Stefano Tessaro

Last update: February 24, 2017

Department of Computer Science
University of California, Santa Barbara
Harold Frank Hall, Room 1117
Santa Barbara, CA 93106, USA

E-mail: *tessaro@cs.ucsb.edu*
Web: *http://www.cs.ucsb.edu/∼tessaro/*

Research Interests

Foundations and applications of cryptography; Computer security; Theory of computation.

Employment

- **University of California, Santa Barbara**, Santa Barbara, CA. *2013 — present*
  Assistant professor.
  Holder of the *Glen and Susanne Culler Chair* in Computer Science.
- **Massachusetts Institute of Technology**, Cambridge, MA. *2012 — 2013*
  Research scientist (until 11/2012: postdoctoral associate).
- **University of California, San Diego**, La Jolla, CA. *2010 — 2012*
  Postdoctoral scholar.
- **ETH Zurich**, Zurich, Switzerland. *2005 — 2010*
  Research and teaching assistant.
- **IBM Research**, Zurich Research Lab, Switzerland. *Winter 2004/05*
  Research intern.

Education

- **ETH Zurich**, Zurich, Switzerland. *2005 — 2010*
  PhD in Computer Science (Dr. Sc. ETH): October 2010.
  Advisor: Ueli Maurer.
  Thesis title: *Computational Indistinguishability Amplification*.
- **ETH Zurich**, Zurich, Switzerland. *2000 — 2005*
  MSc ETH in Computer Science (with honors): November 2005.
  GPA: 5.93 / 6.00.

Awards & Honors

- **Alfred P. Sloan Research Fellowship**, 2017.
- **Best Paper Award** at EUROCRYPT 2017.
- **NSF CAREER Award**, 2016.
- **Northrop Grumman Excellence in Teaching Award**, 2016.
- **Hellman Fellowship**, 2015.
- **Postdoctoral fellowship** for prospective researchers from the Swiss National Science Foundation (SNF) (Declined).
- **Paper invited to Journal of Cryptology** at CRYPTO 2016.
- **Best student paper award** at TCC 2011.

- ◇ **ETH Medal** for outstanding doctoral dissertation (awarded to top 8% PhD graduates within each year at ETH Zurich).
- ◇ **Willi Studer Award** for highest GPA among computer science graduate 2005 / 06 at ETH Zurich.

Publications

Conference Papers

[C.1] Christian Cachin and Stefano Tessaro. **Asynchronous verifiable information dispersal.** In *Proceedings of 24th IEEE Symposium on Reliable Distributed Systems (SRDS 2005)*, pp. 191–202, 2005.

[C.2] Christian Cachin and Stefano Tessaro. **Optimal resilience for erasure-coded Byzantine distributed storage.** In *Proceedings of the International Conference on Dependable Systems and Networks (DSN 2006)*, pp. 115–124, 2006.

[C.3] Ueli Maurer and Stefano Tessaro. **Domain extension of public random functions: Beyond the birthday barrier.** In *Advances in Cryptology — CRYPTO 2007*, LNCS, vol. 4622, pp. 187–204, 2007.

[C.4] Ueli Maurer and Stefano Tessaro. **Basing PRFs on constant-query weak PRFs: Minimizing assumptions for efficient symmetric cryptography.** In *Advances in Cryptology — ASIACRYPT 2008*, LNCS, vol. 5350, pp. 161–178, 2008.

[C.5] Robert König, Ueli Maurer, and Stefano Tessaro. **Abstract storage devices.** In *SOFSEM 2009*, LNCS, vol. 5404, pp. 341–352, 2009.

[C.6] Ueli Maurer and Stefano Tessaro. **Computational indistinguishability amplification: Tight product theorems for system composition.** In *Advances in Cryptology — CRYPTO 2009*, LNCS, vol. 5677, pp. 355–373, 2009.

[C.7] Anja Lehmann and Stefano Tessaro. **A modular design for hash functions: Towards making the Mix-Compress-Mix approach practical.** In *Advances in Cryptology — ASIACRYPT 2009*, LNCS, vol. 5912, pp. 364–381, 2009.

[C.8] Ueli Maurer and Stefano Tessaro. **A hardcore lemma for computational indistinguishability: Security amplification for arbitrarily weak PRGs with optimal stretch.** In *Theory of Cryptography — TCC 2010*, LNCS, vol. 5978, pp. 237–254, 2010.

[C.9] Marc Fischlin, Anja Lehmann, Thomas Ristenpart, Thomas Shrimpton, Martijn Stam, and Stefano Tessaro. **Random oracles with(out) programmability.** In *Advances in Cryptology — ASIACRYPT 2010*, LNCS, vol. 6477, pp. 303–320, 2010.

[C.10] Stefano Tessaro. **Security amplification for the cascade of arbitrarily weak PRPs: Tight bounds via the interactive hardcore lemma.** In *Theory of Cryptography — TCC 2011*, LNCS, vol. 6597, pp. 37–54, 2011.
Best student paper award, Invited to the Journal of Cryptology.

[C.11] Thomas Holenstein, Robin Künzler, and Stefano Tessaro. **Equivalence of the random oracle model and the ideal cipher model, revisited.** In *Proceedings of the 43rd ACM Symposium on Theory of Computing (STOC 2011)*, pp. 89-98, 2011.

[C.12] Peter Gaži and Stefano Tessaro. **Efficient and optimally secure key-length extension for block ciphers via randomized cascading.** In *Advances in Cryptology — EUROCRYPT 2012*, LNCS, vol. 7327, pp. 63-80, 2012.

[C.13] Mihir Bellare, Thomas Ristenpart, and Stefano Tessaro. **Multi-instance security and its application to password-based cryptography.** In *Advances in Cryptology — CRYPTO 2012*, LNCS, vol. 7417, pp. 312–329, 2012.

[C.14] Mihir Bellare, Stefano Tessaro, and Alexander Vardy. **Semantic security for the wiretap channel.** In *Advances in Cryptology — CRYPTO 2012*, LNCS, vol. 7417, pp. 294–311, 2012.

[C.15] Yevgeniy Dodis, Thomas Ristenpart, John Steinberger, and Stefano Tessaro. **To hash or not to hash again? (In)differentiability results for H^2 and HMAC.** In *Advances in Cryptology — CRYPTO 2012.* LNCS, vol. 7417, pp. 348–366, 2012.

[C.16] Daniele Micciancio and Stefano Tessaro. **An equational approach to secure multi-party computation.** In *Innovations in Theoretical Computer Science — ITCS 2013*, pp. 355–372, 2013.

[C.17] Elette Boyle, Shafi Goldwasser, and Stefano Tessaro. **Communication locality in secure multi-party computation: How to run sublinear algorithms in a distributed setting.** In *Theory of Cryptography — TCC 2013*, LNCS, vol. 7785, pp. 356–376, 2013.

[C.18] Huijia Lin and Stefano Tessaro. **Amplification of chosen-ciphertext security.** In *Advances in Cryptology – EUROCRYPT 2013,* LNCS, vol 7881, pp. 503–519, 2013.

[C.19] Flavio Calmon, Mayank Varia, Muriel Médard, Mark Christiansen, Ken Duffy, and Stefano Tessaro. **Bounds on inference.** In *Proceedings of the 51st Annual Allerton Conference on Communication, Control, and Computing,* 2013.

[C.20] Joël Alwen, Manuel Barbosa, Pooya Farshim, Rosario Gennaro, S. Dov Gordon, Stefano Tessaro, and David A. Wilson. **On the relationship between functional encryption, fully homomorphic encryption, and obfuscation.** In *Proceedings of the 14th IMA International Conference on Cryptography and Coding,* LNCS, vol. 8308, pp. 65–84, 2013.

[C.21] Stefano Tessaro and David A. Wilson. **Bounded-collusion identity-based encryption from semantically-secure public-key encryption: Generic constructions with short ciphertexts.** In *Public-Key Cryptography — PKC 2014*, LNCS, vol. 8383, pp. 257–274, 2014.

[C.22] David Cash and Stefano Tessaro. **The locality of searchable symmetric encryption.** In *Advances in Cryptology — EUROCRYPT 2014*, LNCS, vol. 8441, pp. 351–368, 2014.

[C.23] Mihir Bellare, Igors Stepanovs, and Stefano Tessaro. **Poly-Many Hardcore Bits for Any One-Way Function and a Framework for Differing-Inputs Obfuscation.** In *Advances in Cryptology — ASIACRYPT 2014 (Volume 2)*, LNCS, vol. 8874, pp. 102–121, 2014.

[C.24] Ran Canetti, Huijia Lin, Stefano Tessaro, Vinod Vaikuntanathan. **Obfuscation of probabilistic circuits and applications.** In *Theory of Cryptography – TCC 2015 (Volume 2)*, LNCS, vol. 9015, pp. 468–497, 2015

[C.25] Peter Gaži, Jooyoung Lee, Yannick Seurin, John Steinberger, and Stefano Tessaro. **Relaxing full-codebook security: A Refined analysis of key-length extension schemes**. In *Fast Software Encryption FSE 2015*, LNCS vol. 9054, pp. 319–341, 2015.

[C.26] Peter Gaži, Krzysztof Pietrzak, and Stefano Tessaro. **The exact PRF security of truncation: Tight bounds for keyed sponges and truncated CBC**. In *Advances in Cryptology – CRYPTO 2015 (Part I)*, LNCS, vol. 9215, pp. 368–387, 2015.

[C.27] Peter Gaži, Krzysztof Pietrzak, and Stefano Tessaro. **Generic security of NMAC and HMAC with input whitening**. In *Advances in Cryptology — ASIACRYPT 2015 (Part II)*, LNCS, vol. 9453, pp. 85–109, 2015.

[C.28] Stefano Tessaro. **Optimally secure block ciphers from ideal primitives**. In *Advances in Cryptology — ASIACRYPT 2015 (Part II)*, LNCS, vol. 9453, pp. 437–462, 2015.

[C.29] David Cash, Eike Kiltz, and Stefano Tessaro. **Two-round man-in-the-middle security from LPN**. In *Theory of Cryptography — TCC 2016-A (Part I)*, LNCS, vol. 9562, pp. 225–248, 2016.

[C.30] Binyi Chen, Huijia Lin, and Stefano Tessaro. **Oblivious Parallel RAM: Improved efficiency and generic constructions**. In *Theory of Cryptography — TCC 2016-A (Part II)*, LNCS, vol. 9563, pp. 205–234, 2016.

[C.31] Mihir Bellare, Igors Stepanovs, and Stefano Tessaro. **Contention in Cryptoland: Obfuscation, leakage and UCE**. In *Theory of Cryptography — TCC 2016-A (Part II)*, LNCS, vol. 9563, pp. 542–564, 2016.

[C.32] Peter Gaži and Stefano Tessaro. **Provably robust Sponge-based PRNGs and KDFs**. In *Advances in Cryptology — EUROCRYPT 2016 (Part I)*, LNCS, vol. 9665, pp. 87–116, 2016.

[C.33] Mihir Bellare, Daniel J. Bernstein, and Stefano Tessaro. **Hash-function based PRFs: AMAC and its multi-user security**. In *Advances in Cryptology — EUROCRYPT 2016 (Part I)*, LNCS, vol. 9665, pp. 566–595, 2016.

[C.34] Joel Alwen, Binyi Chen, Chethan Kamath, Vladimir Kolmogorov, Krzysztof Pietrzak, and Stefano Tessaro. **On the complexity of Scrypt and proofs of space in the parallel random oracle model**. In *Advances in Cryptology — EUROCRYPT 2016 (Part II)*, LNCS, vol. 9666, pp. 358–387, 2016.

[C.35] Cetin Sahin, Victor Zakhary, Amr El Abbadi, Huijia Lin, and Stefano Tessaro. **TaoStore: Overcoming asynchronicity in oblivious data storage** . In *IEEE Symposium on Security & Privacy (S&P) 2016*, IEEE, 2016.

[C.36] Viet Tung Hoang and Stefano Tessaro. **Key-alternating ciphers and key-length extension: Exact bounds and multi-user security**. In *Advances in Cryptology — CRYPTO 2016*, LNCS, 2016.
Invited to the Journal of Cryptology.

[C.37] Mihir Bellare, Viet Tung Hoang, and Stefano Tessaro. **Message-recovery attacks on Feistel-based Format Preserving Encryption.** In *ACM CCS 2016*, ACM, 2016.

[C.38] Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Bruce M. Kapron, Valerie King, and Stefano Tessaro. **Simultaneous secrecy and reliability amplification for a general channel model.** In *Theory of Cryptography — TCC 2016-B*, LNCS, 2016.

[C.39] Viet Tung Hoang and Stefano Tessaro. **The multi-user security of double encryption.** In *Advances in Cryptology – EUROCRYPT 2017*, LNCS, 2017.

[C.40] Pratik Soni and Stefano Tessaro. **Public-seed pseudorandom permutations.** In *Advances in Cryptology – EUROCRYPT 2017*, LNCS, 2017.

[C.41] Joël Alwen, Binyi Chen, Krzysztof Pietrzak, Leonid Reyzin, and Stefano Tessaro. **Scrypt is maximally memory-hard.** In *Advances in Cryptology – EUROCRYPT 2017*,

LNCS, 2017.
Best-paper award.

Journal Papers

[J.1] Jean-Sébastien Coron, Thomas Holenstein, Robin Künzler, Jacques Patarin, Yannick Seurin, and Stefano Tessaro. **How to build an ideal cipher: The indifferentiability of the Feistel Construction.** In *Journal of Cryptology*, pp. 1–54, November 2014.

Short Papers

[S.1] Christian Cachin and Stefano Tessaro. **Brief announcement: Optimal resilience for erasure-coded Byzantine distributed storage.** In *Proceedings of the 19th International Conference in Distributed Computing (DISC 2005)*, LNCS, vol. 3724, pp. 497–498, 2005.

[S.2] Christian Cachin and Stefano Tessaro. **Brief announcement: Asynchronous verifiable information dispersal.** In *Proceedings of the 19th International Conference in Distributed Computing (DISC 2005)*, LNCS, vol. 3724, pp. 503–504, 2005.

[S.3] Peter Gaži and Stefano Tessaro. **Secret-key Cryptography from ideal primitives: A systematic overview**. Proceedings of the Information Theory Workshop (ITW 2015). 2015. (Invited Paper)

Manuscripts

[U.1] Petros Mol and Stefano Tessaro. **Secret-key authentication beyond the challenge-response paradigm: Definitional issues and new protocols.** Manuscript, 2012.

[U.2] Stefano Tessaro and David A. Wilson. **Obfuscating many-to-one functional re-encryption, and its connection to fully-homomorphic encryption.** Manuscript, 2013.

Funding

- NSF CNS-1423566, "Better Security for Efficient Secret-Key Cryptography", $498,751.00 (sole PI) *2014–17*
- NSF CNS-1528178, "Oblivious Cloud Storage Systems, from Theory to Practice — Simpler, More Efficient, More Robust", $498,987.00 (co-PI, PI: Huijia Lin, co-PI: Amr El Abbadi) *2015–18*
- NSF IIS-1528041, "Low-Cost Deduplication and Search for Versioned Datasets", $499,998.00 (co-PI, PI: Tao Yang) *2015–18*
- NSF CNS-1553758 (CAREER), "The Theoretical Foundations of Symmetric Cryptography", $422,212.00 (sole PI). *2016–2021*
- Hellman Foundation, Hellman fellowship, $21,500. *2015-16*
- Gareatis Foundation, Gift, $17,500 (joint with Huijia Lin). *2014–15*

Service

- **Program committee member** of CRYPTO 2011, TCC 2013, IMA Cryptography & Coding 2013, CRYPTO 2014, SCN 2014, ASIACRYPT 2014, TCC 2015, ACNS 2015, ACM CCS 2015, SCN 2016, ICITS 2016, ACM CCS 2016, NDSS 2017, CRYPTO 2017.

- ◇ Reviewer for the *Journal of Cryptology*, *SIAM Journal on Computing (SICOMP)*, *IEEE Transactions on Information Theory*.
- ◇ External reviewer for several major conferences including CRYPTO, EUROCRYPT, ASIACRYPT, TCC, STOC, FOCS, IEEE S&P, ICALP, FSE, PKC, SAC, SCN, CT-RSA, ICITS, and DSN.
- ◇ Local organizing committee member of TCC 2010.
- ◇ **Internal service at UC Santa Barbara**
  - · Faculty Recruitment Committee *Winter 2015*
  - · Graduate Admission Committee *Winter 2014, 2016*
  - · Coordinator for Computer Science Distinguished Lectures *2014-16*.

Talks

Selected Invited Talks

- ◇ **Information-theoretic indistinguishability: New techniques and applications.**
  Workshops on Mathematics of Information-theoretic Cryptography, Singapore. *9/2016*
  ICITS 2016, Tacoma, Washington. *8/2016*
- ◇ **The memory hardness of Scrypt.**
  Early Symmetric Cryptography Workshop, Luxembourg. *1/2016*
  Real-World Cryptography 2017, New York, NY. *1/2016*
  Simons Reunion Workshop, Simons Institute, Berkeley, CA. *8/2016*
- ◇ **TaoStore: Overcoming asynchronicity in oblivious data storage**.
  DIMACS/MACS Workshop on Cryptography in the RAM Model of Computation *6/2016*
- ◇ **A cryptographic perspective on the wiretap channel.**
  Nexus of Information and Computation Theories Institute Henri Poincaré, Paris, France. *3/2016*
- ◇ **Contention in Cryptoland: Obfuscation, leakage and UCE.**
  Simons Workshop on Securing Computation, Berkeley, CA. *6/2015*
- ◇ **Secret-key cryptography from ideal primitives: A systematic overview.**
  Information Theory Workshop (ITW 2015), Jerusalem, Israel. *5/2015*
- ◇ **Optimally secure block ciphers from ideal primitives**
  Tel Aviv University, Tel Aviv, Israel. *5/2015*
- ◇ **Poly-many hardcore bit for every one-way function.**
  IST Austria *8/2014*
  Oberwolfach Seminar on Cryptography *7/2014*
- ◇ **The locality of symmetric searchable encryption.**
  Oberwolfach Seminar on Cryptography *7/2014*
- ◇ **Ideal models in symmetric cryptography.**
  Workshop on "Visions of Cryptography" in honor of Turing Award winners Shafi Goldwasser and Silvio Micali. Weizmann Institute, Rehovot, Israel. *12/2013*

◇ **Theoretical foundations for applied cryptography.**
University of Southern California, Los Angeles, CA. *04/2013*
University of Virginia, Charlottesville, VA. *03/2013*
Stony Brook University, Stony Brook, NY. *03/2013*
Purdue University, West Lafayette, IN. *03/2013*
University of California, Santa Barbara, Santa Barbara, CA. *02/2013*
Ohio State University, Columbus, OH. *01/2013*

◇ **Amplification of chosen-ciphertext security.**
New York Area Crypto Day, City College, New York, NY. *04/2013*

◇ **Semantic security for the wiretap channel.**
Workshop on "Formal and Computational Cryptographic Proofs", Isaac Newton Institute for Mathematical Sciences, University of Cambridge, UK. *04/2012*
New York Area Crypto Day, Columbia University, New York, NY. *03/2012*
Qualcomm Security Seminar, San Diego, CA. *01/2012*
MIT CIS Seminar, Cambridge, MA. *12/2011*

◇ **Equivalence of the random oracle model and the ideal cipher model, revisited.**
Boston University Security Seminar, Boston, MA. *03/2012*
MIT CIS Seminar, Cambridge, MA. *12/2011*
Dagstuhl Seminar on Public-Key Cryptography, Dagstuhl, Germany. *9/2011*

◇ **Computational indistinguishability amplification.**
Darmstadt University of Technology, Germany. *04/2009*

◇ **Minimizing assumptions for efficient symmetric cryptography.**
EPFL, Lausanne, Switzerland. *11/2008*

◇ **Domain extension of public random functions.**
ECRYPT Hash Function Workshop, Leiden University, The Netherlands. *6/2008*

Conference Talks

◇ EUROCRYPT 2016, TCC 2016, ASIACRYPT 2015, CRYPTO 2015, EUROCRYPT 2013, CRYPTO 2012, TCC 2011, ASIACRYPT 2010, TCC 2010, ASIACRYPT 2009, CRYPTO 2009, SOFSEM 2009, ASIACRYPT 2008, CRYPTO 2007, DISC 2005.

Other Talks

◇ Held several **outreach talks** on cryptography for general audience and for prospective computer science students at ETH Zurich.

Teaching

◇ **University of California, Santa Barbara**. Taught the following classes:

- CS290G – Introduction to Modern Cryptography (Graduate) *W2014, W2016*
- CS138 – Formal Languages and Automata *F2014, F2015*
- CS290G – Research Topics in Cryptography (Graduate) *W2015*
- CS177 – Computer Security *Sp2015, Sp2016*

◇ **Teaching assistant at ETH Zurich** for classes on discrete mathematics, information theory, and cryptography held by Prof. Ueli Maurer and Prof. Stefan Wolf (between 2002 and 2010). Additionally co-organized a student seminar on research topics in cryptography with Martin Hirt (Summer semester 2008).

Advising

◇ **Postdocs.**

· Viet Tung Hoang (2015-16, next position: Tenure-track assistant professor at Florida State University)

◇ **Graduate students.**

· Binyi Chen (PhD) *In progress*

· Pratik Soni (PhD) *In progress*

· Benjamin Terner (PhD) *In progress*

· Wei Dai (MS) *Graduated 8/2016*

· John Retterer-Moore (MS) *Graduated 8/2015*

· David Wilson (at MIT, informally co-advised with Shafi Goldwasser, graduated: Summer 2014, now at Lincoln Labs).

◇ Advisor of three master / diploma theses and one semester thesis during my graduate studies at ETH Zurich, jointly with Prof. Ueli Maurer.