Stefano Tessaro

Last update: May 24, 2023

Paul G. Allen School of Computer Science & Engineering
University of Washington
Seattle, WA 98195-2350, USA

tessaro@cs.washington.edu
https://homes.cs.washington.edu/∼tessaro/

Research Interests

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

Employment

- **Paul G. Allen School of Computer Science & Engineering**
  University of Washington, Seattle, WA.
  Associate professor (with tenure). *2019 —*
  Paul G. Allen Development Professor *2022 —*
- **University of California, Santa Barbara**, Santa Barbara, CA. *2013 — 2018*
  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.

Awards & Honors

- **Alfred P. Sloan Research Fellowship**, 2017.
- **NSF CAREER Award**, 2016.
- **Northrop Grumman Excellence in Teaching Award**, 2016.
- **Hellman Fellowship**, 2015.
- **Best Paper Award** at EUROCRYPT 2017.
- **Best Student Paper Award** at TCC 2011.

- ◇ **Papers [C.50], [C.41], [C.36], [C.10] invited to the Journal of Cryptology**.
- ◇ **Postdoctoral fellowship** for prospective researchers from the Swiss National Science Foundation (SNF) (Declined).
- ◇ **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 graduates in 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*, pp. 198–217, 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 (Part I)*, LNCS, vol. 9814, pp. 3–32, 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*, pp. 444–455, 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 (Part I)*, LNCS, vol. 9985, pp. 235–261, 2016.

[C.39] Viet Tung Hoang and Stefano Tessaro. **The multi-user security of double encryption.** In *Advances in Cryptology – EUROCRYPT 2017 (Part II)*, LNCS, vol. 10211, pp. 381–411, 2017.

[C.40] Pratik Soni and Stefano Tessaro. **Public-seed pseudorandom permutations.** In *Advances in Cryptology – EUROCRYPT 2017 (Part II)*, LNCS, vol. 10211, pp. 412–441, 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 (Part III)*, LNCS, vol. 10212, pp. 33–62, 2017.
Best-paper award. Invited to the Journal of Cryptology.

[C.42] Huijia Lin and Stefano Tessaro. **Indistinguishability obfuscation from trilinear maps and block-wise local PRGs.** In *Advances in Cryptology – CRYPTO 2017 (Part I)*, LNCS, vol. 10401, pp. 630–660, 2017.

[C.43] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. **Information-theoretic indistinguishability via the Chi-squared method.** In *Advances in Cryptology – CRYPTO 2017 (Part III)*, LNCS, vol. 10403, pp. 497–523, 2017.

[C.44] Elette Boyle, Niv Gilboa, Yuval Ishai, Huijia Lin, and Stefano Tessaro. **Foundations of homomorphic secret sharing.** *ITCS 2018*, pp. 21:1–21:21, 2018.

[C.45] Priyanka Bose, Viet Tung Hoang, and Stefano Tessaro. **Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds**. In *Advances in Cryptology – EUROCRYPT 2018 (Part I)*, LNCS, vol. 10820, pp. 468–499, 2018.

[C.46] Pratik Soni and Stefano Tessaro. **Naor-Reingold Goes Public: The Complexity of Known-key Security.** In *Advances in Cryptology – EUROCRYPT 2018 (Part III)*, LNCS, vol. 10822 , pp. 653–684, 2018.

[C.47] Daniel Agun, Jinjin Shao, Shiyu Ji, Stefano Tessaro, Tao Yang. **Privacy and Efficiency Tradeoffs for Multiword Top K Search with Linear Additive Rank Scoring.** In *WWW 2018*, pp. 1725-1734, 2018.

[C.48] Viet Tung Hoang, Stefano Tessaro, and Ni Trieu. **The Curse of Small Domains: New Attacks on Format-Preserving Encryption.** In *Advances in Cryptology – CRYPTO 2018 (Part I)*, LNCS, vol. 10991, pp. 221-251.

[C.49] Viet Tung Hoang, Stefano Tessaro, and Aishwarya Thiruvengadam. **The Multi-user Security of GCM, Revisited: Tight Bounds for Nonce Randomization.** In *ACM CCS 2018*, pp. 1429-1440, 2018.

[C.50] Stefano Tessaro and Aishwarya Thiruvengadam. **Provable Time-Memory Trade-Offs: Symmetric Cryptography Against Memory-Bounded Adversaries.** In *Theory of Cryptography — TCC 2018 (Part I)*, LNCS, vol. 11239, pp. 3-32, 2018.
Invited to the Journal of Cryptology.

[C.51] Joseph Jaeger and Stefano Tessaro. **Tight Time-Memory Trade-Offs for Symmetric Encryption.** In *Advances in Cryptology — EUROCRYPT 2019 (Part I)*, LNCS, vol. 11476, pp. 467-497, 2019.

[C.52] Sandro Coretti, Yevgeniy Dodis, Harish Karthikeyan, and Stefano Tessaro. **Seedless Fruit Is the Sweetest: Random Number Generation, Revisited.** In *Advances in Cryptology — CRYPTO 2019 (Part I)* , LNCS, vol. 11692, pp. 205-234, 2019.

[C.53] Binyi Chen and Stefano Tessaro. **Memory-Hard Functions from Cryptographic Primitives.** In *Advances in Cryptology — CRYPTO 2019 (Part II)* , LNCS, vol. 11693, pp. 543–572, 2019.

[C.54] Ashrujit Ghoshal and Stefano Tessaro. **On the Memory-Tightness of Hashed ElGamal.** In *Advances in Cryptology — EUROCRYPT 2020 (Part II)* , LNCS, vol. 12106, pp. 33–62, 2020.

[C.55] Ashrujit Ghoshal, Joseph Jaeger, and Stefano Tessaro. **The Memory-Tightness of Authenticated Encryption.** In *Advances in Cryptology — CRYPTO 2020 (Part I)* , LNCS, vol. 12170, pp. 127–156, 2020.

[C.56] Pratik Soni and Stefano Tessaro. **On the Query Complexity of Constructing PRFs from Non-adaptive PRFs.** In *Security and Cryptography for Networks — SCN 2020* , LNCS, vol. 12238, pp. 546–565, 2020.

[C.57] Yevgeniy Dodis, Pooya Farshim, Sogol Mazaheri, and Stefano Tessaro. **Towards Defeating Backdoored Random Oracles: Indifferentiability with Constant Adaptivity.** In *Theory of Cryptography — TCC 2020*, LNCS, vol. 12552, pp. 241–273, 2020.

[C.58] Joseph Jaeger and Stefano Tessaro. **Expected-Time Cryptography: Generic Techniques and Applications to Concrete Soundness.** In *Theory of Cryptography — TCC 2020*, LNCS, vol. 12552, pp. 414–443, 2020.

[C.59] Wei Dai, Stefano Tessaro, and Xihu Zhang. **Super-Linear Time-Memory Trade-Offs for Symmetric Encryption.** In *Theory of Cryptography — TCC 2020*, LNCS, vol. 12552, pp. 335–365, 2020.

[C.60] Pooya Farshim and Stefano Tessaro. **Password Hashing and Preprocessing.** In *Advances in Cryptology - EUROCRYPT 2021*, LNCS, vol. 12697, pp. 64–91, 2021.

[C.61] Tianren Liu, Stefano Tessaro, and Vinod Vaikuntanathan. **The t-wise Independence of Substitution-Permutation Networks.** In *Advances in Cryptology - CRYPTO 2021*, LNCS, vol. 12828, pp. 454–483, 2021.

[C.62] Ashrujit Ghoshal and Stefano Tessaro. **Tight State-Restoration Soundness in the Algebraic Group Model.** In *Advances in Cryptology - CRYPTO 2021*, LNCS, vol. 12827, pp. 64–93, 2021.

[C.63] Joseph Jaeger, Fang Song, and Stefano Tessaro. **Quantum Key-Length Extension.** In *Theory of Cryptography — TCC 2021*, LNCS, vol. 13042, pp. 209–239, 2021.

[C.64] Yu Long Chen and Stefano Tessaro. **Better Security-Efficiency Treade-Offs in Permutation-Based Two-Party Computation.** In *Advances in Cryptology - ASIACRYPT 2021*, LNCS, vol. 13091, pp. 275–304, 2021.

[C.65] Stefano Tessaro and Xihu Zhang. **Tight Security for Key-Alternating Ciphers with Correlated Sub-keys.** In *Advances in Cryptology - ASIACRYPT 2021*, LNCS, vol. 13092, pp. 435–464, 2021.

[C.66] Stefano Tessaro and Chenzhi Zhu. **Short Pairing-Free Blind Signatures with Exponential Security.** In *Advanced in Cryptology — EUROCRYPT 2022*, LNCS, vol. 13276, pp. 782–811, 2022.

[C.67] Ashrujit Ghoshal, Riddhi Ghosal, Joseph Jaeger, and Stefano Tessaro. **Hiding in Plain Sight: Memory-tight Proofs via Randomness Programming.** In *Advanced in Cryptology — EUROCRYPT 2022*, LNCS, vol. 13276, pp. 706–735, 2022.

[C.68] Nirvan Tyagi, Sofia Celi, Thomas Ristenpart, Nick Sullivan, Stefano Tessaro, and Christopher A. Wood. **A Fast and Simple Partially Oblivious PRF, with Applications.** In *Advanced in Cryptology — EUROCRYPT 2022*, LNCS, vol. 13276, pp. 674–705, 2022.

[C.69] Sandro Coretti, Yevgeniy Dodis, Harish Karthikeyan, Noah Stephens-Davidowitz, and Stefano Tessaro. **On Seedless PRNGs and Premature Next.** In *Information-theoretic Cryptography — ITC 2022*, LIPICs vol. 230, pp. 9:1–9:20, 2022.

[C.70] Sujaya Maiyya, Seif Ibrahim, Caitlin Scarberry, Divyakant Agrawal, Amr El Abbadi, Huijia Lin, Stefano Tessaro, and Victor Zakhary. **QuORAM: A Quorum-Replicated Fault Tolerant ORAM Datastore.** In *USENIX Security 2022*, pp. 3665–3682, 2022.

[C.71] Mihir Bellare, Elizabeth C. Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, and Chenzhi Zhu. **Better than Advertised Security for Non-interactive Threshold Signatures.** In *Advanced in Cryptology — CRYPTO 2022*, LNCS, vol. 13510, pp. 517–550, 2022.

[C.72] Nirvan Tyagi, Ben Fisch, Andrew Zitek, Joseph Bonneau, and Stefano Tessaro. **VeRSA: Verifiable Registries with Efficient Client Audits from RSA Authenticated Dictionaries.** In *ACM CCS 2022*, pp. 2793–2807, 2022.

[C.73] Stefano Tessaro and Chenzhi Zhu. **Revisiting BBS Signatures.** In *Advanced in Cryptology — EUROCRYPT 2023*, LNCS, vol. 14008, pp. 691–721, 2023.

[C.74] Stefano Tessaro and Chenzhi Zhu. **Threshold and Multi-Signature Schemes from Linear Hash Functions.** In *Advanced in Cryptology — EUROCRYPT 2023*, LNCS, vol. 14008, pp. 628–658, 2023.

[C.75] Tianren Liu, Angelos Pelecanos, Stefano Tessaro, and Vinod Vaikuntanathan. **Layout Graphs, Random Walks and the t-wise Independence of SPN Block Ciphers.** In *Advanced in Cryptology — CRYPTO 2023*, LNCS, to appear.

[C.76] Elizabeth Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, and Chenzhi Zhu. **Snowblind: A Threshold Blind Signature in Pairing-Free Groups.** In *Advanced in Cryptology — CRYPTO 2023*, LNCS, to appear.

[C.77] Ashrujit Ghoshal and Stefano Tessaro. **The Query-Complexity of Preprocessing Attacks.** In *Advanced in Cryptology — CRYPTO 2023*, LNCS, to appear.

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.

[J.2] Justin Chan, Landon P. Cox, Dean P. Foster, Shyam Gollakota, Eric Horvitz, Joseph Jaeger, Sham M. Kakade, Tadayoshi Kohno, John Langford, Jonathan Larson, Puneet Sharma, Sudheesh Singanamalla, Jacob E. Sunshine, and Stefano Tessaro. **PACT: Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing.** In *IEEE Data Eng. Bull.*, vol. 43, number 2, pp. 15–35, 2020.

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)

[S.4] Cetin Sahin, Aaron Magat, Victor Zakhary, Amr El Abbadi, Huijia Lin, Stefano Tessaro. **Understanding the Security Challenges of Oblivious Cloud Storage with Asynchronous Accesses**. ICDE 2017. Demo paper.

[S.5] Victor Zakhary, Cetin Sahin, Amr El Abbadi, Huijia Lin, Stefano Tessaro. **Pharos: Privacy Hazards of Replicating ORAM Stores.** EDBT 2018. Demo paper. **Best Demonstration Award.**

Reports

[R.1] R. L. Rivest, M.C. Schiefelbein, M.A. Zissman, J. Bay, E. Bugnion, J. Finnerty, I. Liccardi, B. Nelson, A.S. Norige, E.H. Shen, J. Wanger, R. Yahalom, J.D. Alekseyev, C. Brubaker, L. Ferretti, C. Ishikawa, M. Raykova, B. Schlaman, R.X. Schwartz, E. Sudduth, and S. Tessaro. **Automated Exposure Notification for COVID-19.** Lincoln Labs and MIT Technical report.

Volumes

[V.1] Stefano Tessaro. **2nd Conference on Information-Theoretic Cryptography.** LIPIcs 199, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

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

- ◇ Gareatis Foundation, Gift, $17,500 (joint with Huijia Lin). *2014–15*
- ◇ 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*
- ◇ Hellman Foundation, Hellman fellowship, $21,500. *2015-16*
- ◇ NSF CNS-1553758 (CAREER), "The Theoretical Foundations of Symmetric Cryptography", $422,212.00 (sole PI). *2016–21*
- ◇ Alfred P. Sloan Foundation, Sloan fellowship, $60,000. *2017-19*
- ◇ NSF CNS-1719146, "Memory-hard Cryptography", $499,758.00 (sole PI). *2017–20*
- ◇ NSF CNS-2026774, "A Concrete Look at Advanced Cryptography", $1,200,000 (PI; co-PI: Huijia Lin). *2020–24*
- ◇ JP Morgan Faculty Research Award, $150,000 (joint with Huijia Lin). *2020-22*

- ◇ CISCO Research Award, $200,000 (co-PI, joint with Huijia Lin). *2022*
- ◇ Microsoft Research Award, $90,000 *2022*
- ◇ NSF CNS-2154174, "Theoretical Foundations of Block Ciphers" (PI, joint with Vinod Vaikuntanathan (MIT)). Total: $1,200,000 (My share: $600k) *2022-26*.

Visits

- ◇ Simons Institute, University of California, Berkeley. Summer program on Cryptography. Visiting scientist. *6-8/2015*.
- ◇ Simons Institute, University of California, Berkeley. Program on Lattices. Visiting scientist *2-3/2020*
- ◇ NTT Research, Sunnyvale, CA. Visiting Scientist. *7-8/2021*
- ◇ Simons Insititute, University of California, Berkeley. Summer Cluster: Lattices and Beyond. Visiting Scientist. *6/2022*

Service

- ◇ **Editorship.** Associate editor for the Journal of Cryptology. *2018 – present.*
- ◇ **Steering committee member.** Conference on Information-Theoretic Cryptography (ITC). *2019 – present.*
- ◇ **Program chair.** Conference on Information-Theoretic Cryptography (ITC). *2021*
- ◇ **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, ICITS 2017, TCC 2017, IEEE S&P 2018, EUROCRYPT 2019, ITC 2020, SODA 2021, ITC 2021 (chair), IEEE S&P 2022, TCC 2022, USENIX Security 2023, TCC 2023.
- ◇ Reviewer for several journals, including *Journal of Cryptology*, *SIAM Journal on Computing (SICOMP)*, *IEEE Transactions on Information Theory*, ...
- ◇ Organizer of SPOTNIQ – Summer School of on Symmetric Proof Techniques (Bertinoro, Italy), July-August 2018.
- ◇ Local organizing committee member of TCC 2010.
- ◇ Reviewer and panelist for the National Science Foundation (NSF).
- ◇ External reviewer for other funding agencies, e.g., Israel Science Foundation, CHIST-ERA, NWO, DFG.
- ◇ **Internal service at UW.**
  - · Undergraduate admission committee 2019/20
  - · Graduate admission committee 2020/21
  - · Graduate admission committee (co-chair) 2021-23
- ◇ **Internal service at UC Santa Barbara.** Faculty Recruitment Committee, Graduate Admission Committee, Coordinator for Computer Science Distinguished Lectures, Faculty Executive Committee, College of Engineering.

Talks

Selected Invited Talks

◇ **Pairing-free Blind Signatures with Exponential Security.**
National Institute of Standards and Technology *01/2023*

◇ **The t-wise Indepenedence of Substitution-Permutation Networks**
NTT Upgrade 2021 Event *9/2021*

◇ **Exposure Notification: Barriers, Challenges, and a few Lessons Learned**
The Web of Health track at WWW 2021 (Distinguished invited speaker) *4/2021*
Web Seminar on Contact Tracing, TU Darmstadt *12/2020*
Distributed Systems Seminar, UC Santa Barbara *11/2020*
UW Engineering Lecture *10/2020*

◇ **Space-Time Trade-offs in Symmetric Cryptography**
Dagstuhl Seminar on Symmetric Cryptography. 1/2020
Bertinoro Workshop on Lower Bounds in Cryptography. Bertinoro, Italy. *7/2019*

◇ **Recent Developments in Format-Preserving Encryption**
ICERM Workshop on Encrypted Search, Brown University, Providence, RI *6/2019*

◇ **NTT 2018 Distinguished Cryptographer Lecture Series**
NTT Labs, Musashino, Japan *12/2018*

◇ **A tutorial on information-theoretic Indistinguishability**
CROSSING/IACR Spring School on
Combinatorial Techniques in Cryptography, Malta *4/2022*
SPOTNIQ Summer School, Bertinoro, Italy. *8/2018*

◇ **Foundations of Applied Cryptography**
crypt@bit summer school, University of Bonn (one week of lectures) *7/2018*

◇ **The Chi-Squared Method**
Dagstuhl Seminar on Symmetric Cryptography *1/2018*

◇ **Information-theoretic indistinguishability:**
new techniques and applications
Ecole Normale Superieure, Paris, France. *5/2017*
Workshops on Mathematics of Information-theoretic
Cryptography **(Keynote)**, Singapore. *9/2016*
International Conference on Information-Theoretic
Security (ICITS 2016) **(Keynote)**, Tacoma, Washington. *8/2016*

◇ **The memory hardness of Scrypt**
Early Symmetric Cryptography Workshop, Luxembourg. *1/2017*
Real-World Cryptography 2017 **(Invited Talk)**, New York, NY. *1/2017*
Simons Reunion Workshop, Simons Institute, Berkeley, CA. *8/2016*

◇ **Provably-robust Sponge-based PRNGs**
wr0ng – Random Number Generation Done Right, Paris, France. *5/2017*

◇ **Public-seed Pseudorandom Permutations**
Workshop on Complexity of Cryptography Primitives
and Assumptions, New York, NY. *6/2017*

◇ **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**
  Workshop on Communication Security **(Keynote)**, Paris, France. *5/2017*
  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*
- **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

- CRYPTO 2019, CCS 2018, CRYPTO 2017, CCS 2016, 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 **outreach talks** on cryptography for general audience and for prospective computer science students, at the University of Washington, at UCSB (as part of the MESA days), and at ETH Zurich.

Teaching

◇ **University of Washington**.

- CSE 526 — Cryptography (Graduate) *Sp2020, Sp2023*
- CSE 490C – Cryptography (Undergraduate) *Au 2021*
- CSE 599 – Advanced Cryptography (Graduate) *Wi 2021, Au 2022*
- CSE 312 — Foundations of Computing II *Au2019, Sp 2022*
- CSE 590P — Applied Cryptography *Sp2019, Au2020*

◇ **University of California, Santa Barbara**.

- CS290G — Introduction to Modern Cryptography (Graduate) *W2014, W2016, W2018*
- CS138 — Formal Languages and Automata *F2014, F2015, Sp2018*
- CS290G — Research Topics in Cryptography (Graduate) *W2015, W2017*
- CS177 — Computer Security *Sp2015, Sp2016, F2016, F2017, F2018*

◇ **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**

- Marshall Ball (2021, PhD Columbia, CI Fellow; joint with Huijia Lin; Now Assistant Professor at NYU)
- Joseph Jaeger (2019-2021, PhD UCSD; Now Assistant Professor at Georgia Tech)
- Aishwarya Thiruvengadam (2017-18, PhD UMD; Now Assistant Professor at IIT Madras)
- Viet Tung Hoang (2015-16 PhD UC Davis; Now tenured Associate Professor at Florida State University)

◇ **Graduate students (Current)**

- Ashrujit Ghoshal (PhD)
- Chenzhi Zhu (PhD)
- Ji Luo (PhD)
- Hanjun Li (PhD)
- Champ Chairattana-Apirom (PhD)
- Marian Dietz (PhD)
- Yao-Ching Hsieh (PhD)

◇ **Graduate students (Graduated)**

- Xihu Zhang (MS UW 2022; now at Oracle)
- Pratik Soni (PhD UCSB 2020; now postdoc at CMU; Assistant Professor at University of Utah starting Fall 2023)
- Daniel Agun (PhD UCSB, 2020)

- Binyi Chen (PhD UCSB 2019; now at Espresso Systems)
- Wei Dai (MS UCSB 2016; now Research Partner at Bain Capital Crypto)
- John Retterer-Moore (MS 2015).
- David Wilson (at MIT, informally co-advised with Shafi Goldwasser, graduated: Summer 2014, now at Lincoln Labs).