Colleen M. Swanson

travellingcryptographer.com • swan@travellingcryptographer.com

Research Interests
Computer security and applied cryptography, privacy-enhancing technologies, security/privacy-related public policy, information-theoretic and public-key cryptography, combinatorial cryptography

Education
PhD in Computer Science, 2013
University of Waterloo, Waterloo, Ontario, Canada
Supervisor: Douglas Stinson
Thesis: *Unconditionally Secure Signature Schemes, User-Private Information Retrieval, and the Generalized Russian Cards Problem*

Master of Mathematics in Combinatorics and Optimization, 2008
University of Waterloo, Waterloo, Ontario, Canada
Supervisor: David Jao
Thesis: *Security in Key Agreement: Two-Party Certificateless Schemes*

Bachelor of Arts in Mathematics, *summa cum laude*, 2006
Mount Holyoke College, South Hadley, Massachusetts
Supervisors: Farshid Hajir, Donal O'Shea
Thesis: *Algebraic Number Fields and Codes*

Employment
Research Fellow, Computer Science — September 2015–August 2016
University of California at Davis, Davis, California

Research Fellow, Computer Science and Engineering, — September 2013–August 2015
University of Michigan, Ann Arbor, Michigan

Publications
C. M. Swanson and D. R. Stinson. Unconditionally secure signature schemes revisited. *Journal of Mathematical Cryptology*, vol. 10 (2016), 35–67.

S. Khattak, T. Elahi, L. Simon, C. M. Swanson, S. J. Murdoch, and I. Goldberg. SoK: Making sense of censorship resistance systems. *Proceedings on Privacy Enhancing Technologies* 2016(4), 37–61.

C. M. Swanson and D. R. Stinson. Extended results on privacy against coalitions of users in user-private information retrieval protocols. *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences*, vol. 7 (2015), 415–437.

C. M. Swanson and D. R. Stinson. Additional constructions to solve the generalized Russian cards problem using combinatorial designs. *The Electronic Journal of Combinatorics*, vol. 21 (2014), paper #P3.29, 31 pp.

D. R. Stinson, C. M. Swanson, and T. van Trung. A new look at an old construction: constructing (simple) 3-designs from resolvable 2-designs. *Discrete Mathematics*, vol. 325 (2014), 23–31.

E. Wustrow, C. M. Swanson, and J. A. Halderman. TapDance: End-to-middle anticensorship without flow blocking. In: *Proc. 23rd USENIX Security Symposium (USENIX '14)*, 2014.

C. Swanson and D. Stinson. Combinatorial solutions providing improved security for the generalized Russian cards problem. *Designs, Codes and Cryptography*, vol. 72 (2014), 345–367.

M. Rushanan, D. Foo Kune, and C. M. Swanson, and A. D. Rubin. SoK: Security and privacy in implantable medical devices and body area networks. In: *Proc. IEEE Symposium on Security and Privacy (Oakland '14)* (2014), 524-539.

C. Swanson and D. Stinson. Extended combinatorial constructions for peer-to-peer user-private information retrieval. *Advances in Mathematics of Communications*, vol. 6 (2012), 479–497.

C. Swanson and D. Stinson. Unconditionally secure signature schemes revisited. In: *Proc. 5th International Conference on Information Theoretic Security (ICITS 2011). LNCS*, vol. 6673 (2011), 100–116.

C. Swanson, R. Urner, and E. Lank. Naïve security in a Wi-Fi world. In: *Proc. IFIP AICT*, *Trust Management IV*, vol. 321 (2010), 32–47.

C. Swanson, C. and D. Jao. A study of two-party certificateless authenticated key agreement protocols. In: *Proc. INDOCRYPT 2009*, *LNCS*, vol. 5922 (2009), 57–71.

K. Henry, C. Swanson, Q. Xie, and K. Daudjee. Efficient hierarchical quorums in unstructured peer-to-peer networks. In: *Proc. CoopIS 2009*, *LNCS*, vol. 5870 (2009), 183–200.

Conference Talks
Unconditionally secure signature schemes revisited. ICITS 2011. Amsterdam, The Netherlands. (May 2011)

Naïve security in a Wi-Fi world. IFIPTM 2010. Morioka, Japan. (June 2010)

Two-party certificateless authenticated key agreement protocols. INDOCRYPT 2009. Delhi, India. (December 2009)

Efficient hierarchical quorums in unstructured peer-to-peer networks. CoopIS 2009. Vilamoura, Portugal. (November 2009)

Selected Honors and Awards
University of Waterloo: David R. Cheriton Graduate Scholarship (2010–2013); Provost Doctoral Entrance Award for Women (2009–2010); Graduate Scholarship (2008)

Mount Holyoke College:
- Sarah Williston Prize (ranked first in class)
- Mary Lyon Scholar (honors undergraduate thesis)
- Academic excellence: Sarah Williston Senior Prize Scholarship (2006); Sarah Williston Scholar & Prize (2004–2006); Class of 1937 Prize (Mathematics, 2005); Gina Jacobsen Prize (Mathematics, 2004); Mildred L. Sanderson Prize (Mathematics, 2003); Leadership Award (2002)

New York State Higher Education System: Robert C. Byrd Honors Scholarship, 2002–2006

Teaching and Mentoring Experience
Graduate Student Mentoring September 2013–August 2015
Computer Science and Engineering, University of Michigan

Guest Lecturer, undergraduate cryptography course Winter 2014
Computer Science and Engineering, University of Michigan
- "Introduction to elliptic curve cryptography"

Guest Lecturer, undergraduate security course Fall 2014
Computer Science and Engineering, University of Michigan
- "Introduction to public key cryptography"
- "Anonymity and anticensorship systems"
- "Privacy, big data, and de-anonymization"

Instructional/Teaching Assistant September 2007–August 2012
Faculty of Mathematics, University of Waterloo

Professional Affiliations
Phi Beta Kappa, Mount Holyoke College Chapter

Centre for Applied Cryptographic Research (CACR), University of Waterloo
Cryptography, Security and Privacy Research Group (CrySP), University of Waterloo

Interests
French/Russian, cooking, music, sewing, yoga