CURRICULUM VITAE

Ran Canetti

February 15, 2013

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:

Associate Director for Research of the Center for Reliable Information Systems and Cyber Security (RISCS) at Boston University, since September 2011.

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

Director, The Check Point Institute for Information Security, since 2008 (on leave).

Associate Professor, School of Computer Science, Tel Aviv University, since 2008 (on leave).

Researcher, 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:

Foundations of cryptography, network and system security, distributed algorithms and systems.

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.

Other Activities:

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 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:

Ben Riva (PhD, Tel Aviv University. Expected graduation: 2014)

Nir Bitansky (PhD, Tel Aviv University. Expected graduation: 2014)

Omer Paneth (PhD, Boston University. Expected grauation: 2015)

Rita Vald (Msc, TelAviv university. Expected graduation: 2016)

Daniel Shahaf (Msc, Tel Aviv University. Expected graduation: 2013)

Past students:

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)

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

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

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

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

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

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).

Post-doctoral advisees:

Abhishek Jain (PhD UCLA, since 2012)

Rachel Huijia Lin (PhD Cornell, since 2011)

Adam O'neill (PhD GeorgiaTech, since 2011)

Noam Livne (PhD Weizmann, 2010-11)

Sebastian Gajek (PhD Bochum, 2009-2011)

Honors and Prizes:

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:

"Secure And Composable Execution of Outsourced Database Queries", with G. Kollios, submission to NSF Satc call, Nov 2012.

"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 Grant, 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:

[P4] R Canetti, S. Halevi, M. Steiner. Mitigating Dictionary Attacks on Password-Based Local Storage. Patent application submitted August 2006.

[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:

[B3] 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.

[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:

[J24] N. Bitansky, R. Canetti. On Strong Simulation and Composable Point Obfuscation. Journal of Cryptology, to appear.

[J23] R, Canetti, B. Riva, G. N. Rothblum. Refereed Delegation of Computation. Information and Computation, to appear.

[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. Nonadaptive 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:

[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.

Surveys and Tutorials:

[V7] R. Canetti: Composable Formal Security Analysis: Juggling Soundness, Simplicity and Efficiency. ICALP (2) 2008: 1-13

[V6] R. Canetti. Treading the impossible: A tour of set-up assumptions for realizing universally composable security. AsiaCrypt '07, 2007.

[V5] R. Canetti. Security and Composition of Cryptographic Protocols (Part II). SIGACT News, Vol. 37, No. 4, Dec. 2006.

[V4] R. Canetti. Security and Composition of Cryptographic Protocols (Part I). SIGACT News, Vol. 37, No. 3, Sept. 2006.

[V3] A. Perrig, R. Canetti, D. Tygar, D. Song, "The Tesla Broadcast Authentication Protocol", CryptoBytes, Vol. 5, No. 2, 2002.

[V2] R. Canetti, R. Gennaro, A. Herzberg, D. Naor, "Proactive security: Long-term Protection against break-ins", CryptoBytes, Vol. 3, No. 1, 1997.

[V1] M. Bellare, R. Canetti and H. Krawczyk, "The HMAC construction", CryptoBytes, Vol. 2, No. 1, 1996.

Internet Drafts:

[I9] R. Canetti and L. Dondeti. ESP with TESLA authentication. draft msec-ipsec-tesla-01.txt, October 2006.

[I8] M. Baugher, R. Canetti, P.C. Cheng, P. Rohatgi, "MESP: Multicast Encapsulating Security Payload," draft-ietf-msec-mesp-00.txt, October 2002.

[I7] A. Perrig, R. Canetti, B. Whillock, "TESLA: Multicast Source Authentication Transform Specification with MESP", draft-ietf-msec-tesla-spec-00.txt, October 2002.

[I6] B. Aiello, S. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. Keromytis, O. Reingold, "The JFK protocol," draft-ietf-ipsec-jfk-04.txt, July 2002.

[I5] R. Canetti, P.C. Cheng and P. Rohatgi, “Multicast Data Security Transformations: Requirements, Considerations, and Proposed Design”, Internet Draft draft-irtf-smug-data-transforms.txt, May 2000.

[I4] T. Hardjono, R. Canetti, M. Baugher, P. Dinsmore, “Secure IP Multicast: Problem areas, Framework, and Building Blocks”, Internet Draft draft-irtf-smug-framework-00.txt, Oct 1999.

[I3] R. Canetti and B. Pinkas, “A taxonomy of multicast security issues”, Internet Draft draft-canetti-secure-multicast-taxonomy-00.txt, May 1998.

[I2] R. Canetti, P. Cheng, H. Krawczyk, “A DH-less encryption mode for IKE,” draft-ietf-ipsec-dhless-enc-mode-00.txt, July 1998.

[I1] R. Canetti, P. C. Cheng, and H. Krawczyk, “Revised Encryption Mode in ISAKMP/Oakley” Internet Draft draft-ietf-ipsec-revised-encryption-mode-00.txt, May 1997.