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. D. Luchaup, T. Shrimpton, T. Ristenpart and S. Jha, "Formatted Encryption beyond Regular Languages", *ACM SIGSAC Conference on Computer and Communication Security – CCS'14*, pp. (TBD), ACM, 2014

2. 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 Security Symposium*, pp. 877-891, USENIX, 2014

3. K. Dyer, S. Coull, T. Ristenpart and T. Shrimpton, "Protocol Misidentification Made Easy with Format-Transforming Encryption", *ACM SIGSAC Conference on Computer and Communication Security – CCS'13*, pp. 61-72, ACM, 2013

4. K. Dyer, S. Coull, T. Ristenpart and T. Shrimpton, "Peek-a-Boo, I Still See You: Why Traffic Analysis Countermeasures Fail", *IEEE Symposium on Security and Privacy 2012*, pp. 332-346, IEEE, 2012

5. 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

Publications (General)

1. T. Ristenpart, T. Shrimpton and H. Shacham, "Careful with Composition: Limitations of the Indifferentiability Framework", *Advances in Cryptology – EUROCRYPT 2011, Lecture Notes in Computer Science*, vol. 6632, pp. 487-506, Springer, 2011

2. 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

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. 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

5. J. Black, P. Rogaway, and T. Shrimpton, "Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV", *Advances in Cryptology — CRYPTO 2002*, Lecture Notes in Computer Science, Vol. 2442. pp. 320-335, Springer-Verlag, 2002.

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: 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: 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
John Black (CU Boulder, USA), Scott Coull (Red Jack, USA), Yevgeniy Dodis (NYU, USA), Kevin Dyer (Portland State, USA), Marc Fischlin (TU-Darmstadt, Germany), Will Landecker (Portland State, USA), Anja Lehmann (IBM-Zurich, Switzerland), Onur Özen (EPFL, Switzerland), Kenneth Paterson (Royal Holloway, UK), Thomas Ristenpart (Cornell Tech, USA), Phillip Rogaway (UC Davis, USA), Hovav Shacham (UC San Diego, USA), Martijn Stam (University of Bristol, UK), Robert Terashima (Portland State, USA), Stefano Tessaro (UC Santa Barbara, USA)

Graduate and Postdoctoral Advisors
Phillip Rogaway (UC Davis)