Thomas Eric Shrimpton

Department of Computer and Information Science and Engineering
E301 CSE Bldg.
P. O. Box 116120
University of Florida
Gainesville, FL 32611 USA

office: +1 352 294-2092
FAX: +1 352 273-0738

Email: teshrim@ufl.edu
WWW: http://www.cise.ufl.edu/~teshrim/

Current Appointments

Associate Professor *9/16-present*
Department of Computer and Information Science and Engineering
University of Florida

Other Positions

Associate Professor *9/12-8/16*
Assistant Professor *6/04-6/12*
Department of Computer Science, Portland State University

Assistant Professor *9/07-8/09*
Faculty of Informatics, University of Lugano, Switzerland

Visiting Professor *6/06-12/06*
School of Computer and Communication Sciences, EPFL, Lausanne, Switzerland

Research Areas

Cryptography, applied cryptography, censorship circumvention, network security, hardware security, secure data structures, adversarial signal processing

Education

University of California, Davis *9/98–6/04*
Ph.D. in Electrical Engineering.
Thesis: Provably-Secure Cryptographic Hashing.
Adviser: Phillip Rogaway.

University of Maryland, Baltimore County *9/94–6/97*
M.S. in Electrical Engineering.
Thesis: Information-Theoretic Enumeration of Cyclostationary Signals

Virginia Polytechnic Institute and State University *9/89–5/94*
B.S. in Electrical Engineering.

Publications
(Note: Various author-ordering conventions observed)

42. C. Patton, T. Shrimpton "Security in the Presence of Key Reuse: Context-Separable Interfaces and their Applications", *Advances in Cryptology – CRYPT0 2019, Lecture Notes in Computer Science*, vol. 11692, pp. 738-768, Springer, 2019

41. D. Clayton, C. Patton, T. Shrimpton, "Probabilistic Data Structures in Adversarial Environments" *ACM SIGSAC Conference on Computer and Communication Security – CCS'19*, pp. 1317-1334, ACM, 2019

40. J. Choi, D. Tian, G. Hernandez, C. Patton, B. Mood, T. Shrimpton, K. Butler, P. Traynor: "A Hybrid Approach to Secure Function Evaluation using SGX." *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security – AsiaCCS 2019*, pp. 100-113, ACM, 2019

39. C. Patton, T. Shrimpton, "Partially Specified Channels: The TLS 1.3 Record Layer without Elision" *ACM SIGSAC Conference on Computer and Communication Security – CCS'18*, pp. 1415-1428, ACM, 2018

38. L. Vargas, G. Hazarika, R. Culpepper, K. Butler, T. Shrimpton, D. Szajda, P. Traynor, "Mitigating Risk While Complying with Data Retention Laws" *ACM SIGSAC Conference on Computer and Communication Security – CCS'18*, pp. 2011-2027, ACM, 2018

37. A. Chhotaray, A. Nahiyan, T. Shrimpton D. Forte, M. Tehranipoor, "Standardizing Bad Cryptographic Practice: A Teardown of the IEEE Standard for Protecting Electronic-design Intellectual Property" *ACM SIGSAC Conference on Computer and Communication Security – CCS'17*, pp. 1533-1546, ACM, 2017

36. A. Boldyreva, C. Patton, T. Shrimpton "Hedging Public-Key Encryption in the Real World", *Advances in Cryptology – CRYPT0 2017, Lecture Notes in Computer Science*, vol. 10403, pp. 462-494, Springer, 2017

35. B. Reaves, L. Blue, H. Abdullah, L. Vargas, P. Traynor, T. Shrimpton, "AuthentiCall: Efficient Identity and Content Authentication for Phone Calls", *USENIX Security Symposium*, pp. 575-592, USENIX, 2017

34. L. Dixon, T. Ristenpart and T. Shrimpton, "Network Traffic Obfuscation and Automated Internet Censorship", *IEEE Security and Privacy*, vol. 14, pp. 43-53, IEEE, 2016

33. T. Shrimpton and R. Seth Terashima, "Salvaging Weak Bounds for Blockcipher-Based Constructions", *Advances in Cryptology – CRYPT0 2016, Lecture Notes in Computer Science*, vol. 10031, pp. 429-454, Springer, 2016

32. T. Shrimpton, M. Stam and B. Warinschi, "A Modular Treatment of Cryptogaphic APIs: the Symmetric-Key Case", *Advances in Cryptology – CRYPT0 2016, Lecture Notes in Computer Science*, vol. 9814, pp. 277-307, Springer, 2016

31. L. Wang, K. Dyer, A. Akella, T. Ristenpart and T. Shrimpton, "Seeing Though Network-Protocol Obfuscation" *ACM SIGSAC Conference on Computer and Communication Security – CCS'15*, pp. 57-69, ACM, 2015

30. K. Dyer, S. Coull and T. Shrimpton, "Marionette: A Programmable Network Traffic Obfuscation System", *Proceedings of the 24th USENIX Security Symposium*, pp. 367-382, USENIX Security, 2015

29. R. S. Terashima and T. Shrimpton, "A Provable Security Analysis of Intel's Secure Key RNG", *Advances in Cryptology – EUROCRYPT 2015, Lecture Notes in Computer Science*, vol. 9056, pp. 77-100, Springer, 2015

Publications (continued)

28. 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. 1292-1303, ACM, 2014

27. 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 Security, 2014

26. 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

25. 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

24. T. Shrimpton and R. Seth Terashima, "A Modular Framework for Building Variable-Input-Length Tweakable Ciphers", *Advances in Cryptology – ASIACRYPT 2013, Lecture Notes in Computer Science*, vol. 8269, pp. 405-423, Springer, 2013

23. W. Landecker, T. Shrimpton and R. Seth Terashima, "Tweakable Blockciphers with Beyond Birthday-Bound Security", *Advances in Cryptology – CRYPTO 2012, Lecture Notes in Computer Science*, vol. 7417, pp. 14-30, Springer, 2012

22. 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

21. 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

20. 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

19. M. Fischlin, A. Lehmann, T. Ristenpart, T. Shrimpton, M. Stam and S. Tessaro, "Random Oracles With(out) Programmability", *Advances in Cryptology – ASIACRYPT 2010, Lecture Notes in Computer Science*, vol. 6477, pp. 303-320, Springer, 2010

18. J. Black, P. Rogaway, T. Shrimpton and M. Stam, "An Analysis of the Blockcipher-Based Hash Functions from PGV", *Journal of Cryptology*, vol. 23, no. 4, pp. 519-545, Springer, 2010

17. O. Özen, T. Shrimpton, M. Stam, "Attacking the Knudsen-Preneel Compression Function" *Fast Software Encryption 2010, Lecture Notes in Computer Science*, vol. 6147 , pp. 94-115, Springer, 2010 [**Awarded "Best Paper"**]

16. J. Black, M. Cochran and T. Shrimpton, "On the Impossibility of Highly Efficient Blockcipher-Based Hash Functions", *Journal of Cryptology*, vol. 22, no. 3, pp. 311-329, Springer, 2009

15. 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

Publications
(continued)

14. T. Shrimpton and M. Stam, "Building a Collision-Resistant Compression Function From Non-Compressing Primitives", *35th International Colloquium on Automata, Languages and Programming – ICALP 2008, Lecture Notes in Computer Science*, vol. 5126, pp. 643-654, Springer, 2008

13. T. Ristenpart and T. Shrimpton, "How to Build a Hash Function From Any Collision-Resistant Function", *Advances in Cryptology – ASIACRYPT 2007, Lecture Notes in Computer Science*, vol. 4833, pp. 147-163, Springer, 2007

12. E. Andreeva, G. Neven, B. Preneel and T. Shrimpton, "Seven-Property Preserving Iterated Hashing: ROX", *Advances in Cryptology – ASIACRYPT 2007, Lecture Notes in Computer Science*, vol. 4833, pp. 130-146, Springer, 2007

11. S. Singh and T. Shrimpton, "Verifying Delivered QoS in Multi-hop Wireless Networks", *IEEE Transactions on Mobile Computing* vol. 6, no. 12, pp. 1370-1383, 2007

10. 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

9. P. MacKenzie, T. Shrimpton and M. Jakobsson, "Threshold Password-Authenticated Key Exchange", *Journal of Cryptology*, vol. 19, no. 1, pp. 27-66, Springer, 2006

8. J. Black, M. Cochran and T. Shrimpton, "On the Impossibility of Highly Efficient Blockcipher-Based Hash Functions", *Advances in Cryptology – EUROCRYPT 2005, Lecture Notes in Computer Science*, vol. 3494, pp. 526-541, Springer, 2005

7. 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

6. P. MacKenzie, T. Shrimpton and M. Jakobsson, "Threshold Password-Authenticated Key Exchange (Extended Abstract)", *Advances in Cryptology – CRYPTO 2002, Lecture Notes in Computer Science*, vol. 2442, pp. 385-400, Springer-Verlag, 2002.

5. J. Black, P. Rogaway, and T. Shrimpton, "Encryption Scheme Security in the Presence of Key-Dependent Messages", *Selected Areas in Cryptography — SAC 2002*, Lecture Notes in Computer Science, Vol. 2595, pp. 62-75, Springer-Verlag, 2002.

4. 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.

3. T. E. Shrimpton and S. V. Schell, "Source Enumeration Using a Signal Selective Information Theoretic Criterion", *Proc. 1997 IEEE Military Communications Conf.,* Monterey, CA, Nov. 1997, pp. 1092-1097

2. S. V. Schell and T. E. Shrimpton, "Super-Exponentially Convergent Blind Fractionally-Spaced Equalization and Cochannel Interference Mitigation", *Proc. 1996 IEEE Military Communications Conf.*, McLean, VA, Oct. 1996, pp. 607-611

1. S. V. Schell and T. E. Shrimpton, "Super-Exponentially Convergent Blind Fractionally-Spaced Equalization", *Proc. 29th Asilomar Conf. on Sig., Sys., and Comp.*, Pacific Grove, CA, Oct. 1995, pp. 703-709

Manuscripts

4. A. Chhotaray, T. Shrimpton, "Provable-Security Foundations for Design-Hiding Schemes for Stateless Circuits", in submission (2020)

3. C. Patton, T. Shrimpton, "The Security Impact of Translating Papers into Standards", in submission (2020)

2. H. Abdullah, M. Rahman, W. Garcia, L. Blue, K. Warren, A. Yadav, T. Shrimpton, P. Traynor: "Hear 'No Evil', See 'Kenansville': Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems", in submission (2019)

1. P. Rogaway and T. Shrimpton, "The SIV Mode of Operation for Deterministic or Nonce-Based Authenticated-Encryption", contributed to NIST/ANS X9.102.

Funding

DARPA Resiliant Anonymous Communication for Everyone (RACE). Period: 2019-2023. Amount: **$1,400,000**

NSF Secure and Trustworthy Computing. "Securing the Voice Processing Pipeline". Period: 2019-2022, Amount: **$1,200,000** (Co-PI portion: $400,000)

NSF Secure and Trustworthy Computing. "API-centric Cryptography". Period: 2019-2022, Amount: **$450,000**

NSF Student Travel grant. Period 2019. Amount: **$18,000**

NIST. "Utilizing NIST Entropy as a Service and Chaotic Circuits for Management of Electronics Supply Chain". Period: 2016-2019. Amount: **$497,000** (Co-PI portion: $150,000)

NSF Student Travel. Period 2017. Amount: **$18,000**

Gift from Eric Schmidt, Google Executive CEO. Amount: **$100,000 (Unsolicited gift.)**

NSF Secure and Trustworthy Computing. "Distribution-Sensitive Cryptography". Period: 2015-2019. Amount: **$400,000**.

NSF Secure and Trustworthy Computing. "Tweakable-blockcipher-based Cryptography". Period: 2013-2017. Amount: **$443,000**.

NSF **CAREER** award. "CAREER: Design Principles for Cryptographic Hash Functions: Foundations, Primitives, and Transforms". Period: 2009-2014. Amount: **$400,000**.

NSF Cybertrust. "Making Proofs-of-Work Work". Period: 2006-2009 Amount: **$399,711**.

Advising

James Howes (CS PhD, University of Florida, Advisor. Expected 2023),
David Clayton (CS PhD, University of Florida, Advisor. Expected 2022),
Animesh Chhotaray (CS PhD, University of Florida, Advisor. Expected 2021.),
Christopher Patton (CS PhD, University of Florida, Advisor. Expected 2020),
Robert Terashima (CS PhD, Portland State University, Advisor. 2015)
Kevin Dyer (CS PhD, Portland State University, Advisor. 2015)

Christian Peeters (CS PhD, Universtity of Florida, co-chair. Expected 2020),
Nolen Scaife (CS PhD, Universtity of Florida, co-chair. 2019)

Matthew Carr (Math PhD, University of Florida, committee member. Expected 2021),
Endrit Fejzullahu (Math PhD, University of Florida, committee member. Expected 2021),
Vanessa Frost (CS PhD, Universtity of Florida, committee member. Expected 2021),
Joseph Choi (CS PhD, Universtity of Florida, committee member. Expected 2021),
Logan Blue (CS PhD, Universtity of Florida, committee member. Expected 2020),
Jasmine Bowers (CS PhD, Universtity of Florida, committee member. Expected 2020),
Luis Vargas (CS PhD, Universtity of Florida, committee member. Expected 2020),
Hadi Abdullah (CS PhD, Universtity of Florida, committee member. Expected 2020),
Md Tauhidur Rahmon (EE PhD, Universtity of Florida, committee member. 2017),
Bradley Reaves (CS PhD, Universtity of Florida, committee member. 2017),
Jean-Paul Degabrille (PhD, Royal Holloway University of London, Vita committee, 2014)
Nichole Schimanski (Math PhD, Portland State University, committee member)
Morgan Miller (MS, University of Lugano, 2010)
Alex Ross (MS, Portland State University, 2009)
Stephan Bekefi, (Computer Science Undergraduate Honors Thesis, 2007)

Invited Talks

Invited Lecturer, European Summer School on Real-World Cryptography, July 2018

Invited Lecturer, European Summer School on Real-World Cryptography, July 2017

Invited Lecturer, Romanian Summer School on Cryptography, July 2014

Invited Lecturer, Scandinavian Summer School on Cryptography. July 2013

Visiting Fellow, Issac Newton Institute, Cambridge University, "A long answer to the simple question: Is SSL/TLS secure?", January 2012

Keynote Lecturer, Fast Software Encryption (FSE) 2010. "A provable security perspective on the design of hash functions." Seoul, Korea, February 2010

Invited Lecturer, Ecrypt Autumn School on Hash Functions. Tenerife, Spain, November 2009

Invited Lecturer, Ecrypt Summer School on Provable Security. Barcelona, Spain, September 2009

"Cryptographic Hashing: Basics, Blockciphers, and Beyond." Presented at: IBM Research Labs (Zürich, Switzerland, May 2008); University of Oregon (Oregon, USA, May 2007); University of Bristol (Bristol, UK, November 2006); Katholieke Universiteit Leuven (Leuven Belgium, September 2006); Summer Research Institute, Ecole Polytechnique Federale de Lausanne (EPFL) (Lausanne, Switzerland, July 2006); INTEL (Oregon, USA, March 2005);

Desiderata for Future Hash Functions. Panelist, NIST Cryptographic Hash Function Worshop, Washington D. C. October 2005

Cryptographic Hashing Tutorial (and Recent Results). Presented at CRYPTO '04 Graduate Student Birds-of-a-Feather, August 2004

Cryptographic Hashing: Blockcipher-Based Constructions, Revisited. Presented at DIMACS Workshop on Cryptography: Theory meets Practice, New Jersey, USA November 2004.

Courses Taught (*from scratch)

Introduction to Cryptography (University of Florida, 2016-2020)*
Randomized Algorithms and Probabilistic Analysis (Portland State, 2014-2015)*
Graduate Theory of Computation (Portland State, 2013)*
Theory of Computation (Portland State, 2012)
Counting, Probability and Computing (Portland State, 2010-2012)*
Modern Cryptography (Portland State, 2004-2007, 2009-2015)*
Advanced Topics in Cryptography (Portland State, 2005-2006)*
Abstract Algebra and Mathematical Reasoning (University of Lugano, 2007)*
Modern Cryptography and Communication Security (University of Lugano, 2007-2009)*
Combinatorics (University of Lugano, 2008)*
Discrete Structures II (University of Lugano, 2009)*
Signals and Systems (UC Davis, 2004)
Design and Analysis of Algorithms (UC Davis, 2003)

Professional Service

Organizing Committee: Real World Cryptography (RWC), 2012-2020

Program Chair: Real World Cryptography (RWC) 2021

General Chair: CRYPTO 2011

Secretary, International Association for Cryptologic Research (IACR): 2007-2010

Program Committee Member: CRYPTO 2020, RWC 2020, CRYPTO 2019, RWC 2019 IEEE Security and Privacy Symposium 2019, RWC 2018, ACM CCS 2018, USENIX Security 2017, PoPETS 2017, FSE/ToSC 2017, NDSS 2017, ACM CCS 2016, EUROCRYPT 2016, FSE 2016, FSE 2015, SCN 2014, CRYPTO 2014, ASIACRYPT 2013, CRYPTO 2012, EUROCRYPT 2011, Public Key Cryptography 2011, ASIACRYPT 2010, EUROCRYPT 2009, CRYPTO 2008, International Conference on Applied Cryptography and Network Security 2007 and 2008, 7th International Workshop on Information Security Applications, IEEE Security in Storage Workshop 2005, Conference on Information Security and Cryptography 2005,

Referee for: Journal of Cryptography, IEEE Transactions on Information Theory, Journal of Computer Security, Journal of Systems and Software

Proposal Referee for Army Research Office, NSF (multiple SaTC small and medium panels, SaTC frontier panel 2014), Belgian FWO proposals (Post-doctoral Fellowships, 2012-14)

Univesity Service (UF)

Teaching committee (Cybersecurity area coordinator): 2019-,
Graduate Affairs committee: 2019-,
Cybersecurity hiring search committee: 2018-2019,
Steering committee: 2017-2019,
Colloquium committee: 2015-2016,
Facilities committee: 2015-2019.

University Service (PSU)

Math/Stat-ECE-CS statistics course development: 2014-2015
Maseeh College of Engineering and Computer Science, Dean's "Vision 2030" committee
Faculty search committee: 2010, 2011, 2012, 2013
Colloquium chair: 2011-2012
Graduate admissions committee at Portland State: 2005, 2006, 2009, 2011

Industrial Experience

Lucent Technologies, Bell Labs *Research Intern 6/01–8/01*
Developed a provably-secure protocol for password-authenticated key-exchange that is secure against server compromise.

Statistical Signal Processing, Inc. *R & D Consultant 7/97–12/00*
Lead engineer on a large GSM signal separation project, with primary responsibilities for development of adjacent-channel interference suppression and reduced-state joint maximum-likelihood sequence estimation (JMLSE) technologies. Investigated multiple competing signal-separation technologies, including some based on linear-conjugate-linear processors, frequency-shift filters, and variants of JMLSE.

Booz·Allen & Hamilton, Inc. *Sr. Consultant, 3/95-5/97, Consultant 5/94–3/95*
Researched, developed and implemented signal processing and communication algorithms and systems for a broad range of applications including: blind equalization of terrestrial microwave links, cochannel interference mitigation, direction finding in urban environments, blind-array beamforming, signal classification, specific emitter identification. Provided technical advice and oversight for several fielded signals intelligence systems. Identified, helped procure and led two sole-source contracts ($250k, $100k) for cochannel interference mitigation of GSM signals, and time-frequency and higher-order statistical analysis of exotic radar signals. Technical contributor to several multi-million dollar proposal efforts.

National Security Agency *Engineering Intern 1/90–8/93*
Implemented several small-mission, real-time, DSP chip-based signal processing systems.