Craig Costello

Researcher
Microsoft Research
One Microsoft Way, Redmond, Washington, USA
office: +1 (425) 421-5559
email: craigco@microsoft.com
web: http://www.craigcostello.com.au

Education

- *Queensland University of Technology*, PhD in Mathematics & Cryptology, 2013.
  Advisor: Prof. Colin Boyd.
- *Queensland University of Technology*, BAppSc in Mathematics (Hons - 1st Class), 2007.

Research Interests

Algorithmic number theory and computational algebraic geometry: elliptic curves, hyperelliptic curves, abelian varieties, ideal lattices

Applications of the above in cryptography: elliptic curve cryptography, pairing-based cryptography, lattice-based cryptography, real-world implementations (OpenSSL and TLS), learning with errors, cryptanalysis

Awards and Scholarships

- Gregory Schwartz Enrichment Grant (2011)
- Australian-American Fulbright Scholarship in Technology and Communication (2010)
- Queensland Government Smart State Fellowship Ph.D. Grant (2008)
- Australian Postgraduate Award (APA) (2008)
- Queensland University of Technology Vice-Chancellor Ph.D. Scholarship (2008)
- Queensland University of Technology Faculty of Information Technology Ph.D. Scholarship (2008)
- Dean's Award for Excellence in Mathematics in Undergraduate Degree (2007)
- Queensland University of Technology Dean's Scholars Accelerated Honours Program (2005-2007)
- TJ Ryan Memorial Fellowship for Excellence in Academia, Leadership and Community Service (2005)

Publications

[1] Craig Costello, Huseyin Hisil, Colin Boyd, Juan Manuel Gonzalez Nieto, and Kenneth Koon-Ho Wong. Faster pairings on special Weierstrass curves. In *Pairing-Based Cryptography (Pairing) 2009*, *LNCS*, vol. 5671, pp. 89–101. Springer, 2009.

[2] Craig Costello, Tanja Lange, and Michael Naehrig. Faster pairing computations on curves with high-degree twists. In *Public-Key Cryptography (PKC) 2010*, *LNCS*, vol. 6056, pp. 224-242. Springer, 2010.

[3] Craig Costello, Colin Boyd, Juanma Gonzalez-Nieto, and Kenneth Koon-Ho Wong. Avoiding full extension field arithmetic in pairing computations. In *Progress in Cryptology - AFRICACRYPT 2010*, *LNCS*, vol. 6055, pp. 203-224. Springer, 2010.

[4] Craig Costello, Colin Boyd, Juanma Gonzalez-Nieto, and Kenneth Koon-Ho Wong. Delaying mismatched field multiplications in pairing computations. In *Arithmetic in Finite Fields - WAIFI 2010*, *LNCS*, vol. 6087, pp. 196-214. Springer, 2010.

[5] Craig Costello and Douglas Stebila. Fixed Argument Pairings. In *Progress in Cryptology - LATINCRYPT 2010*, *LNCS*, vol. 6212, pp. 92-108. Springer, 2010.

[6] Craig Costello and Kristin Lauter. Group Law Computations on Jacobians of Hyperelliptic Curves. In *Selected Areas in Cryptography (SAC) 2011*, *LNCS*, vol. 7118, pp. 92-117. Springer, 2011.

[7] Craig Costello, Kristin Lauter, and Michael Naehrig. Attractive subfamilies of BLS Curves for Implementing High-Security Pairings. In *Progress in Cryptology - INDOCRYPT 2011*, *LNCS*, vol. 7017, pp. 320-342. Springer, 2011.

[8] Joppe W. Bos, Craig Costello, Huseyin Hisil and Kristin Lauter. Fast Cryptography in Genus 2. In *Progress in Cryptology - EUROCRYPT 2013*, *LNCS*, vol. 7881, pp. 194-210. Springer, 2013. **Full version in the Journal of Cryptology**.

[9] Joppe W. Bos, Craig Costello, Huseyin Hisil and Kristin Lauter. High-Performance Scalar Multiplication using 8-Dimensional GLV/GLS Decomposition. In *Cryptographic Hardware and Embedded Systems (CHES) 2013*, *LNCS*, vol. 8086, pp. 331-348. Springer, 2013.

[10] Joppe W. Bos, Craig Costello, and Michael Naehrig. Exponentiating in Pairing Groups. In *Selected Areas in Cryptography (SAC) 2013*, *LNCS*, vol. 8282, pp. 438-455. Springer, 2013.

[11] Joppe W. Bos, Craig Costello, and Andrea Miele. Elliptic and Hyperelliptic Curves: a Practical Security Analysis. In *Public Key Cryptography (PKC) 2014*, *LNCS*, vol. 8383, pp. 203-220. Springer, 2014.

[12] Craig Costello, Huseyin Hisil, and Benjamin Smith. Faster Compact Diffie-Hellman: Endomorphisms on the x-line. In *Progress in Cryptology - EUROCRYPT 2014*, *LNCS*, vol. 8441, pp. 183-200. Springer, 2014.

[13] Craig Costello, Alyson Deines-Schartz, Kristin Lauter, and Tonghai Yang. Constructing Abelian Surfaces for Cryptography via Rosenhain Invariants. In London Mathematical Society (LMS) Journal of Computational Mathematics, 17 (Special Issue on Algorithmic Number Theory).

[14] Huseyin Hisil and Craig Costello. Jacobian Coordinates on Genus 2 Curves. In *Progress in Cryptology - ASIACRYPT 2014*, *LNCS*, vol. 8873, pp. 338-357. Springer, 2014. **Full version in the Journal of Cryptology**.

[15] Joppe W. Bos, Craig Costello, Patrick Longa, and Michael Naehrig. Selecting Elliptic Curves for Cryptography: An Efficiency and Security Analysis. In The Journal of Cryptographic Engineering, May, 2015.

[16] Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In *Proc. IEEE*

Symposium on Security and Privacy (S&P) 2015. IEEE, 2015, to appear.

[17] Craig Costello, Cedric Fournet, Jon Howell, Markulf Kohlweiss, Benjamin Kreuter, Michael Naehrig, Bryan Parno, and Samee Zahur. Gepetto: Versatile Verifiable Computation. In *Proc. IEEE Symposium on Security and Privacy (S&P) 2015*. IEEE, 2015, to appear.

[18] Paulo S. L. M. Barreto, Craig Costello, Rafael Misoczki, Michael Naehrig, Geovandro C. C. F. Pereira, and Gustavo Zanon. Subgroup security in pairing-based cryptography. In *Progress in Cryptology - LATINCRYPT 2015*, *LNCS*, vol. 9230, pp. 245-265. Springer, 2015.

[19] Craig Costello and Patrick Longa. Four$Q$: four-dimensional decompositions on a Q-curve over the Mersenne prime. In *Progress in Cryptology - ASIACRYPT 2015*, *LNCS*, vol. 9452, pp. 214–235. Springer, 2015.

[20] Ping Ngai Chung, Craig Costello, and Benjamin Smith. Fast, uniform, and compact scalar multiplication for elliptic curves and genus 2 Jacobians with applications to signature schemes. To appear in *Selected Areas in Cryptography (SAC) 2016*, *LNCS*. Springer, 2016.

[21] Joost Renes, Craig Costello, and Lejla Batina. Complete addition formulas for prime order elliptic curves. In *Progress in Cryptology - EUROCRYPT 2016*, *LNCS*, vol. 9665, pp. 403–428. Springer, 2016.

[22] Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. To appear in *Progress in Cryptology - CRYPTO 2016*, *LNCS*. Springer, 2016.

[23] Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE. In *Proc.2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016.

[24] Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, and David Urbanik. Efficient compression of SIDH public keys. In *Progress in Cryptology - EUROCRYPT 2017*, *LNCS*, vol. 10210, pp. 679–706. Springer, 2017.

[25] Craig Costello and Benjamin Smith. Montgomery curves and their arithmetic: the case of large characteristic fields. In *Journal of Cryptographic Engineering*. Springer, 2017.

[26] Craig Costello and Huseyin Hisil. A simple and compact algorithm for SIDH with arbitrary degree isogenies. In *Progress in Cryptology - ASIACRYPT 2017*, *LNCS*, vol. 10625, pp. 303–329. Springer, 2017.

Book Chapters

[27] Joppe W. Bos, Craig Costello, and Michael Naehrig. Exponentiating in Pairing Groups. To appear in *Guide to Pairing-Based Cryptography*, 2015.

Dissertations

[28] Craig Costello. *Fast Formulas for Computing Cryptographic Pairings*. PhD thesis, Queensland University of Technology, 2012.

Selected Invited/Contributed Talks

- *The Annual Workshop on Elliptic Curve Cryptography (ECC2017)*, Nijmegen, Netherlands, November 2017.
- *International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE 2016)*, Hyderabad, India, December 2016.
- *National Institute of Standards and Technology (NIST) - Workshop on Elliptic Curve Cryptography Standards*, Maryland, June 2015.
- *American Mathematical Society - Special Session on Arithmetic Geometry*, Las Vegas, April 2015.
- *National Institute of Standards and Technology (NIST) - Workshop on Post-Quantum Cryptography*, Maryland, April 2015.
- *Microsoft Research Annual Privacy Workshop*, Washington, October 2014.
- *The Annual Workshop on Elliptic Curve Cryptography (ECC2014)*, Chennai, India, October 2014.
- *American Mathematical Society - Special Session on Algebraic Curves*, San Diego, January 2013.
- *The Annual Workshop on Elliptic Curve Cryptography (ECC2012)*, Queretaro, Mexico, October 2012.

Program Committees

- *Program Committee member:* WAIFI2018, FC2018, PST2016, ACISP2015, PST2015, SAC2013
- *Journal reviewer:* The Journal of Cryptology, The Journal of Cryptographic Engineering, International Journal of Applied Cryptography (IJACT), IEEE Transactions on Information Theory, Designs Codes and Cryptography

Work History

- **Researcher**, *Microsoft Research, Redmond, USA* (2014–)
- **Post-doc**, *Microsoft Research, Redmond, USA* (2012–2014)
- **Post-doc**, *Technische Universiteit Eindhoven, Netherlands* (2012)
- **Research Intern**, *Microsoft Research, Redmond, USA* (2012)
- **Research Intern**, *Microsoft Research, Redmond, USA* (2011)
- **Visiting Scholar**, *University of California, Irvine* (2010–2011)
- **PhD Candidate**, *Queensland University of Technology, Australia* (2008–2012)

Teaching

Interests and capabilities

- Number Theory, Algebraic Geometry, Discrete Mathematics, Mathematics of Public Key Cryptography, Cryptology, Algebraic Curves

Undergraduate

- Lecturer, *Abstract Mathematical Reasoning, Queensland University of Technology*: 2016

– Teacher's assistant, *Introduction to Cryptology, Queensland University of Technology*: 2010

Graduate

– Teacher's assistant, *Advanced Cryptology, Queensland University of Technology*: 2011-2012
– Lecturer (shared), *Advanced Cryptology, Queensland University of Technology*: 2011-2012

Short courses

– Workshop on Curves and Applications: 2013
– Annual Workshop on Elliptic Curve Cryptography: 2012

Advising

– Alyson Deines-Schartz, Univ. of Washington, Internship at Microsoft Research, 2013
– Andrea Miele, EPFL Switzerland, Internship at Microsoft Research, 2013
– Brian Chung, Univ. of Cambridge, UK, Internship at Microsoft Research, 2015
– Eric Crockett, Georgia Tech., Internship at Microsoft Research, 2015
– Joost Renes, Radboud University, Netherlands, Internship at Microsoft Research, 2016 & 2017