Thomas Eric Shrimpton

Dept. of Computer and Information
Science and Engineering
University of Florida
Gainesville, Florida 32601 USA

Office: +1 352 294-2092

Email: teshrim@ufl.edu
Web: http://cise.ufl.edu/~teshrim/

Professional Preparation

Virginia Polytechnic Institute and State University	Elec. Eng.	B.S. 1994
University of Maryland, Baltimore County	Elec. Eng.	M.S. 1997
University of California, Davis	Elec. Eng.	Ph.D. 2004

Appointments

Associate Professor, Computer Science, University of Florida	*9/15-present*
Associate Professor, Computer Science, Portland State University	*9/12-9/15*
Assistant Professor, Computer Science, University of Lugano (CH)	*9/07-9/09*
Assistant Professor, Computer Science, Portland State University	*6/04-6/12*

Publications (Related)

1. A. Boldyreva, C. Patton and T. Shrimpton, Thomas "Hedging Public-Key Encryption in the Real World", *Advances in Cryptology – CRYPTO 2017, Lecture Notes in Computer Science*, vol. 10403, pp. 462-494, Springer, 2017

2. C. Namprempre, P. Rogaway and T. Shrimpton, "Reconsidering Generic Composition", *Advances in Cryptology – EUROCRYPT 2014, Lecture Notes in Computer Science*, vol. 8441, pp. 257-274, Springer, 2014

3. P. Rogaway and T. Shrimpton, "A Provable-Security Treatment of the Key-Wrap Problem", *Advances in Cryptology – EUROCRYPT 2006, Lecture Notes in Computer Science*, vol. 4004, pp. 373-390, Springer, 2006

4. A. Chhotaray, A. Nahiyan, T. Shrimpton, D. Forte and M. Tehranipoor, "Standardizing Bad Cryptographic Practice: A Teardown of the IEEE P1735 Standard for Protecting Electronic-design Intellectual Property", *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1533-1546, ACM, 2017

5. T. Shrimpton, M. Stam and B. Warinschi, "A Modular Treatment of Cryptographic APIs: The Symmetric-Key Case", *Advances in Cryptology – CRYPTO 2016, Lecture Notes in Computer Science*, vol. 9815, pp. 277-307, Springer, 2016

Publications (General)

1. K. G. Paterson, T. Ristenpart and T. Shrimpton, "Tag size does matter: Attacks and Proofs for the TLS Record Protocol", *Advances in Cryptology – ASIACRYPT 2011, Lecture Notes in Computer Science*, vol. 7073, pp. 372-389, Springer, 2011

2. K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton, "Peek-a-boo, I still see you: Why efficient traffic analysis countermeasures fail", *2012 IEEE Symposium on Security and Privacy*, pp. 332-346, IEEE, 2012

3. D. Luchaup, K. Dyer, S. Jha, T. Ristenpart and T. Shrimpton, "LibFTE: a toolkit for constructing practical, format-abiding encryption schemes", *Proceedings of the 23rd USENIX conference on Security Symposium*, pp. 877-891, USENIX Association, 2014

4. Y. Dodis, T. Ristenpart and T. Shrimpton "Salvaging Merkle-Damgård for Practical Applications", *Advances in Cryptology – EUROCRYPT 2009, Lecture Notes in Computer Science*, vol. 4579, pp. 371-388, Springer, 2009

5. P. Rogaway and T. Shrimpton, "Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance", *Fast Software Encryption 2004, Lecture Notes in Computer Science*, vol. 3017, pp. 371-388, Springer-Verlag, 2004

Synergistic Activities

Developed courses: Cryptography; Counting, Probability and Computing

Broading participation: MS advisor for Ms. Erin Chapman, Ms. Morgan Miller; PhD committee member for Mrs. Nichole Schimanski; advisor for Ms. Tashell Kelley

Invited or Keynote lecturer: Summer School on Real-World Crypto and Privacy (Croatia, 2017), Issac Newton Insitute (Cambridge, UK, 2012), Fast Software Encryption (Seoul, Korea, 2010), Ecrypt Summer School on Provable Security (Barcelona, Spain, September 2009), Ecrypt Autumn School on Cryptographic Hash Functions (Tenerife, Spain, November 2009), Fast Software Encryption 2010 (Seoul, Korea, February 2010).

Secretary, International Association for Cryptologic Research (IACR): 2007-2010; General Chair, CRYPTO 2011; Organizing committee, Real World Cryptography 2013-2017;
Programm committee member: Usenix Security 2017; NDSS 2017; CCS 2016; PoPETS 2017; Fast Software Encryption 2016, 2015, 2013; CRYPTO 2015, 2014, 2012, 2008; ASIACRYPT 2013, 2010; EUROCRYPT 2016, 2014, 2011, 2009; Public Key Cryptography 2011; ICDCS 2011; International Conference on Applied Cryptography and Network Security 2007, 2008; 7th International Workshop on Information Security Applications, IEEE Security in Storage Workshop 2005; Conference on Information Security and Cryptography 2005

Affiliations

Collaborators
See uploaded Collaborators document.

Graduate and Postdoctoral Advisors
Phillip Rogaway (UC Davis)