.
 - Fax: (+61) 2 9850 9551.
 - Email: christophe.doch@mq.edu.au
 - Home page: <http://www.comp.mq.edu.au/~doche>

II Education

- 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.
 - Knowledge of mathematical softwares: GP-PARI, Maple, Magma, and Mathematica.
 - Programming in Java and C/C++.
 - Expertise in $\text{T}_{\text{E}}\text{X}$ and $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$.
- 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

- Academia**
 - **At the Optus Macquarie University Cyber Security Hub:**
 - **Executive Director (since Sept. 2016).**
 - **In the Computing Department of Macquarie University:**
 - Head of Department (Jan. 2014– Jan. 2016)
 - Academic since 2003.
 - At the University of Bordeaux:
 - Postdoctoral fellow (2000–2001)
 - PhD fellow (1998–2000).
- 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 **2013** and **2014**.
- COMP333 – Algorithm Theory and Design in 2015.
- COMP343 – Cryptography and Information Security in **2014**, **2017** and **2018**
- 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 offered from 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 the Faculties of Business and Science and offered since 2012.

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

Research
Funding**1. External**

- ARC Discovery DP180103251, *Privacy-Preserving Online User Matching*, with Chief Investigators X. YI, I. KHALIL and Partner Investigator E. BERTINO.
Amount awarded: \$383,826 over three years (2018–2020).
- 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).
- 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).

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).

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 1050 times in Google Scholar. As Executive Editor, led a team of 15 researchers from Academia and 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. Selected 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, Shanghai. 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

- h-index of 11.
- Over 30 publications cited more than 1,700 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

Research Supervision

1. Postdoctoral Fellow

- Supervisor of Dr M. SHA, Macquarie Research Fellow (2016–2019).

2. 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.

X

Service

1. Department and University

- **Head of Department of Computing (Jan. 2014– Jan. 2016).**
- **Director of Teaching (2008–2013).**
- Member of the Faculty of Science Individual Cases Committee (2011–2014).
- Exemption Officer for the Department (2005–2013).

2. Professional Activities

- Peer Reviewer for the ERA 2015 exercise.
- 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.