

# 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**, 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 (New York)

*August, 2008 – July, 2009*

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 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

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.)

“Cryptographic Primitives and Protocols for Security in Complex Systems,” DARPA Computer Science Study Group, \$100,000

PI, *March, 2009 – March, 2010*

“Understanding Fairness in Secure Two-Party and Multi-Party Computation,” NSF, \$277,782.

PI, *September, 2008 – August, 2011*

“Collaborative Research: Efficient Cryptography Based on Lattices,” NSF, \$138,500.

PI, *September, 2007 – August, 2010*

“Designing Reliable and Secure Tactical MANETs,” DoD MURI, \$1,442,324.  
co-PI, *May, 2007 – April, 2012*

International Technology Alliance in Network and Information Science, US Army Research Laboratory/UK Ministry of Defense, \$3,700,000.  
Associate investigator (TA2/Project 5), *May, 2006 – April, 2016*

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

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

“CAREER: Models and Cryptographic Protocols for Unstructured, Decentralized Systems,” NSF CAREER award, \$400,000.  
PI, *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, *September, 2004 – August, 2008*

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

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

## PhD Students

### **Graduated:**

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

Chiu-Yuen Koo, 2007  
Currently at Google Labs, Mountain View, CA

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

### **Current:**

Samuel Dov Gordon

Arkady Yerukhimovich

Ranjit Kumaresan

## 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

### Program committees:

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

- ACM Workshop on Security and Sensor Networks (SASN) 2004
- Crypto 2003

## **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<sup>+</sup>-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**

Army Research Labs, Adelphi, MD: “Message Authentication Codes (an Introduction),” October 2009.

Microsoft Research, Cambridge: “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 and Y. Lindell. *Introduction to Modern Cryptography*. Chapman & Hall/CRC Press, 2007.
2. 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 Communication and Information Security*, M. Stamp, ed., Springer, 2009 (to appear).
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. J. Katz, R. Ostrovsky, and M. Yung. “Efficient and Secure Authenticated Key Exchange Using Weak Passwords.” *J. ACM*, to appear.
2. O. Horvitz and J. Katz. “Bounds on the Efficiency of ‘Black-Box’ Commitment Schemes.” *Theoretical Computer Science*, to appear.
3. 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.
4. 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.
5. A. Bender, J. Katz, and R. Morselli. “Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles.” *J. Cryptology* 22(1): 114–138, 2009.
6. J. Katz and C.-Y. Koo. “On Expected Constant-Round Protocols for Byzantine Agreement.” *J. Computer and System Sciences* 75(2): 91–112, 2009.
7. J. Katz and Y. Lindell. “Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs.” *J. Cryptology* 21(3): 303–349, 2008.
8. 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.
9. R. Canetti, S. Halevi, and J. Katz. “A Forward-Secure Public-Key Encryption Scheme.” *J. Cryptology* 20(3): 265–294, 2007.
10. J. Katz and M. Yung. “Scalable Protocols for Authenticated Group Key Exchange.” *J. Cryptology* 20(1): 85–113, 2007.
11. D. Boneh, R. Canetti, S. Halevi, and J. Katz. “Chosen-Ciphertext Security from Identity-Based Encryption.” *SIAM J. Computing* 36(5): 1301–1328, 2007.
12. J. Katz and M. Yung. “Characterization of Security Notions for Probabilistic Private-Key Encryption.” *J. Cryptology* 19(1): 67–96, 2006.
13. 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.
14. 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.
15. J. Katz. “Which Languages Have 4-Round Zero-Knowledge Proofs?” Accepted to *Journal of Cryptology* (pending minor revisions). One of 3 papers from TCC 2008 invited to the *Journal of Cryptology*.

16. 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).
17. J. Katz, P. MacKenzie, G. Taban, and V. Gligor. “Two-Server Password-Only Authenticated Key Exchange.” Submitted to *J. Cryptology*.
18. J. Katz, J.-S. Shin, and A. Smith. “Parallel and Concurrent Security of the HB and HB<sup>+</sup> Protocols.” Submitted to *IEEE Trans. Information Theory*.
19. S.D. Gordon, C. Hazay, J. Katz, and Y. Lindell. “Complete Fairness in Secure Two-Party Computation.” Submitted to *J. ACM*.
20. J. Katz, A. Sahai, and B. Waters. “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products.” One of 4 papers from Eurocrypt 2008 invited to the *Journal of Cryptology*.

### Articles in Refereed Conferences and Workshops

1. G. Fuchsbauer, J. Katz, and D. Naccache. “Efficient Rational Secret Sharing in Standard Communication Networks.” *7th Theory of Cryptography Conference, TCC 2010*, to appear.
2. J. Katz and V. Vaikuntanathan. “Signature Schemes with Bounded Leakage Resilience.” *Advances in Cryptology — Asiacrypt 2009*.
3. J. Katz and A. Yerukhimovich. “On Black-Box Constructions of Predicate Encryption Schemes from Trapdoor Permutations.” *Advances in Cryptology — Asiacrypt 2009*.
4. J. Katz and V. Vaikuntanathan. “Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices.” *Advances in Cryptology — Asiacrypt 2009*.
5. G. Ateniese, S. Kamara, and J. Katz. “Proofs of Storage from Homomorphic Identification Protocols.” *Advances in Cryptology — Asiacrypt 2009*.
6. M. Albrecht, C. Gentry, S. Halevi, and J. Katz. “Attacking Cryptographic Schemes Based on ‘Perturbation Polynomials’.” *ACM Conf. Computer and Communications Security 2009*.
7. 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*.
8. D. Boneh, J. Katz, D. Freeman, and B. Waters. “Signing a Linear Subspace: Signatures for Network Coding.” *Public-Key Cryptography — PKC 2009*.
9. Y. Dodis, J. Katz, A. Smith, and S. Walfish. “Composability and On-Line Deniability of Authentication.” *6th Theory of Cryptography Conference, TCC 2009*.

10. S.D. Gordon and J. Katz. “Complete Fairness in Multi-Party Computation Without an Honest Majority.” *6th Theory of Cryptography Conference, TCC 2009*.
11. 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) 2008*.
12. S.D. Gordon, C. Hazay, J. Katz, and Y. Lindell. “Complete Fairness in Secure Two-Party Computation.” *ACM Symposium on Theory of Computing (STOC) 2008*.
13. J. Katz, A. Sahai, and B. Waters. “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products.” *Advances in Cryptology — Eurocrypt 2008*. **One of four papers invited to a special issue of *J. Cryptology*.**
14. S. Kamara and J. Katz. “How to Encrypt with a Malicious Random Number Generator.” *Fast Software Encryption — FSE 2008*.
15. J. Katz and Y. Lindell. “Aggregate Message Authentication Codes.” *RSA Conference — Cryptographers’ Track 2008*.
16. J. Katz. “Bridging Cryptography and Game Theory: Recent Results and Future Directions” (invited paper). *5th Theory of Cryptography Conference, TCC 2008*.
17. J. Katz. “Which Languages Have 4-Round Zero-Knowledge Proofs?” *5th Theory of Cryptography Conference, TCC 2008*. **One of three papers invited to a special issue of *J. Cryptology*.**
18. V. Goyal and J. Katz. “Universally-Composable Computation with an Unreliable Common Reference String.” *5th Theory of Cryptography Conference, TCC 2008*.
19. J. Katz. “Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise” (invited paper). *11th IMA International Conference on Cryptography and Coding Theory*, pp. 1–15, Lecture Notes in Computer Science vol. 4887, Springer, 2007.
20. 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)*, 2007.
21. 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.
22. R. Morselli, B. Bhattacharjee, J. Katz, and M. Marsh. “Exploiting Approximate Transitivity of Trust” (invited paper). *IEEE BroadNets 2007, 4th Intl. Conf. on Broadband Communications, Networks, and Systems*.
23. 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.

24. 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.
25. 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.
26. 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 2007*, pp. 323–341, Lecture Notes in Computer Science vol. 4391, Springer, 2007.
27. S.D. Gordon and J. Katz. “Rational Secret Sharing, Revisited.” *Security and Cryptography for Networks, SCN 2006*, pp. 229–241, Lecture Notes in Computer Science vol. 4116, Springer, 2006. An extended abstract of this work also appeared at *NetEcon 2006*.
28. 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.
29. 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.
30. 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.
31. J. Katz and J.S. Shin. “Parallel and Concurrent Security of the HB and HB<sup>+</sup> Protocols.” *Advances in Cryptology — Eurocrypt 2006*, pp. 73–87, Lecture Notes in Computer Science vol. 4004, Springer, 2006.
32. A. Bender, J. Katz, and R. Morselli. “Ring Signatures: Stronger Definitions, and Constructions without Random Oracles.” *3rd Theory of Cryptography Conference, TCC 2006*, pp. 60–79, Lecture Notes in Computer Science vol. 3876, Springer, 2006.
33. 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.
34. 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.
35. 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.

36. 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.
37. 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.
38. 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*.**
39. R. Canetti, S. Halevi, and J. Katz. “Adaptively-Secure, Non-Interactive Public-Key Encryption.” *2nd Theory of Cryptography Conference, TCC 2005*, pp. 150–168, Lecture Notes in Computer Science vol. 3378, Springer, 2005.
40. J. Katz and Y. Lindell. “Handling Expected Polynomial-Time Strategies in Simulation Based Security Proofs.” *2nd Theory of Cryptography Conference, TCC 2005*, pp. 128–149, Lecture Notes in Computer Science vol. 3378, Springer, 2005.
41. Y. Dodis and J. Katz. “Chosen-Ciphertext Security of Multiple Encryption.” *2nd Theory of Cryptography Conference, TCC 2005*, pp. 188–209, Lecture Notes in Computer Science vol. 3378, Springer, 2005.
42. 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.
43. J. Katz, R. Ostrovsky, and M.O. Rabin. “Identity-Based Zero Knowledge.” *Security in Communication Networks, SCN 2004*, pp. 180–192, Lecture Notes in Computer Science vol. 3352, Springer, 2004.
44. 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.
45. 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.
46. 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.
47. 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.

48. R. Morselli, B. Bhattacharjee, J. Katz, and P. Keleher. “Trust-Preserving Set Operations.” *Proc. IEEE INFOCOM 2004*, vol. 4, pp. 2231–2241, IEEE, 2004.
49. 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.
50. 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.
51. 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.
52. 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.
53. 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.
54. 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.
55. 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.
56. 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.
57. 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.
58. 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.
59. Y. Dodis, J. Katz, S. Xu, and M. Yung. “Strong Key-Insulated Signature Schemes.” *Public-Key Cryptography — PKC 2003*, pp. 130–144, Lecture Notes in Computer Science vol. 2567, Springer, 2003.
60. J. Katz, R. Ostrovsky, and M. Yung. “Forward Secrecy in Password-Only Key-Exchange Protocols.” *Security in Communication Networks, SCN 2002*, pp. 29–44, Lecture Notes in Computer Science vol. 2576, Springer, 2002.

61. 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.
62. 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.
63. 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.
64. E. Buonanno, J. Katz, and M. Yung. “Incremental and Unforgeable Encryption.” *Fast Software Encryption — FSE 2001*, pp. 109–124, Lecture Notes in Computer Science vol. 2355, Springer, 2002.
65. 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.
66. 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.
67. 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.
68. 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.
69. J. Katz and M. Yung. “Unforgeable Encryption and Chosen-Ciphertext-Secure Modes of Operation.” *Fast Software Encryption — FSE 2000*, pp. 284–299, Lecture Notes in Computer Science vol. 1978, Springer, 2001.
70. 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.
71. 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.