

Jonathan Katz

Department of Computer Science and UMIACS
University of Maryland
jkatz@cs.umd.edu

Education

Ph.D. (with distinction), Computer Science, Columbia University, 2002

Dissertation: *Efficient Cryptographic Protocols Preventing “Man-in-the-Middle” Attacks*

Advisors: Zvi Galil and Moti Yung (Columbia University); Rafail Ostrovsky (Telcordia Technologies)

M.Phil., Computer Science, Columbia University, 2001

M.A., Chemistry, Columbia University, 1998

S.B., Mathematics, Massachusetts Institute of Technology, 1996

S.B., Chemistry, Massachusetts Institute of Technology, 1996

Employment History

Associate Professor (with tenure), University of Maryland

July, 2008 – present (Assistant Professor, August, 2002 – June, 2008)

Responsible for maintaining a world-class research program in cryptography and information security. Duties include supervising graduate students and designing and teaching courses in cryptography, theoretical computer science, and network security.

Visiting Research Scientist, IBM T.J. Watson Research Center (Hawthorne, NY)

August, 2008 – July, 2009

Visited and collaborated with the cryptography research group at IBM.

Visiting Professor, École Normale Supérieure (Paris, France)

June – July, 2008

Presented three lectures on my research; collaborated with the cryptography research group at ENS.

Research Fellow, Institute for Pure and Applied Mathematics, UCLA

September – December, 2006

Invited as a core participant for the Fall 2006 program on “Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security.”

Cryptography Consultant, various positions

August, 2002 – present

Designed, analyzed, and supervised the implementation and standardization of cryptographic protocols and algorithms. Provided expert testimony in intellectual property disputes. Performed cryptanalysis of proposed ciphers and security protocols.

Visiting Research Scientist, DIMACS

March – May, 2002

Conducted research in both theoretical and applied cryptography, leading to two published papers.

Instructor, Columbia University

Summer, 1999 – Spring, 2002

Instructor for five semesters. Taught *Introduction to Cryptography, Computability and Models of Computation*, and *Introduction to Computer Programming*.

Research Scientist, Telcordia Technologies

March, 2000 – October, 2001

Member of the Mathematical Sciences Research Center. Conducted basic research in cryptography leading to the filing of two provisional patents. Provided security consulting services for other research groups within Telcordia.

Security Consultant, Counterpane Systems

May, 1999 – March, 2000

Discovered security flaws in email encryption software (PGP); this work was widely covered in the press and led to two published papers and a refinement of the current standards for email encryption. Designed and implemented secure web-based protocols for clients. Contributed to *Secrets and Lies: Digital Security in a Networked World*, by B. Schneier (J. Wiley & Sons, 2000).

Honors and Awards

Invited participant, DARPA Computer Science Study Group, 2009–2010

NSF CAREER award, 2005–2010

University of Maryland GRB semester award, 2005–2006

National Defense Science and Engineering Graduate Fellowship, 1996–1999

NSF Graduate Fellowship, 1996 (declined)

Alpha Chi Sigma award for academic excellence, MIT, 1996

Research Grants

(Dollar amounts listed reflect the University of Maryland portion of the award.)

“TC: Large: Collaborative Research: Practical Secure Two-Party Computation: Techniques, Tools, and Applications,” \$1,000,000.

PI (with Michael Hicks), *August, 2011 – August 2016*

“Delegated, Outsourced, and Distributed Computation,” US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), \$199,226.

May, 2011 – April, 2013

“Toward Practical Cryptographic Protocols for Secure Information Sharing, Phase II CSSG,” DARPA, \$400,000
September, 2010 – August, 2012

“NetSE: Medium: Collaborative Research: Privacy Preserving Social Systems,” NSF, \$880,000
 co-PI (with Bobby Bhattacharjee and Neil Spring), *September, 2010 – August, 2013*

Supplement for “CAREER: Models and Cryptographic Protocols for Unstructured, Decentralized Systems,” NSF, \$80,000.
August, 2009 – August, 2010

“Efficient Security Techniques for Information Flows in Coalition Environments,” US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), \$395,026.
 PI (with Michael Hicks), *May, 2009 – April, 2011*

“Cryptographic Primitives and Protocols for Security in Complex Systems,” DARPA, \$100,000
March, 2009 – March, 2010

“Understanding Fairness in Secure Two-Party and Multi-Party Computation,” NSF, \$277,782.
September, 2008 – August, 2011

“Collaborative Research: Efficient Cryptography Based on Lattices,” NSF, \$138,500.
September, 2007 – August, 2010

“Designing Reliable and Secure Tactical MANETs,” DoD MURI, \$1,442,324.
 co-PI (with John Baras and Virgil Gligor), *May, 2007 – April, 2012*

“Energy Efficient Security Architectures and Infrastructures,” US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), \$162,450.
May, 2009 – April, 2011

“New Techniques for Authenticating Humans (and Other Resource-Constrained Devices),” NSF, \$300,000.
September, 2006 – August, 2009

“Feasibility and Efficiency of Secure Computation,” United States-Israel Binational Science Foundation, \$120,000.
September, 2005 – August, 2009

“CAREER: Models and Cryptographic Protocols for Unstructured, Decentralized Systems,” NSF, \$400,000.
February, 2005 – January, 2010

“Secure Design and Usage of Cryptographic Hash Functions,” University of Maryland GRB semester award.
2005–2006 academic year

“Resilient Storage and Querying in Decentralized Networks,” NSF, \$720,000.
 co-PI (with Bobby Bhattacharjee, Aravind Srinivasan, and Sudarshan Chawathe), *September, 2004 – August, 2008*

“Distributed Trust Computations for Decentralized Systems,” NSF, \$375,000.
co-PI (with Bobby Bhattacharjee), *August, 2003 – July, 2006*

“Collaborative Research: Mitigating the Damaging Effects of Key Exposure,” NSF, \$240,000.
August, 2003 – July, 2006

PhD Students

Graduated:

Arkady Yerukhimovich (graduated in 2011)
Currently at MIT Lincoln Laboratory

S. Dov Gordon (graduated in 2010)
Currently a CI Postdoctoral Fellow at Columbia University

Omer Horvitz (graduated in 2007, co-advised with Prof. Gligor)
Currently at techmeme.com

Chiu-Yuen Koo (graduated in 2007)
Currently at Google Labs, Mountain View, CA

Ruggero Morselli, (graduated in 2006, co-advised with Prof. Bhattacharjee)
Currently at Google Labs, Pittsburgh, PA

Current:

Adam Groce

Ranjit Kumaresan

Postdoctoral Researchers

Dominique Schröder, 2011-2013

Hong-Sheng Zhou, 2010-2012

Seung Geol Choi, 2010-2012

Vassilis Zikas, 2010-2012

Lior Malka, 2009–2010
Currently at Intel, Santa Clara, CA

Ik Rae Jeong, 2005–2005
Currently at Korea University

Professional Activities

Editorial board:

- IEE Proceedings Information Security (*2005–present*)
- Fundamenta Informaticae (*2006–present*)
- International Journal of Applied Cryptography (*2007–present*)

Program chair:

- Applied Cryptography and Network Security (ACNS) 2007
- Cryptography Track, 12th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS) 2010

Program committees:

- Theory of Cryptography Conference (TCC) 2012, 2007, 2006
- RSA — Cryptographers’ Track 2012, 2010, 2007, 2006
- Financial Cryptography 2012
- ACM Conference on Computer and Communications Security (CCCS) 2011, 2006, 2005
- Eurocrypt 2011, 2009, 2008, 2006
- ACM-SIAM Symposium on Discrete Algorithms (SODA) 2011
- Intl. Conf. on Cryptology and Network Security (CANS) 2010
- Intl. Conf. on Pairing-Based Cryptography (Pairing) 2010
- Asiacrypt 2010, 2008, 2007, 2004
- Public-Key Cryptography (PKC) 2010, 2007
- Crypto 2009, 2006, 2005, 2003
- IEEE Symposium on Security & Privacy (Oakland) 2009
- ACM Symposium on Theory of Computing (STOC) 2009
- Applied Cryptography and Network Security (ACNS) 2009, 2006
- IEEE Symposium on Foundations of Computer Science (FOCS) 2008
- Security in Communication Networks 2008
- ICALP 2007
- ACM Workshop on Security and Sensor Networks (SASN) 2006, 2005, 2004
- Security and Cryptography for Networks (SCN) 2006
- VietCrypt 2006
- International Conference on Information Security and Cryptology (ICISC) 2006, 2005
- UCLA/IPAM workshop on “Locally decodable codes...,” 2006
- ACM Conference on Computer and Communications Security (CCCS) 2005
- Workshop on Cryptography over Ad Hoc Networks (WCAN) 2006, 2005
- International Conference on Cryptology in Malaysia (Mycrypt) 2005
- Workshop in Information Security and Applications (WISA) 2004

Invited Courses/Tutorials

Half-day tutorial: “Ruminations on Defining Rational Multi-Party Computation,” Summer School on Rational Cryptography (Bertinoro, Italy), June 2008.

1-hour tutorial: “The Basics of Public-Key Encryption,” Booz Allen Hamilton (Linthicum, MD), October 2007.

2⁺-hour tutorial: “A Survey of Modern Cryptography,” ACM Sigmetrics, June 2007.

Week-long course: “Zero Knowledge: Foundations and Applications,” (Bertinoro, Italy), October 2006.

Half-day tutorial: “Black-Box Reductions, Impossibility Results, and Efficiency Lower Bounds,” UCLA/IPAM, September 2006.

Invited Panel and Session Participation

11th Colloquium for Information System Security Education (Boston University): panel member, “How to Teach Cryptology,” June 2007.

Invited Talks

Microsoft Research (Redmond, WA): “(Ever More) Efficient Secure Two-Party Computation,” March 2011.

PerAda Workshop on Security, Trust, and Privacy (Rome, Italy): “Privacy, Trust, and Security in Pervasive Computing: Challenges and Opportunities,” November 2010.

Tsinghua University (Beijing, China): “Fairness and Partial Fairness in Two-Party Computation,” June 2010

Beijing Institute of Technology: “Rational Secret Sharing,” June 2010.

SKLOIS: The State Key Laboratory Of Information Security (Beijing, China): “Leakage-Resilient Cryptography,” June 2010.

SKLOIS: The State Key Laboratory Of Information Security (Beijing, China): “Rational Secret Sharing,” June 2010.

Workshop on Decentralized Mechanism Design, Distributed Computing, and Cryptography (Princeton University): “Rational Secret Sharing: A Survey,” June 2010.

Microsoft Research (Cambridge, MA): “Rational Secret Sharing,” April 2009.

AT&T Labs: “Fairness and Partial Fairness in Secure Two-Party Computation,” February 2009.

University of Toronto: “Fairness and Partial Fairness in Secure Two-Party Computation,” February 2009.

Joint Mathematics Meetings, AMS Special Session on Algebraic Cryptography and Generic Complexity: “Public-Key Cryptography from a (Theoretical) Cryptographer’s Perspective,” January 2009.

Dagstuhl workshop on Theoretical Foundations of Practical Information Security (Germany): “Partial Fairness in Secure Two-Party Computation,” December 2008.

École Normale Supérieure (Paris, France): “Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise,” July 2008.

École Normale Supérieure (Paris, France): “Predicate Encryption: A New Paradigm for Public-Key Encryption,” July 2008.

École Normale Supérieure (Paris, France): “Fairness in Secure Computation,” June 2008.

UC Berkeley: “Predicate Encryption: A New Paradigm for Public-Key Encryption,” May 2008.

5th Theory of Cryptography Conference (TCC) 2008 (New York): “Bridging Game Theory and Cryptography: Recent Results and Future Directions,” March 2008.

MIT Cryptography and Information Security Seminar: “Complete Fairness in Secure Two-Party Computation,” March 2008.

11th IMA Intl. Conference on Cryptography and Coding Theory (Cirencester, UK): “Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise,” December 2007.

INDOCRYPT 2007 (Chennai, India): “Capability-Based Encryption: A New Paradigm for Public-Key Encryption,” December 2007.

Pennsylvania State University: “Universally-Composable Multi-Party Computation using Tamper-Proof Hardware,” April 2007.

Workshop on Cryptography: Underlying Mathematics, Provability, and Foundations (Fields Institute, Toronto): “Blind Signatures: Definitions and Constructions,” November 2006.

Workshop on Foundations of Secure Multi-Party Computation (UCLA/IPAM): “On Expected Constant-Round Protocols for Broadcast,” November 2006.

Workshop on Public-Key Systems with Special Properties (UCLA/IPAM): “Blind Signatures: Definitions and Constructions,” October 2006.

13th SIAM Meeting on Discrete Mathematics (Victoria, Canada): “New Techniques for Authenticating Humans,” June 2006.

Boston University: “New Techniques for Authenticating Humans (and other Resource-Constrained Devices),” April 2006.

Stevens Institute of Technology: “New Techniques for Authenticating Humans (and other Resource-Constrained Devices),” March 2006.

Georgia Tech: “New Techniques for Authenticating Humans (and other Resource-Constrained Devices),” November 2005.

University of Modena: “Secure Authentication without Traditional Cryptographic Keys,” July 2005.

Workshop on the Past, Present, and Future of Oblivious Transfer (Haifa, Israel): “Round-Optimal Secure Two-Party Computation,” May, 2005.

UCLA: “Secure Remote Authentication Using Biometric Data,” March, 2005.

Luminy Workshop on Cryptography (Marseilles, France): “Secure Remote Authentication Using Biometric Data,” November, 2004.

DIMACS Workshop on *Cryptography: Theory Meets Practice*: “Using Biometric Data for Secure Network-Based Authentication,” October, 2004.

MIT Cryptography and Information Security Seminar: “Round-Optimal Secure Two-Party Computation,” April, 2004.

Korea University: “Scalable and Efficient Protocols for Authenticated Group Key Exchange,” November, 2003.

Korea Information Security Agency (KISA): “Efficient Protocols for Password-Only Authenticated Key Exchange,” November, 2003.

6th Annual International Conference on Information Security and Cryptology (ICISC 2003): “Binary Tree Encryption: Constructions and Applications,” November, 2003.

National Science Foundation (NSF) — Washington Area Trustworthy Systems Hour: “Maintaining Security in the Event of Key Exposure,” April, 2003.

New York University: “Efficient and Non-Malleable Proofs of Plaintext Knowledge and Applications,” July, 2002.

IBM T.J. Watson Research Center: “A Forward-Secure Public-Key Encryption Scheme,” July, 2002.

DIMACS Workshop on *Cryptographic Protocols in Complex Environments*: “Efficient and Non-Malleable Proofs of Plaintext Knowledge and Applications,” May, 2002.

IBM T.J. Watson Research Center: “Practical Password-Authenticated Key Exchange Provably Secure Against Off-Line Dictionary Attacks,” December, 2000.

MIT Cryptography and Information Security Seminar: “Practical and Provably Secure Password-Authenticated Key Exchange,” December, 2000.

Bell Labs (Lucent Technologies) Crypto/Security Seminar: “Cryptographic Counters and Applications to Electronic Voting,” November, 2000.

Publications

Books Authored or Edited

1. J. Katz. *Digital Signatures*. Springer, 2010.
2. J. Katz and Y. Lindell. *Introduction to Modern Cryptography*. Chapman & Hall/CRC Press, 2007.
3. J. Katz and M. Yung, eds. *Applied Cryptography and Network Security, 5th International Conference, ACNS 2007, Proceedings*. Lecture Notes in Computer Science 4521, Springer, 2007.

Book Chapters

1. J. Katz. “Public-Key Cryptography.” In *Handbook of Information and Communication Security*, P. Stavroulakis and M. Stamp, eds., Springer, 2010.
2. J. Katz. “Cryptography.” In *Wiley Encyclopedia of Computer Science and Engineering*, B.W. Wah, ed., John Wiley & Sons, 2008.
3. J. Katz. “Symmetric-Key Encryption.” In *The Handbook of Information Security*, H. Bidgoli, ed., John Wiley & Sons, Inc., 2005.
4. J. Katz. “Cryptography.” In *The Computer Science and Engineering Handbook*, A. Tucker, ed., CRC Press, 2004.

Journal Articles

1. S.D. Gordon, C. Hazay, J. Katz, and Y. Lindell. “Complete Fairness in Secure Two-Party Computation.” *J. ACM*, to appear.
2. S.D. Gordon and J. Katz. “Partial Fairness in Secure Two-Party Computation.” *J. Cryptology*, to appear.
3. J. Katz. “Which Languages Have 4-Round Zero-Knowledge Proofs?” *J. Cryptology*, to appear. One of three papers from TCC 2008 invited to this journal.
4. Y. Ishai, J. Katz, E. Kushilevitz, Y. Lindell, and E. Petrank. “On Achieving the ‘Best of Both Worlds’ in Secure Multiparty Computation.” *SIAM J. Computing* 40(1): 122–141, 2011.
5. J. Katz, J.-S. Shin, and A. Smith. “Parallel and Concurrent Security of the HB and HB⁺ Protocols.” *J. Cryptology* 23(3): 402–421, 2010.
6. O. Horvitz and J. Katz. “Bounds on the Efficiency of ‘Black-Box’ Commitment Schemes.” *Theoretical Computer Science* 411(10): 1251–1260, 2010.
7. J. Katz, R. Ostrovsky, and M. Yung. “Efficient and Secure Authenticated Key Exchange Using Weak Passwords.” *J. ACM* 57(1): 78–116, 2009.
8. J. Katz, C.-Y. Koo, and R. Kumaresan. “Improving the Round Complexity of VSS in Point-to-Point Networks.” *Information & Computation* 207(8): 889–899, 2009.
9. I. Haitner, O. Horvitz, J. Katz, C.-Y. Koo, R. Morselli, and R. Shaltiel. “Reducing Complexity Assumptions for Statistically-Hiding Commitment.” *J. Cryptology* 22(3): 283–310, 2009.
10. A. Bender, J. Katz, and R. Morselli. “Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles.” *J. Cryptology* 22(1): 114–138, 2009.
11. J. Katz and C.-Y. Koo. “On Expected Constant-Round Protocols for Byzantine Agreement.” *J. Computer and System Sciences* 75(2): 91–112, 2009.
12. J. Katz and Y. Lindell. “Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs.” *J. Cryptology* 21(3): 303–349, 2008.
13. E.-J. Goh, S. Jarecki, J. Katz, and N. Wang. “Efficient Signature Schemes with Tight Security Reductions to the Diffie-Hellman Problems.” *J. Cryptology* 20(4): 493–514, 2007.
14. R. Canetti, S. Halevi, and J. Katz. “A Forward-Secure Public-Key Encryption Scheme.” *J. Cryptology* 20(3): 265–294, 2007.
15. J. Katz and M. Yung. “Scalable Protocols for Authenticated Group Key Exchange.” *J. Cryptology* 20(1): 85–113, 2007.

16. D. Boneh, R. Canetti, S. Halevi, and J. Katz. “Chosen-Ciphertext Security from Identity-Based Encryption.” *SIAM J. Computing* 36(5): 1301–1328, 2007.
17. J. Katz and M. Yung. “Characterization of Security Notions for Probabilistic Private-Key Encryption.” *J. Cryptology* 19(1): 67–96, 2006.
18. R. Gennaro, Y. Gertner, J. Katz, and L. Trevisan. “Bounds on the Efficiency of Generic Cryptographic Constructions.” *SIAM J. Computing* 35(1): 217–246, 2005.
19. W. Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili. “A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks.” *ACM Trans. on Information and System Security* 8(2): 228–258, 2005.
20. J. Katz, A. Sahai, and B. Waters. “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products.” Accepted to *J. Cryptology* (pending minor revisions). One of 4 papers from Eurocrypt 2008 invited to this journal.
21. J. Katz, P. MacKenzie, G. Taban, and V. Gligor. “Two-Server Password-Only Authenticated Key Exchange.” Accepted to *J. Computer and System Sciences* (pending minor revisions).
22. J. Katz and C.-Y. Koo. “On Constructing Universal One-Way Hash Functions from Arbitrary One-Way Functions.” Accepted to *J. Cryptology* (pending minor revisions).

Articles in Refereed Conferences and Workshops

1. Y. Huang, D. Evans, J. Katz, and L. Malka. “Faster Secure Two-Party Computation Using Garbled Circuits.” *USENIX Security Symposium 2011*.
2. J. Garay, J. Katz, R. Kumaresan, and H.-S. Zhou. “Adaptively Secure Broadcast, Revisited.” *ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 179–186, ACM, 2011.
3. J. Katz and V. Vaikuntanathan. “Round-Optimal Password-Based Authenticated Key Exchange.” *8th Theory of Cryptography Conference (TCC)*, pp. 293–310, LNCS vol. 6597, Springer, 2011. **One of three papers invited to a special issue of *J. Cryptology*.**
4. A. Groce, J. Katz, and A. Yerukhimovich. “Limits of Computational Differential Privacy in the Client/Server Setting.” *8th Theory of Cryptography Conference (TCC)*, pp. 417–431, LNCS vol. 6597, Springer, 2011.
5. Z. Brakerski, J. Katz, G. Segev, and A. Yerukhimovich. “Limits on the Power of Zero-Knowledge Proofs in Cryptographic Constructions.” *8th Theory of Cryptography Conference (TCC)*, pp. 559–578, LNCS vol. 6597, Springer, 2011.
6. J. Katz, D. Schröder, and A. Yerukhimovich. “Impossibility of Blind Signatures from One-Way Permutations.” *8th Theory of Cryptography Conference (TCC)*, pp. 615–629, LNCS vol. 6597, Springer, 2011.

7. Y. Huang, L. Malka, D. Evans, and J. Katz. “Efficient Privacy-Preserving Biometric Identification.” *Network & Distributed System Security Conference (NDSS) 2011*.
8. S.D. Gordon, J. Katz, and V. Vaikuntanathan. “A Group Signature Scheme from Lattice Assumptions.” *Advances in Cryptology — Asiacrypt 2010*, pp. 395–412, LNCS vol. 6477, Springer, 2010.
9. Z. Brakerski, Y. Tauman Kalai, J. Katz, and V. Vaikuntanathan. “Public-Key Cryptography Resilient to Continual Memory Leakage.” *Proc. 51st Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 501–510, IEEE, 2010.
10. J. Katz and L. Malka. “Secure Text Processing with Applications to Private DNA Matching.” *Proc. 17th ACM Conf. on Computer and Communications Security*, pp. 485–492, ACM, 2010.
11. A. Groce and J. Katz. “A New Framework for Efficient Password-Based Authenticated Key Exchange.” *Proc. 17th ACM Conf. on Computer and Communications Security*, pp. 516–525, ACM, 2010.
12. S.D. Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich. “Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure.” *12th Intl. Symp. on Stabilization, Safety, and Security of Distributed Systems*, pp. 144–158, LNCS vol. 6366, Springer, 2010. **Invited to a special issue of *Information & Computation*.**
13. D. Gordon and J. Katz. “Partial Fairness in Secure Computation.” *Advances in Cryptology — Eurocrypt 2010*, pp. 157–176, LNCS vol. 6110, Springer, 2010.
14. R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin. “Secure Network Coding over the Integers.” *Public-Key Cryptography (PKC)*, pp. 142–160, LNCS vol. 6056, Springer, 2010.
15. G. Fuchsbauer, J. Katz, and D. Naccache. “Efficient Rational Secret Sharing in Standard Communication Networks.” *7th Theory of Cryptography Conference (TCC)*, pp. 419–436, LNCS vol. 5978, Springer, 2010.
16. J. Katz and V. Vaikuntanathan. “Signature Schemes with Bounded Leakage Resilience.” *Advances in Cryptology — Asiacrypt 2009*, pp. 703–720, LNCS vol. 5912, Springer, 2009.
17. J. Katz and A. Yerukhimovich. “On Black-Box Constructions of Predicate Encryption Schemes from Trapdoor Permutations.” *Advances in Cryptology — Asiacrypt 2009*, pp. 197–213, LNCS vol. 5912, Springer, 2009.
18. J. Katz and V. Vaikuntanathan. “Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices.” *Advances in Cryptology — Asiacrypt 2009*, pp. 636–652, LNCS vol. 5912, Springer, 2009.

19. G. Ateniese, S. Kamara, and J. Katz. “Proofs of Storage from Homomorphic Identification Protocols.” *Advances in Cryptology — Asiacrypt 2009*, pp. 319–333, LNCS vol. 5912, Springer, 2009.
20. M. Albrecht, C. Gentry, S. Halevi, and J. Katz. “Attacking Cryptographic Schemes Based on ‘Perturbation Polynomials’.” *Proc. 16th ACM Conf. on Computer and Communications Security*, pp. 1–10, ACM, 2009.
21. J. Alwen, J. Katz, Y. Lindell, G. Persiano, A. Shelat, and I. Visconti. “Collusion-Free Multiparty Computation in the Mediated Model.” *Advances in Cryptology — Crypto 2009*, pp. 524–540, LNCS vol. 5677, Springer, 2009.
22. D. Boneh, J. Katz, D. Freeman, and B. Waters. “Signing a Linear Subspace: Signatures for Network Coding.” *Public-Key Cryptography (PKC)*, pp. 68–87, LNCS vol. 5443, Springer, 2009.
23. Y. Dodis, J. Katz, A. Smith, and S. Walfish. “Composability and On-Line Deniability of Authentication.” *6th Theory of Cryptography Conference (TCC)*, pp. 146–162, LNCS vol. 5444, Springer, 2009.
24. S.D. Gordon and J. Katz. “Complete Fairness in Multi-Party Computation Without an Honest Majority.” *6th Theory of Cryptography Conference (TCC)*, pp. 19–35, LNCS vol. 5444, Springer, 2009.
25. J. Katz, C.-Y. Koo, and R. Kumaresan. “Improving the Round Complexity of VSS in Point-to-Point Networks.” *Intl. Colloquium on Automata, Languages, and Programming (ICALP)*, pp. 499–510, LNCS vol. 5126, Springer, 2008.
26. S.D. Gordon, C. Hazay, J. Katz, and Y. Lindell. “Complete Fairness in Secure Two-Party Computation.” *Proc. 40th Annual ACM Symposium on Theory of Computing (STOC) 2008*, pp. 413–422, ACM, 2008.
27. J. Katz, A. Sahai, and B. Waters. “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products.” *Advances in Cryptology — Eurocrypt 2008*, pp. 146–162, LNCS vol. 4965, Springer, 2008. **One of four papers invited to a special issue of *J. Cryptology*.**
28. S. Kamara and J. Katz. “How to Encrypt with a Malicious Random Number Generator.” *Fast Software Encryption (FSE)*, pp. 303–315, LNCS vol. 5086, Springer, 2008.
29. J. Katz and Y. Lindell. “Aggregate Message Authentication Codes.” *RSA Conference — Cryptographers’ Track*, pp. 155–169, LNCS vol. 4964, Springer, 2008.
30. J. Katz. “Bridging Cryptography and Game Theory: Recent Results and Future Directions” (invited paper). *5th Theory of Cryptography Conference (TCC)*, pp. 251–272, LNCS vol. 4948, Springer, 2008.

31. J. Katz. “Which Languages Have 4-Round Zero-Knowledge Proofs?” *5th Theory of Cryptography Conference (TCC)*, pp. 73–88, LNCS vol. 4948, Springer, 2008. **One of three papers invited to a special issue of *J. Cryptology*.**
32. V. Goyal and J. Katz. “Universally-Composable Computation with an Unreliable Common Reference String.” *5th Theory of Cryptography Conference (TCC)*, pp. 142–154, LNCS vol. 4948, Springer, 2008.
33. J. Katz. “Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise” (invited paper). *11th IMA Intl. Conference on Cryptography and Coding Theory*, pp. 1–15, Lecture Notes in Computer Science vol. 4887, Springer, 2007.
34. J. Garay, J. Katz, C.-Y. Koo, and R. Ostrovsky. “Round Complexity of Authenticated Broadcast with a Dishonest Majority.” *Proc. 48th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 658–668, IEEE, 2007.
35. O. Horvitz and J. Katz. “Universally Composable Two-Party Computation in Two Rounds.” *Advances in Cryptology — Crypto 2007*, pp. 111–129, Lecture Notes in Computer Science vol. 4622, Springer, 2007.
36. R. Morselli, B. Bhattacharjee, J. Katz, and M. Marsh. “Exploiting Approximate Transitivity of Trust” (invited paper). *4th Intl. Conf. on Broadband Communications, Networks, and Systems (BroadNets)*, pp. 515–524, IEEE, 2007.
37. J. Katz. “On Achieving the ‘Best of Both Worlds’ in Secure Multiparty Computation.” *Proc. 39th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 11–20, ACM, 2007.
38. J. Katz. “Universally-Composable Multi-Party Computation using Tamper-Proof Hardware.” *Advances in Cryptology — Eurocrypt 2007*, pp. 115–128, Lecture Notes in Computer Science vol. 4515, Springer, 2007.
39. J. Katz and C.-Y. Koo. “Round-Efficient Secure Computation in Point-to-Point Networks.” *Advances in Cryptology — Eurocrypt 2007*, pp. 311–328, Lecture Notes in Computer Science vol. 4515, Springer, 2007.
40. C. Hazay, J. Katz, C.-Y. Koo, and Y. Lindell. “Concurrently-Secure Blind Signatures without Random Oracles or Setup Assumptions.” *4th Theory of Cryptography Conference (TCC)*, pp. 323–341, Lecture Notes in Computer Science vol. 4391, Springer, 2007.
41. S.D. Gordon and J. Katz. “Rational Secret Sharing, Revisited.” *Security and Cryptography for Networks (SCN)*, pp. 229–241, Lecture Notes in Computer Science vol. 4116, Springer, 2006. An extended abstract of this work also appeared at *NetEcon 2006*.
42. J. Katz and C.-Y. Koo. “On Expected Constant-Round Protocols for Byzantine Agreement.” *Advances in Cryptology — Crypto 2006*, pp. 445–462, Lecture Notes in Computer Science vol. 4117, Springer, 2006.

43. Y. Dodis, J. Katz, L. Reyzin, and A. Smith. “Authenticated Key Agreement from ‘Close’ Secrets.” *Advances in Cryptology — Crypto 2006*, pp. 232–250, Lecture Notes in Computer Science vol. 4117, Springer, 2006.
44. C.-Y. Koo, V. Bhandari, J. Katz, and N. Vadiya. “Reliable Broadcast in Radio Networks: The Bounded Collision Case.” *Proc. 25th Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 258–262, ACM, 2006.
45. J. Katz and J.S. Shin. “Parallel and Concurrent Security of the HB and HB⁺ Protocols.” *Advances in Cryptology — Eurocrypt 2006*, pp. 73–87, Lecture Notes in Computer Science vol. 4004, Springer, 2006.
46. A. Bender, J. Katz, and R. Morselli. “Ring Signatures: Stronger Definitions, and Constructions without Random Oracles.” *3rd Theory of Cryptography Conference (TCC)*, pp. 60–79, Lecture Notes in Computer Science vol. 3876, Springer, 2006.
47. J. Katz and J.S. Shin. “Modeling Insider Attacks on Group Key-Exchange Protocols.” *Proc. 12th ACM Conf. on Computer and Communications Security*, pp. 180–189, ACM, 2005.
48. O. Horvitz and J. Katz. “Lower Bounds on the Efficiency of ‘Black-Box’ Commitment Schemes.” *International Colloquium on Automata, Languages, and Programming (ICALP)*, pp. 128–139, Lecture Notes in Computer Science vol. 3580, Springer, 2005. **Invited to a special issue of *Theoretical Computer Science*.**
49. J. Katz, P. MacKenzie, G. Taban, and V. Gligor. “Two-Server Password-Only Authenticated Key Exchange.” *Applied Cryptography and Network Security (ACNS)*, pp. 1–16, Lecture Notes in Computer Science vol. 3531, Springer, 2005.
50. X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith. “Secure Remote Authentication Using Biometric Data.” *Advances in Cryptology — Eurocrypt 2005*. pp. 147–163, Lecture Notes in Computer Science vol. 3494, Springer, 2005.
51. R. Canetti, S. Halevi, J. Katz, Y. Lindell, and P. MacKenzie. “Universally Composable Password-Based Key Exchange.” *Advances in Cryptology — Eurocrypt 2005*, pp. 404–421, Lecture Notes in Computer Science vol. 3494, Springer, 2005.
52. I. Haitner, O. Horvitz, J. Katz, C.-Y. Koo, R. Morselli, and R. Shaltiel. “Reducing Complexity Assumptions for Statistically-Hiding Commitment.” *Advances in Cryptology — Eurocrypt 2005*, pp. 58–77, Lecture Notes in Computer Science vol. 3494, Springer, 2005. **Invited to a special issue of *Theoretical Computer Science*.**
53. R. Canetti, S. Halevi, and J. Katz. “Adaptively-Secure, Non-Interactive Public-Key Encryption.” *2nd Theory of Cryptography Conference (TCC)*, pp. 150–168, Lecture Notes in Computer Science vol. 3378, Springer, 2005.
54. J. Katz and Y. Lindell. “Handling Expected Polynomial-Time Strategies in Simulation Based Security Proofs.” *2nd Theory of Cryptography Conference (TCC)*, pp. 128–149, Lecture Notes in Computer Science vol. 3378, Springer, 2005.

55. Y. Dodis and J. Katz. “Chosen-Ciphertext Security of Multiple Encryption.” *2nd Theory of Cryptography Conference (TCC)*, pp. 188–209, Lecture Notes in Computer Science vol. 3378, Springer, 2005.
56. D. Boneh and J. Katz. “Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption.” *RSA Conference — Cryptographers’ Track*, pp. 87–103, Lecture Notes in Computer Science vol. 3376, Springer, 2005.
57. J. Katz, R. Ostrovsky, and M.O. Rabin. “Identity-Based Zero Knowledge.” *Security in Communication Networks (SCN)*, pp. 180–192, Lecture Notes in Computer Science vol. 3352, Springer, 2004.
58. R. Morselli, J. Katz, and B. Bhattacharjee. “A Game-Theoretic Framework for Analyzing Trust-Inference Protocols.” *Second Workshop on the Economics of Peer-to-Peer Systems*, Boston, MA, 2004.
59. J. Katz and R. Ostrovsky. “Round-Optimal Secure Two-Party Computation.” *Advances in Cryptology — Crypto 2004*, pp. 335–354, Lecture Notes in Computer Science vol. 3152, Springer, 2004.
60. I.R. Jeong, J. Katz, D.H. Lee. “One-Round Protocols for Two-Party Authenticated Key Exchange.” *Applied Cryptography and Network Security (ACNS)*, pp. 220–232, Lecture Notes in Computer Science vol. 3089, Springer, 2004.
61. R. Canetti, S. Halevi, and J. Katz. “Chosen-Ciphertext Security from Identity-Based Encryption.” *Advances in Cryptology — Eurocrypt 2004*, pp. 207–222, Lecture Notes in Computer Science vol. 3027, Springer, 2004.
62. R. Morselli, B. Bhattacharjee, J. Katz, and P. Keleher. “Trust-Preserving Set Operations.” *Proc. IEEE INFOCOM*, pp. 2231–2241, IEEE, 2004.
63. Y. Dodis, M. Franklin, J. Katz, A. Miyaji, and M. Yung. “A Generic Construction for Intrusion-Resilient Public-Key Encryption.” *RSA Conference — Cryptographers’ Track*, pp. 81–98, Lecture Notes in Computer Science vol. 2964, Springer, 2004.
64. J. Katz. “Binary Tree Encryption: Constructions and Applications” (invited paper). *6th Intl. Conference on Information Security and Cryptology (ICISC)*, pp. 1–11, Lecture Notes in Computer Science vol. 2971, Springer, 2003.
65. J. Katz and N. Wang. “Efficiency Improvements for Signature Schemes with Tight Security Reductions.” *Proc. 10th ACM Conf. on Computer and Communications Security*, pp. 155–164, ACM, 2003.
66. J. Katz and M. Yung. “Scalable Protocols for Authenticated Group Key Exchange.” *Advances in Cryptology — Crypto 2003*, pp. 110–125, Lecture Notes in Computer Science vol. 2729, Springer, 2003.
67. R. Gennaro, Y. Gertner, and J. Katz. “Lower Bounds on the Efficiency of Encryption and Digital Signature Schemes.” *Proc. 35th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 417–425, ACM, 2003.

68. J. Katz, R. Ostrovsky, and A. Smith. “Round Efficiency of Multi-Party Computation with Dishonest Majority.” *Advances in Cryptology — Eurocrypt 2003*, pp. 578–595, Lecture Notes in Computer Science vol. 2656, Springer, 2003.
69. R. Canetti, S. Halevi, and J. Katz. “A Forward-Secure Public-Key Encryption Scheme.” *Advances in Cryptology — Eurocrypt 2003*, pp. 255–272, Lecture Notes in Computer Science vol. 2656, Springer, 2003.
70. J. Katz. “Efficient and Non-Malleable Proofs of Plaintext Knowledge and Applications.” *Advances in Cryptology — Eurocrypt 2003*, pp. 211–228, Lecture Notes in Computer Science vol. 2656, Springer, 2003.
71. A. Khalili, J. Katz, and W. Arbaugh. “Toward Secure Key Distribution in Truly Ad-Hoc Networks.” *2003 Symposium on Applications and the Internet Workshops*, pp. 342–346, IEEE, 2003.
72. Y. Dodis, M. Franklin, J. Katz, A. Miyaji, and M. Yung. “Intrusion-Resilient Public-Key Encryption.” *RSA Conference — Cryptographers’ Track*, pp. 19–32, Lecture Notes in Computer Science vol. 2612, Springer, 2003.
73. Y. Dodis, J. Katz, S. Xu, and M. Yung. “Strong Key-Insulated Signature Schemes.” *Public-Key Cryptography (PKC)*, pp. 130–144, Lecture Notes in Computer Science vol. 2567, Springer, 2003.
74. J. Katz, R. Ostrovsky, and M. Yung. “Forward Secrecy in Password-Only Key-Exchange Protocols.” *Security in Communication Networks (SCN)*, pp. 29–44, Lecture Notes in Computer Science vol. 2576, Springer, 2002.
75. J. Katz and M. Yung. “Threshold Cryptosystems Based on Factoring.” *Advances in Cryptology — Asiacrypt 2002*, pp. 192–205, Lecture Notes in Computer Science vol. 2501, Springer, 2002.
76. K. Jallad, J. Katz, and B. Schneier. “Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG.” *Information Security Conference*, pp. 90–101, Lecture Notes in Computer Science vol. 2433, Springer, 2002.
77. Y. Dodis, J. Katz, S. Xu, and M. Yung. “Key-Insulated Public-Key Cryptosystems.” *Advances in Cryptology — Eurocrypt 2002*, pp. 65–82, Lecture Notes in Computer Science vol. 2332, Springer, 2002.
78. E. Buonanno, J. Katz, and M. Yung. “Incremental and Unforgeable Encryption.” *Fast Software Encryption (FSE)*, pp. 109–124, Lecture Notes in Computer Science vol. 2355, Springer, 2002.
79. J. Katz, R. Ostrovsky, and M. Yung. “Efficient Password-Authenticated Key-Exchange Using Human-Memorizable Passwords.” *Advances in Cryptology — Eurocrypt 2001*, pp. 474–494, Lecture Notes in Computer Science vol. 2045, Springer, 2001.

80. J. Katz, R. Ostrovsky, and S. Myers. “Cryptographic Counters and Applications to Electronic Voting.” *Advances in Cryptology — Eurocrypt 2001*, pp. 78–92, Lecture Notes in Computer Science vol. 2045, Springer, 2001.
81. G. Di Crescenzo, J. Katz, R. Ostrovsky, and A. Smith. “Efficient and Non-Interactive, Non-Malleable Commitment.” *Advances in Cryptology — Eurocrypt 2001*, pp. 40–59, Lecture Notes in Computer Science vol. 2045, Springer, 2001.
82. J. Katz and B. Schneier. “A Chosen-Ciphertext Attack Against Several E-mail Encryption Protocols.” *Proc. 9th USENIX Security Symposium*, pp. 241–246, USENIX, 2000.
83. J. Katz and M. Yung. “Unforgeable Encryption and Chosen-Ciphertext-Secure Modes of Operation.” *Fast Software Encryption (FSE)*, pp. 284–299, Lecture Notes in Computer Science vol. 1978, Springer, 2001.
84. J. Katz and M. Yung. “Complete Characterization of Security Notions for Probabilistic, Private-Key Encryption.” *Proc. 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pp. 245–254, ACM, 2000.
85. J. Katz and L. Trevisan. “On the Efficiency of Local Decoding Procedures for Error-Correcting Codes.” *Proc. 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pp. 80–86, ACM, 2000.

Other

1. R. Morselli, B. Bhattacharjee, J. Katz, and M. Marsh, “KeyChains: A Decentralized Public-Key Infrastructure,” Technical Report CS-TR-4788, University of Maryland Computer Science Department, March, 2006.