CURRICULUM VITAE

Ran Canetti

September 26, 2021

Address:

Department of computer Science, Boston University
111 Cummington St.,
Boston, MA 02215
Email: *canetti@bu.edu*

Education:

Postdoctoral Training: Lab of Computer Science, MIT, 1995-6. Supervisor: Prof. Shafi Goldwasser.

Ph.D.: The Weizmann Institute, Rehovot, Israel, 1995.
The thesis is entitled "Studies in Secure Multiparty Computation and Applications", under the supervision of Prof. Oded Goldreich.

M.Sc.: Technion, Haifa, Israel, 1991. The thesis is entitled "Tradeoffs between Randomness and Communication Complexity", under the supervision of Prof. Oded Goldreich.

B.A.: Technion, Haifa, Israel.
B.A. in Physics, *cum laude,* 1990.
B.A. in Computer Science, *cum laude,* 1989.

Positions Held:

Director for Research of the Center for Reliable Information Systems and Cyber Security (RISCS) at Boston University, since July 2013.

Professor, Department of Computer Science, Boston University, since 2011.

Director, The Check Point Institute for Information Security, 2008-2019.

Head of Scientific Comimittee, the Interdisciplinary Cybersecurity Research Center, Tel Aviv University, 2014-2019.

Professor, School of Computer Science, Tel Aviv University, 2014-2019.

Associate Professor, School of Computer Science, Tel Aviv University, 2008-2014.

Research Staff Member, Department of Network Security and Cryptography, IBM T.J. Watson Research Center, 1996-2008.

Visiting Scientist, Computer Science and Artificial Intelligence Laboratory, MIT, 2004-2008.

Research Interests:

Cryptography, network and system security, cybersecurity and law

Professional Activity:

Journal Editorship:

Editorial Board Member, Information and Computation, since 2007.

Associate Editor, Journal of Cryptology, since 2002.

Conference Program Committees:

Program Committee co-chair, Crypto, 2012 and 2013.

Program Committee Chair, TCC (Theoretical Cryptography Conference), 2008.

PC member for Crypto'00, PODC'01, Crypto'01, NDSS'03, FMCS'03, FOCS'03, TCC'04, FMCS'04, SCN'04, ACNS'05, CSFW'05, FOCS'05, DCC'06, CSFW'06, WATC'07, TCC'07, ICALP'07, STOC'09, FCC'09, Eurocrypt'10, POST14, ESORICS'15, Eurocrypt'16, Crypto 2017, TCC 2017, WWW 2019, Crypto 2019, FAT 2020, ACM-Law '20, CSF 2020, 2021, Crypto 2021.

Other activity:

Steering Comittee Member, Zero Knowledge Proofs Standards, since 2018.

General Chair, TCC 2016a.

Chair of the Crypto Forum Research Group (CFRG) of the Internet Research Task Force (IRTF). The mission of the group is to investigate and develop cryptographic mechanisms for use in Internet protocols. 2004-2011.

Chair of the Multicast Security (MSEC) Working Group of the Internet Engineering Task Force (IETF). The mission of the group is to develop a protocol-suite for securing multicast communication on the Internet. 2000-2008.

Organized (with Mayank Varia, Elaine Shi, and MAriana Raykova) the Crypto in the RAM Model Workshop, MIT, June 2016.

Organized (with Iftach Haitner, Benny Applebaum, Eran Tromer and Alon Rosen) The Crypto In The Desert Workshop, Sde Boker, Israel, January 2016.

Organized (with Shafi Goldwasser and Yael Kalai) the Charles River Crypto Day, December 2011 and 2012, at Boston University.

Organized (with Shafi Goldwasser) a workshop on verifiable computation, MIT, August 2010.

Organized (with Alon Rosen and Ronitt Rubinfeld) a workshop on electronic voting and its social and legal aspects. Tel Aviv University and IDC Herzeliyya, May 2009.

Organized (with Shafi Goldwasser) a workshop on cryptography for cloud computing, MIT, August 2009.

Organized (with Shafi Goldwasser, Gunter Muller and Rainer Steinwandt) a workshop on the theoretical foundations of practical information security, Schloss Dagstuhl, Germany, December 2008.

Organized (with J. Preskill and D. Mayers from Caltech) a workshop on Security of Quantum and Classical Protocols, Caltech, December 2005.

Organized (with J. Mitchell from Stanford) a workshop on Security Analysis of Cryptographic Protocols, DIMACS, June 2004.

Organized (with U. Maurer from ETH and R. Ostrovsky from UCLA) a workshop on Cryptographic Protocols in Complex Environments, DIMACS, May 2002.

Plenary and invited talks at: ICALP 2008, Asiacrypt 2007, Usenix Security 2007, PODC 2004, FMCS 2004, SPC/CONCUR 2003, PODSY 2003.

Current students:

Patik Sarkar (PhD. Expected graduation: 2023)

Ari Karchmer (PhD. Expected graduation: 2023)

Luowen Qian (PhD. Expected graduation: 2024)

Shlomi Hod (PhD. Expected graduation: 2025)

Megan Chen (PhD. Expected graduation: 2025)

Past students:

Rita Vald (PhD, Tel Aviv university. Graduated: 2020. Researcher at Intuit Research)

Oxana Poburinnaya (PhD, Boston University. Graduated: 2019. Currently at the Simons Institute.)

Yilei Chen (PhD, Boston University. Grauated: 2018. Faculty at Tsinghua University.)

Amit Lichtenberg (MSc, Tel Aviv University. Graduated: 2018.)

Omer Paneth (PhD, Boston University. Graduated: Spetember 2016. Faculty at Tel Aviv U.)

Saleet Klein (MSc, Tel Aviv University. Graduated: June 2016. Currently PhD student at MIT.)

Nir Bitansky (PhD, Tel Aviv University, graduated 2014. Faculty at Tel Aviv U.)

Ben Riva (PhD, Tel Aviv University, graduated 2013. Chief Scientist, Curv Inc.)

Margarita Vald (Msc, Tel Aviv University, graduated 2012)

Omer Paneth (Msc, Tel Aviv University, graduated 2011)

Itay Itzhaki (Msc, Tel Aviv University, graduated 2011)

Mayank Varia (PhD, MIT, graduated 2010. Currently at BU.)

Nir Bitansky (MSc, Tel Aviv University, graduated 2010)

Ronny Dakdouk (PhD, Yale, graduated 2009. Co-advised with Joan Feigenbaum. Currently at Google.)

Dah-Yoh Lim (PhD, MIT, graduated 2008. Co-advised with Shafi Goldwasser. Currently at Amazon.)

Waseem Daher (M.Eng, MIT, graduated 2008. Co-advised with Ron Rivest. Currently at Google.)

Akshay Patil (M.Eng, MIT, graduated 2005. Co-advised with Ron Rivest. Currently at Google.)

Served on the Ph.D. committees of Benjamin Reed (UC Santa Cruz, 2000), Stefan Dziembowski (U. of Arhus, Denmark, 2001), Alon Rosen (Weizmann Inst., 2003), Jesper Nielsen (U. of Arhus, Denmark, 2003), Jesus Almensa (U. Arhus, 2005), Susan Hoenberger (MIT, 2006), Matt Lepinski (MIT, 2006), Shabsi Walfish (NYU, 2007), Zuzana Beerliova (ETH, 2008), Mikkel Kroigard (Arhus, 2010), Claudio Orlandi (Arhus, 2011), Antigoni Polychroniadou (Arhus, 2017)

Post-doctoral advisees:

Gabriel Kapthuk (PhD. Johns Hopkins, Since 2020.)

Nick Spooner (PhD. UC Berkeley, since 2020.)

Eylon Yogev (PhD Weizmann, since 2020. Joint with TAU.)

Aloni Cohen (PhD MIT, since 2019, joint with BU Law School.)

Xiao Wong (PhD UMD, 2018-2019. Currenctly faculty at U. Illinois.)

Ran Cohen (PhD BIU, 2018-2019. Currenctly at NEU.)

Silas Richelson (PhD UCLA, 2015-2017. Currenctly faculty at UCR.)

Alessandra Scafuro (PhD U. Salerno, 2015-2017. Currently faculty at UNC.)

Abhishek Jain (PhD UCLA, 2012-2014, currently faculty at Johns Hopkins)

Rachel Huijia Lin (PhD Cornell, 2011-2013, currently faculty at UCSB)

Adam O'neill (PhD GeorgiaTech, 2011-2013, currently faculty at UMass Amherst)

Noam Livne (PhD Weizmann, 2010-11)

Sebastian Gajek (PhD Bochum, 2009-2011)

Honors and Prizes:

Fellow of the Association of Computing Machinery (ACM), Class of 2020.

IEEE Security and Privacy Conference Test of Time Award May 2020. given for [C28].

RSA Conference Award in Mathematics. 2018.

Fellow of the International Association for Cryptologic Research (IACR), 2014.

IBM Research Outstanding Innovation Award, 2006. Given for work on sound foundations for modern cryptography.

IBM Corporate Award, 2005. Given for the continued impact of the HMAC algorithm [S1].

IBM Research Best Paper Award, 2004. Given for [J14].

IBM Research Outstanding Innovation Award, 2004.

IBM Research Best Paper Award, 2001. Given for [C34].

IBM Research Division Award, 1999. Given for contribution to the IPSEC standard.

IBM Innovation Award, 1997. Given for the design of the HMAC message authentication function.

The Kennedy Thesis Award, The Weizmann Institute, 1996.

The Rothschild post-doctoral scholarship, 1995-6.

The Gutwirth Special Excellence Fellowship, the Technion, 1992-

Research Funding:

"Optimized Relations Auditing for Compliance with Laws and Ethical Statements (ORACLES)," $4M, DARPA SIEVE (with Bestavros, Cohen, Goldwasser, Reyzin, Varia), 2020-2024.

"Verifying Computations Securely and Robustly in Post-Quantum Era," $4M, DARPA SIEVE (with Goldwasser, Kalai, Reyzin, Vaikuntanathan, Vidick), 2020-2024.

"InTrans: Modular Security on an Open Cloud,", NSF SaTC, $500K, (with Bestavros, Varia), 2019-2021.

"ACHILLES: Assured CryptograpHic Integration of muLtiple Languages for Encrypted Systems," IARPA, $3.2M (with 11 PIs), 2019-2024.

“ Towards Mechanized Proofs of Composable Security Properties”, NSF SaTC, $1.2M (with Kfouri, Stoughton, Varia.) 2018-2022.

“New directions in succinct proofs, knowledge extraction, and software obfuscation”, ISF, 815K ILS, 2014-2019.

“Frontier: A Modular Approach to Cloud Security”, NSF SATC, 2014-2019, $10M (lead PI for 13 PIs).

“EAGER: Holistic security for cloud computing: Verifiable Computation and Databases”, NSF SATC grant, 2013-15, $300K.

“New Directions in Cryptography: Non-Black-Box Techniques against Non-Black-Box Attacks”, NSF Algorithmic Foundations grant 1218461, $480K, 2012-2015.

“Cryptographic program obfuscation and applications”, ISF, 840K ILS, 2009-2013.

“New Directions in Program Obfuscation”, European Union Marie Curie Grant, 80K Euro, 2008-2012.

“Composition of Cryptographic Protocols”, US-Israel Binational Science Foundation Grant 2006317, with R. Pass (Cornell) and A. Rosen (Inderdisciplinary College, Tel Aviv). $106K, 2007-2011.

“Program Obfuscation: Foundations and Applications”, NSF Grant CFF-0635297, With S. Goldwasser, MIT and Yael Kalai, Georgia Tech. $330K, 2006-2009.

“Cryptographic Foundations of CyberTrust”, NSF CyberTrust Grant 0430450, With S. Goldwasser, MIT. $450K, 2004-2007.

Patents:

[P5] D. Papadopoulos, N. Triandopoulos, R. Canetti. Authenticated hierarchical set operations and applications. US patent number 9049185, 2015.

[P4] R Canetti, S. Halevi, M. Steiner. Mitigating Dictionary Attacks on Password-Based Local Storage. US patent number 8108683, 2012.

[P3] R. Canetti, M. Charikar, R. Kumar, S. Rajagopalan, A. Sahai, A. Tomkins. Non-transferable Anonymous Credentials. U.S. Patent No. 7,222,362, May 2007.

[P2] R. Canetti and A. Herzberg, A Mechanism for Keeping a Key Secret from Mobile Eavesdroppers. US patent No. 5,412,723, May 1995.

[P1] R. Canetti and A. Herzberg, Secure Communication and Computation in an Insecure Environment. US patent No. 5,469,507, November 1995.

Standards:

[S3] M. Baugher, R. Canetti, L. Dondeti, F. Lindholm, “Group Key management Architecture,” Internet Engineering Task Force RFC 4046, 2005.

[S2] A. Perrig, R. Canetti, B. Briscoe, D. Tygar, D. Song, “TESLA: Multicast Source Authentication Transform”, Internet Engineering Task Force RFC 4082, 2005.

[S1] H. Krawczyk, M. Bellare and R. Canetti, “HMAC: Keyed-Hashing for Message Authentication”, Internet Engineering Task Force RFC 2104, February 1997. Also appears as an American National Standard Institute (ANSI) standard X9.71 (2000), and as a Federal Information Processing Standard No. 198, National Institute of Standards and Technology (NIST), 2002.

Publications:

Books and Book Chapters:

[B6] Ran Canetti, Juan A. Garay (Eds.): Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Proceedings. Lecture Notes in Computer Science 8042 amd 8043, Springer.

[B5] Security and Composition of Cryptographic Protocols. Chapter in *Secure Multiparty Computation,* Ed. Manoj Prabhakaran and Amit Sahai. Cryptology and Information Security Series, IOS Press, 2013.

[B4] Reihaneh Safavi-Naini, Ran Canetti (Eds.): Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference,. Proceedings. Lecture Notes in Computer Science 7417, Springer.

[B3] Ran Canetti (Ed.): Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008. Lecture Notes in Computer Science 4948, Springer.

[B2] Journal of Cryptology Special Issue on Byzantine Agreement. R. Canetti, (Ed.) Vol. 18, No. 3, 2005.

[B1] Chapter on the Decisional Diffie-Hellman assumption. Encyclopedia of Cryptography and Security, H. van Tilborg, Henk (Ed.), Springer-Verlag, 2005.

PhD Thesis:

"Studies in Secure Multiparty Computation and Applications," 1996.
Available on-line at http://philby.ucsd.edu/cryptolib/BOOKS/ran-phd.html

Publications in refereed journals:

[J33] Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, Adam D. Smith. Reusable Fuzzy Extractors for Low-Entropy Distributions. J. Cryptol. 34(1): 2 (2021)

[J32] Ran Canetti. Universally Composable Security. Journal of the ACM (JACM) 67 (5), 1-94 (2020)

[J31] Nir Bitansky, Ran Canetti, Sanjam Garg, Justin Holmgren, Abhishek Jain, Huijia Lin, Rafael Pass, Sidharth Telang, Vinod Vaikuntanathan. Indistinguishability Obfuscation for RAM Programs and Succinct Randomized Encodings. SIAM J. Comput. 47(3): 1123-1210 (2018)

[J30] Ran Canetti, Ling Cheung, Dilsun Kirli Kaynar, Moses Liskov, Nancy A. Lynch, Olivier Pereira, Roberto Segala. Task-structured probabilistic I/O automata. J. Comput. Syst. Sci. 94: 63-97 (2018)

[J29] Nir Bitansky, Ran Canetti, Yael Tauman Kalai, Omer Paneth. On Virtual Grey Box Obfuscation for General Circuits. Algorithmica 79(4): 1014-1051 (2017)

[J28] Nir Bitansky, Ran Canetti, Alessandro Chiesa, Shafi Goldwasser, Huijia Lin, Aviad Rubinstein, Eran Tromer: The Hunting of the SNARK. J. Cryptology 30(4): 989-1066 (2017)

[J27] Ran Canetti, Huijia Lin, Rafael Pass. Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions. SIAM J. Comput. 45(5): 1793-1834 (2016)

[J26] Nir Bitansky, Ran Canetti, Omer Paneth, Alon Rosen. On the Existence of Extractable One-Way Functions. SIAM J. Comput. 45(5): 1910-1952 (2016)

[J25] G. Asharov, R. Canetti, C. Hazay. Towards a Game Theoretic View of Secure Computation. J. Cryptology 29(4): 879-926 (2016)

[J24] N. Bitansky, R. Canetti. On Strong Simulation and Composable Point Obfuscation. J. Cryptology 27(2): 317-357 (2014)

[J23] R, Canetti, B. Riva, G. N. Rothblum. Refereed Delegation of Computation. Information and Computation 226: 16-36 (2013).

[J22] R. Canetti, J. Herzog. Universally Composable Symbolic Analysis of Mutual Authentication and Key-Exchange Protocols. J. Cryptology 24(1): 83-147 (2011)

[J21] B. Barak, R. Canetti, Y. Lindell, R. Pass, and T. Rabin. Secure Computation without Authentication. J. Cryptology 24(4): 720-760 (2011)

[J20] Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, Roberto Segala. Analyzing Security Protocols Using Time-Bounded Task-PIOAs. Discrete Event Dynamic Systems, Vol. 18, No.1 (2008).

[J19] D. Boneh, R. Canetti, S. Halevi, and J. Katz, “Chosen-Ciphertext Security from Identity-Based Encryption,” SIAM J. Comput. 36(5): 1301-1328 (2007)

[J18] R. Canetti, S. Halevi, and J. Katz, “Forward-Secure Encryption,” J. Cryptology 20(3): 265-294 (2007)

[J17] R. Canetti, E. Kushilevitz and Y. Lindell, “On the Limitations of Universally Composable Two-Party Computation Without Set-up Assumptions,” J. Cryptology 19(2): 135-167 (2006).

[J16] Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Using Probabilistic I/O Automata to Improve the Analysis of Cryptographic Protocols. In ERCIM News, 63: 40-41, October 2005

[J15] B. Aiello, S. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. Keromytis, O. Reingold, “Just Fast Keying: Key Agreement In A Hostile Internet”, ACM Trans. Inf. Syst. Secur. 7(2): 242-273 (2004).

[J14] R. Canetti, O. Goldreich, and S. Halevi “The Random-Oracle Model, Revisited”, J. ACM 51(4): 557-594 (2004).

[J13] R. Canetti, I. Damgård, S. Dziembowski, Y. Ishai, T. Malkin, “On Adaptive vs. Non-adaptive Security of Multiparty Protocols,” J. Cryptology 17(3): 153-207 (2004).

[J12] R. Canetti, J. Kilian, E. Petrank, A. Rosen,“Black-Box Concurrent Zero-Knowledge Requires $\tilde{\Omega}(\log n)$ Rounds”, SIAM J. Comput. 32(1): 1-47 (2002).

[J11] R. Canetti, “Security and composition of multi-party cryptographic protocols”, Journal of Cryptology Special Issue on Multiparty Computation 13(1): 143-202 (2000).

[J10] R. Canetti, S. Halevi and A. Herzberg, “Maintaining Authenticated Communication”, Journal of Cryptology Special Issue on Multiparty Computation 13(1): 61-105 (2000).

[J9] R. Canetti, E. Kushilevitz, R. Ostrovsky and A. Rosen, “Randomness vs. Fault-Tolerance”, Journal of Cryptology Special Issue on Multiparty Computation 13(1): 107-142 (2000).

[J8] R. Canetti, J. B. Friedlander, S. V. Konyagin, M. Larsen, D. Lieman, I. Shparlinski, “On the statistical properties of Diffie-Hellman distributions”, Israel J. Math., 2000, v.120, 23-46.

[J7] R. Canetti, J. Friedlander and I. Shparlinski, “On certain exponential sums and the distribution of Diffie-Hellman triples”, *J. of the London Mathematical Society,* (2) 59 (1999) 799–812.

[J6] A. Bar-Noy, R. Canetti, S. Kutten, Y. Mansour, and B. Schieber, “Bandwidth Allocation with Preemption”, *SIAM Journal on Computing*, Vol. 28, 1999, pp. 1806-1828.

[J5] R. Canetti and S. Irani, “On the Power of Preemption in Randomized Scheduling”, *SIAM Journal on Computing,* Vol. 27 No. 4, 1998, pp. 993-1015.

[J4] R. Canetti, “On BPP and the Polynomial-Time Hierarchy”, *IPL 57,* 1996, pp. 237-241.

[J3] R. Canetti, G. Even and O. Goldreich, “Lower bounds for Sampling Algorithms for Estimating the Average”, *IPL 53,* 1995, pp. 17-25.

[J2] R. Canetti and O. Goldreich, “Bounds on Tradeoffs between Randomness and Communication Complexity”, *computational complexity* **3**, 1993, pp.141-167.

[J1] R. Canetti, P. Fertig, S. Kravitz, D. Malkhi, R. Pinter, S. Porat, A. Teperman, “The Parallel C (pC) Programming Language”, *IBM Journal of Research and Development, Vol 35, no. 5/6,* November 1991, pp. 727-742.

Publications in refereed conferences:

[C 127] Ran Canetti, Ari Karchmer. Covert Learning: How to Learn with an Untrusted Intermediary. Theory of Cryptography (TCC), 2021.

[C126] Ran Canetti, Rosario Gennaro, Steven Goldfeder, Nikolaos Makriyannis, Udi Peled. UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts. CCS 2020: 1769-1787

[C125] Christian Badertscher, Ran Canetti, Julia Hesse, Bjoern Tackmann, Vassilis Zikas. Universal Composition with Global Subroutines: Capturing Global Setup within plain UC. Theory of Cryptography (TCC), 2020.

[C124] Ran Canetti, Oxana Poburinnaya. Towards Multiparty Computation Withstanding Coercion of All Parties. Theory of Cryptography (TCC), 2020.

[C123] Ran Canetti, Pratik Sarkar, Xiao Wang. Efficient and Round-Optimal Oblivious Transfer and Commitment with Adaptive Security. AsiaCrypt 2020.

[C122] Ran Canetti, Sunoo Park, Oxana Poburinnaya: Fully Deniable Interactive Encryption. CRYPTO (1) 2020: 807-835

[C121] Foteini Baldimtsi, Ran Canetti, Sophia Yakoubov: Universally Composable Accumulators. CT-RSA 2020: 638-666

[C120] Ran Canetti, Marten van Dijk, Hoda Maleki, Ulrich Rhrmair, Patrick Schaumont: Using Universal Composition to Design and Analyze Secure Complex Hardware Systems. DATE 2020: 520-525

[C119] Ran Canetti, Pratik Sarkar, Xiao Wang: Blazing Fast OT for Three-Round UC OT Extension. Public Key Cryptography (2) 2020: 299-327

[C118] Kyle Hogan, Hoda Maleki, Reza Rahaeimehr, Ran Canetti, Marten van Dijk, Jason Hennessey, Mayank Varia, Haibin Zhang. On the Universally Composable Security of OpenStack. IEEE SecDev 2019.

[C117] Ran Canetti, Alley Stoughton, Mayank Varia. EasyUC: Using EasyCrypt to Mechanize Proofs of Universally Composable Security. CSF 2019: 167-183

[C116] Ran Canetti, Yilei Chen, Justin Holmgren, Alex Lombardi, Guy N. Rothblum, Ron D. Rothblum, Daniel Wichs. Fiat-Shamir: from practice to theory. STOC 2019: 1082-1090

[C115] Ran Canetti, Aloni Cohen, Nishanth Dikkala, Govind Ramnarayan, Sarah Scheffler, Adam D. Smith. From Soft Classifiers to Hard Decisions: How fair can we be? FAT 2019: 309-318

[C114] Ran Canetti, Amit Lichtenberg. Certifying Trapdoor Permutations, Revisited. TCC (1) 2018: 476-506

[C113] Ran Canetti, Yilei Chen, Leonid Reyzin, Ron D. Rothblum: Fiat-Shamir and Correlation Intractability from Strong KDM-Secure Encryption. EUROCRYPT (1) 2018: 91-122

[C112] Ran Canetti, Oxana Poburinnaya, Mariana Raykova: Optimal-Rate Non-Committing Encryption. ASIACRYPT (3) 2017: 212-241

[C111] Ran Canetti, Kyle Hogan, Aanchal Malhotra, Mayank Varia: A Universally Composable Treatment of Network Time. CSF 2017: 360-375

[C110] Ran Canetti, Yilei Chen: Constraint-Hiding Constrained PRFs for NC1 from LWE. EUROCRYPT (1) 2017: 446-476

[C109] Ran Canetti, Justin Holmgren, Silas Richelson: Towards Doubly Efficient Private Information Retrieval. TCC (2) 2017: 694-726

[C108] Ran Canetti, Oxana Poburinnaya, Muthuramakrishnan Venkitasubramaniam: Equivocating Yao: Constant-Round Adaptively Secure Multiparty Computation in the Plain Model. STOC 2017.

[C107] Ran Canetti, Srinivasan Raghuraman, Silas Richelson, Vinod Vaikuntanathan: Chosen-Ciphertext Secure Fully Homomorphic Encryption. PKC (2) 2017: 213-240

[C106] Ran Canetti, Oxana Poburinnaya, Muthuramakrishnan Venkitasubramaniam: Better Two-Round Adaptive Multi-party Computation. PKC (2) 2017: 396-427

[C105] Ran Canetti, Yilei Chen, Justin Holmgren, Mariana Raykova: Adaptive Succinct Garbled RAM or: How to Delegate Your Database. TCC (B2) 2016: 61-90

[C104] Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, Key Derivation From Noisy Sources With More Errors Than Entropy. Eurocrypt 2016.

[C103] Ran Canetti, Justin Holmgren, Fully Succinct Garbled RAM. ITCS 2016: 169-178

[C102] Ran Canetti, Daniel Shahaf, Margarita Vald, Universally Composable Authentication and Key-Exchange with Global PKI. Public Key Cryptography (2) 2016: 265-296

[C101] Ran Canetti, Yilei Chen, Leonid Reyzin, On the Correlation Intractability of Obfuscated Pseudorandom Functions. TCC (A1) 2016: 389-415

[C100] R. Canetti, A. Cohen, Y. Lindell. A Simpler Variant of Universally Composable Security for Standard Multiparty Computation. CRYPTO (2) 2015: 3-22.

[C99] R. Canetti, V. Goyal, A. Jain. Concurrent Secure Computation with Optimal Query Complexity. CRYPTO (2) 2015: 43-62

[C98] C. Mavroforakis, N. Chenette, A. O'Neill, G. Kollios, Ran Canetti. Modular Order-Preserving Encryption, Revisited. SIGMOD Conference 2015: 763-777

[C97] Ran Canetti, Justin Holmgren, Abhishek Jain, Vinod Vaikuntanathan: Indistinguishability Obfuscation of Iterated Circuits and RAM Programs. STOC 2015.

[C96] Ran Canetti, Shafi Goldwasser, Oxana Poburinnaya: Adaptively Secure Two-party Computation From Indistinguishability Obfuscation. TCC 2015.

[C95] Ran Canetti, Huijia Lin, Stefano Tessaro, Vinod Vaikuntanathan: Obfuscation of Probabilistic Circuits and Applications. TCC 2015.

[C94] Ran Canetti, Yael Tauman Kalai, Omer Paneth: On the possibility of virtual black box obfuscation in the random oracle model. TCC 2015.

[C93] Ran Canetti, Abhishek Jain, Alessandra Scafuro: Practical UC security with a Global Random Oracle. ACM Conference on Computer and Communications Security 2014: 597-608

[C92]Nir Bitansky, Ran Canetti, Henry Cohn, Shafi Goldwasser, Yael Tauman Kalai, Omer Paneth, Alon Rosen: The Impossibility of Obfuscation with Auxiliary Input or a Universal Simulator. CRYPTO (2) 2014: 71-89

[C91] Nir Bitansky, Ran Canetti, Yael Tauman Kalai, Omer Paneth: On Virtual Grey Box Obfuscation for General Circuits. CRYPTO (2) 2014: 108-125

[C90] Ran Canetti, Abhishek Jain, Omer Paneth: Client-Server Concurrent Zero Knowledge with Constant Rounds and Guaranteed Complexity. CRYPTO (2) 2014: 337-350

[C89] Ran Canetti, Vladimir Kolesnikov, Charles Rackoff, Yevgeniy Vahlis: Secure Key Exchange and Sessions without Credentials. SCN 2014: 40-56

[C88] N. Bitansky, R. Canetti, O. Paneth, A. Rosen. On the existence of extractable one-way functions. STOC 2014.

[C87] R. Canetti, O. Paneth, D. Papadopoulos, N. Triandopoulos. Verifiable Set Operations over Outsourced Databases. PKC 2014.

[C86] B. Barak, N. Bitansky, R. Canetti, Y. Kalai, O. Paneth, A. Sahai. Obfuscation for Evasive Functions. TCC 2014.

[C85] R. Canetti, H. Lin, R. Pass. From Unprovability to Environmental Friendliness, FOCS 2013.

[C84] N. Bitansky, R. Canetti, A. Chiesa, E. Tromer. Recursive Composition and Bootstrapping for SNARKs and Proof-Carrying Data. STOC 2013.

[C83] R, Canetti, H.Lin, O. Paneth. Public Coin Concurrent Zero-Knowledge in the Global Hash Model. TCC 2013.

[C82] R. Canetti, M. Vald. Universally Composable Security with Local Adversaries. SCN 2012: 281-301

[C81] R. Canetti, B. Riva, G. N. Rothblum. Two Protocols for Delegation of Computation. ICITS 2012: 37-61

[C80] R. Canetti, D. Dachman-Soled, V. Vaikuntanathan, and H. Wee. Efficient Password Authenticated Key Exchange via Oblivious Transfer. PKC (Public Key Cryptography) Conference, 2012.

[C79] N. Bitansky, R. Canetti, S. Halevi. Leakage Tolerant Protocols. Theory of Crypology Conference (TCC), 2012.

[C78] N. Bitansky, R. Canetti, A. Chiesa, E. Tromer. From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again. Innovations in Theoretical Computer Science, 2012.

[C77] N. Bitansky, R. Canetti, S. Goldwasser, S. Halevi, Y. Tauman Kalai, G N. Rothblum. Program Obfuscation with Leaky Hardware. ASIACRYPT 2011.

[C76] R. Canetti, B. Riva, G. N. Rothblum. Practical delegation of computation using multiple servers. ACM Conference on Computer and Communications Security (CCS) 2011.

[C75] G. Asharov, R. Canetti, C. Hazay. Towards a Game Theoretic View of Secure Computation. Eurocrypt 2011.

[C74] R. Canetti, S. Chari, S. Halevi, B. Pfitzmann, A. Roy, M. Steiner and W. Venema. Composable Security Analysis of OS Services. ACNS, 2011.

[C73] R. Canetti, H. Lin, R. Pass. Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions, FOCS 2010.

[C72] N. Bitansky, R. Canetti. On Strong Simulation and Composable Point Obfuscation. CRYPTO, 2010.

[C71] R. Canetti, G. Rothblum, M. Varia. Obfuscating Hyperplane Membership. Theory of Cryptograph Conference (TCC) 2010.

[C70] R. Canetti, Y. Kalai, M. Varia, D. Wichs. On Symmetric Encryption and Point Obfuscation. Theory of Cryptograph Conference (TCC) 2010.

[C69] R. Canetti, R. R. Dakdouk. Towards a Theory of Extractable Functions. TCC 2009: 595-613

[C68] R. Canetti, Mayank Varia. Non-malleable Obfuscation. TCC 2009: 73-90

[C67] W. Daher, R. Canetti: POSH: a generalized captcha with security applications. AISec 2008: 1-10

[C66] R. Canetti, Ling Cheung, Dilsun Kirli Kaynar, Nancy A. Lynch, Olivier Pereira: Modeling Computational Security in Long-Lived Systems. CONCUR 2008: 114-130

[C65] R. Canetti, R. R. Dakdouk: Obfuscating Point Functions with Multibit Output. EUROCRYPT 2008: 489-508

[C64] R. Canetti, R. R. Dakdouk. Extractable Perfectly One-Way Functions. ICALP (2) 2008: 449-460

[C63] R. Canetti, D. Eiger, S. Goldwasser, D.Y. Lim. How to Protect Yourself without Perfect Shredding. ICALP (2) 2008: 511-523

[C62] R. Canetti, L. Cheung, D. Kaynar, N. Lynch and O. Pereira. Compositional Security for Task-PIOAs. 20th Computer Security Foundations Conference (CSF), July 2007.

[C61] R. Canetti, S. Hohenberger. Chosen Ciphertext Secure Proxy Reencryption. ACM CCS (Computer and Communication Security) 2007.

[C60] R. Canetti, R. Pass, A. Shelat. Cryptography from sunspots: How to use an imperfect reference string. 48th Foundations of Computer Science (FOCS) 2007.

[C59] R. Canetti, R. Rivest, M. Sudan, L. Trevisan, S. Vadhan, H. Wee. Amplification of Collision Resistance: A complexity-theoretic treatment. Crypto 2007.

[C58] R. Canetti, Y. Dodis, R. Pass and S. Walfish. Universally Composable Security with Pre-Existing Setup. The fourth Theory of Cryptology Conference (TCC), 2007.

[C57] R. Canetti, L. Cheung, N. Lynch and O. Pereira. On the Role of Scheduling in Simulation-Based Security. The 7th Workshop on Issues in the Theory of Security (WITS), 2007.

[C56] R Canetti, S. halevi, M. Steiner. Mitigating Dictionary Attacks on Password-Based Local Storage. Crypto 2006.

[C55] R. Canetti, L. Cheung, D. Kaynar, M. Liskov, N. Lynch, O. Pereira, and R. Segala. Time-Bounded Task-PIOAs: A Framework for Analyzing Security Protocols. In 20th symposium on distributed computing (DISC), 2006. Long version at MIT-LCS-TR-1001, August 2005.

[C54] R. Canetti, L. Cheung, D. Kaynar, M. Liskov, N. Lynch, O. Pereira, and R. Segala. Task-Structured Probabilistic I/O Automata. In Workshop on discrete event systems (WODES), 2006.

[C53] R. Canetti, J. Herzog. Universally Composable Symbolic Analysis of Mutual Authentication and Key-Exchange Protocols. The Third Theory of Cryptograph Confernece (TCC), 2006: 380-403.

[C52] B. Barak, R. Canetti, Y. Lindell, R. Pass, and T. Rabin. Secure Computation without Authentication. Crypto 2005.

[C51] R. Canetti, S. Halevi, J. Katz, Y. Lindell, P. D. Mackenzie: Universally Composable Password-Based Key Exchange. EUROCRYPT 2005: 404-421.

[C50] R. Canetti, S. Halevi, M. Steiner, "Hardness Amplification For Computational Riddles", The second Theory of Cryptograph Confernece (TCC), 2005.

[C49] R. Canetti, S. Halevi and J, Katz, "Adaptively Secure Non-Interactive Public-Key Encryption", The second Theory of Cryptograph Confernece (TCC), 2005.

[C48] B. Barak, R. Canetti, J. Nielsen and R. Pass, " Universally Composable Protocols with Relaxed Set-Up Assumptions." *45th FOCS,* 2004.

[C47] R. Canetti, "Universally Composable Notions of Signature, Certification, and Authentication", *17th IEEE Computer Security Foundations Workshop (CSFW),* 2004.

[C46] R. Canetti, O. Goldreich, and S. Halevi, "On the random-oracle methodology as applied to length-restricted signature schemes," *The First Theory of Cryptography Conference (TCC),* 2004.

[C45] R. Canetti, S. Halevi, and J. Katz, "Chosen-Ciphertext Security from Identity-Based Encryption," *Eurocrypt '04,* 2004.

[C44] R. Canetti, H. Krawczyk, and J. Nielsen, "Relaxing Chosen Ciphertext Security of Encryption Schemes," *Crypto '03,* 2003.

[C43] R. Canetti and T. Rabin, "Universal Composition with Joint State," *Crypto '03,* 2003.

[C42] H. Schertzer, R, Canetti, P. Karger, T. Rabin, D. Toll, "Authenticating Mandatory Access Controls and Preserving Privacy for a High-Assurance Smart Card," *ESORICS 03,* 2003.

[C41] R. Canetti, E. Kushilevitz, and Y. Lindell, "On the limitations of universally composable two-party computation without set-up assumptions," *Eurocrypt '03,* 2003.

[C40] R. Canetti, S. Halevi and J. Katz, "Forward-Secure Encryption," *Eurocrypt '03,* 2003.

[C39] A. Azagury, R. Canetti, M. Factor, S. Halevi, E. Henis, D. Naor, N. Rinetzky, O. Rodeh, and J. Satran, "A Two Layered Approach for Securing an Object Store Network," *First IEEE International Security In Storage Workshop,* 2002.

[C38] R. Canetti, Y. Lindell, R. Ostrovsky, A. Sahai, "Universally composable two-party and multi-party secure computation" *34th STOC,* 2002.

[C37] R. Canetti and H. Krawczyk, "Security Analysis of IKE's Signature-based Key-Exchange Protocol", *Crypto 02,* 2002.

[C36] B. Aiello, S. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. Keromytis, O. Reingold, "Efficient, DoS-Resistant Secure Key Exchange for Internet Protocols," *ACM Computers and Communications Security conference (CCS),* 2002.

[C35] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," *Eurocrypt 02,* 2002.

[C34] R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," *42nd FOCS,* 2001. Full version at eprint.iacr.org/2000/067 and ECCC TR01-016.

[C33] R. Canetti and M. Fischlin, "Universally Composable Commitments," *Crypto 01,* 2001.

[C32] R. Canetti, I. Damgård, S. Dziembowski, Y. Ishai, T. Malkin, "On Adaptive vs. Non-adaptive Security of Multiparty Protocols," *Eurocrypt 01,* 2001.

[C31] R. Canetti, H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels," *Eurocrypt 01,* 2001.

[C30] R. Canetti, Y. Ishai, R. Kumar, M. K. Reiter, R. Rubinfeld, R. N. Wright, "Selective private function evaluation with applications to private statistics," *Principles of Distributed Computing (PODC),* 2001.

[C29] R. Canetti, J. Kilian, E. Petrank, A. Rosen, "Black-box concurrent zero-knowledge requires Omega (log n) rounds," *33rd STOC,* 2001.

[C28] A. Perrig, R. Canetti, D. Tygar, D. Song, "Efficient and Secure Source Authentication for Multicast", *Network and Distributed System Security Symposium (NDSS2001),* 2001.

[C27] R. Canetti, O. Goldreich, S. Goldwasser, S. Micali, "Resettable zero-knowledge," *32nd STOC,* 2000.

[C26] A. Perrig, R. Canetti, J. D. Tygar, D. X. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *IEEE Symposium on Security and Privacy,* 2000.

[C25] R. Canetti, Y. Dodis, S. Halevi, E. Kushilevitz, A. Sahai, "Exposure-Resilient Functions and All-or-Nothing Transforms," *Eurocrypt 02,* 2000.

[C24] R. Canetti, P-C. Cheng, F. Giraud, D. Pendarakis, J.R. Rao, R. Rohatgi, D. Saha, "IPSec-based Host Architecture for Secure Internet Multicast", *Network and Distributed System Security Symposium (NDSS2000),* 2000.

[C23] R. Canetti, C. Meadows, P. Syverson, "Environmental Requirements for Authentication Protocols," *Symposium on Requirements Engineering for Information Security (SREIS01),* 2001.

[C22] R. Canetti, R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Adaptive Security for Threshold Cryptosystems," *Crypto 99,* 1999.

[C21] R. Canetti, T. Malkin, K. Nissim, "Efficient Communication-Storage Tradeoffs for Multicast Encryption," *Eurocrypt 99,* 1999.

[C20] R. Canetti and Shafi Goldwasser, "A practical threshold cryptosystem resilient against adaptive chosen ciphertext attacks", *Eurocrypt '99,* 1999.

[C19] R. Canetti and Rafi Ostrovsky, "Secure computation with hidden cheaters (or, What if *nobody* is totally honest?)", *31st STOC,* 1999.

[C18], R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor and B. Pinkas, "A taxonomy of multicast security issues and efficient constructions", *Infocom '99,* 1999.

[C17] M. Bellare, R. Canetti and H. Krawczyk, "A Modular Approach to the Design and Analysis of Authentication and Key-Exchange Protocols", *30th STOC,* 1998.

[C16] R. Canetti, D. Micciancio and O. Reingold, "From Collision Resistance to Perfect One-Wayness", *30th STOC,* 1998.

[C15] R. Canetti, O. Goldreich and S. Halevi, "The Random-Oracle Model, Revisited", *30th STOC,* 1998.

[C14] R. Canetti, C. Dwork, M. Naor and R. Ostrovsky, "Deniable Encryptions", in proceedings of *CRYPTO '97,* LNCS 1294, 90-105, 1997.

[C13] R. Canetti, "Towards realizing random oracles: Hash functions that hide all partial information", in proceedings of *CRYPTO '97,* LNCS 1294, 455-470, 1997.

[C12] R. Canetti, S. Halevi and A. Herzberg, "How to Maintain Authenticated Communication", *16th PODC,* 15-25, 1997.

[C11] R. Canetti, E. Kushilevitz, R. Ostrovsky and A. Rosen, “Randomness vs. Fault-Tolerance”, *16th PODC,* 35-45, 1997.

[C10] M. Bellare, R. Canetti and H. Krawczyk, “Cascaded Pseudo-Randomness and its Concrete Security”, *37th FOCS,* 504-513, 1996.

[C9] R. Canetti and R. Gennaro, “Incoercible Secure Computation”, *37th FOCS,* 514-523, 1996.

[C8] M. Bellare, R. Canetti and H. Krawczyk, “Keying Hash Functions for Message Authentication”, proceedings of CRYPTO ’96, LNCS 1109, 1-15, 1996.

[C7] R. Canetti, U. Feige, O. Goldreich and M. Naor, “Adaptively Secure Multiparty Computation”, *28th STOC,* 639-648, 1996.

[C6] A. Bar-Noy, R. Canetti, S. Kutten, Y. Mansour, and B. Schieber, “Bandwidth Allocation with Preemption”, *27th STOC,* 616-625, 1995.

[C5] R. Canetti and S. Irani, “On the Power of Preemption in Randomized Scheduling”, *27th STOC,* 606-615, 1995.

[C4] R. Canetti and A. Herzberg, “Maintaining Security in the Presence of Transient Faults”, in proceedings of CRYPTO ’94, LNCS 839, 425-438, 1994.

[C3] M. Ben-Or, R. Canetti and O. Goldreich, “Asynchronous Secure Computation”, *25th STOC,* 52-61, 1993.

[C2] R. Canetti and T. Rabin, “Fast Asynchronous Byzantine Agreement with Optimal Resilience”, *25th STOC,* 42-51, 1993. Full version available at theory.lcs.mit.edu/c̃anetti.

[C1] R. Canetti and O. Goldreich, “Bounds on Tradeoffs between Randomness and Communication Complexity”, *31st FOCS*, 766-775, 1990.