
Adam Davison Smith

<http://www.cse.psu.edu/~asmith>

RESEARCH INTERESTS

Cryptography, Data Privacy, Quantum Computing, Theoretical Computer Science.

EDUCATION

- ◇ Ph.D. in Computer Science — **Massachusetts Institute of Technology** September 2004
Thesis: *Maintaining Secrecy when Information Leakage is Unavoidable*
- ◇ S.M. in Computer Science — **Massachusetts Institute of Technology** September 2001
Thesis: *Multi-party Quantum Computation*
- ◇ B.Sc. in Mathematics and Computer Science — **McGill University** June 1999
Joint Honours, Governor General's Medal

EMPLOYMENT

- ◇ **Associate Professor, Pennsylvania State University** July 2010–present
- ◇ Assistant Professor, Pennsylvania State University January 2007–June 2010
- ◇ Visiting Scientist, Institute for Pure and Applied Mathematics, UCLA Fall 2006
- ◇ Visiting Scientist, Massachusetts Institute of Technology Spring 2006
- ◇ Post-doctoral Fellow, Weizmann Institute of Science, Israel September 2004–August 2006
- ◇ Graduate Research Assistant, Massachusetts Institute of Technology 1999–2004
- ◇ Research Intern, Microsoft Research Summer 2002–Summer 2003
- ◇ Research Intern, Telcordia Technologies Summer 2000
- ◇ Research Assistant, McGill University Summer 1998–Summer 1999

AWARDS & SCHOLARSHIPS

- ◇ *US Presidential Early Career Award for Scientists and Engineers (PECASE)*, 2009.
- ◇ US National Science Foundation *CAREER* Award, 2008.
- ◇ Runner-up, *2006 Privacy-Enabling Technology Award* for the paper “Calibrating Noise to Sensitivity in Private Data Analysis”.
- ◇ *Microsoft Graduate Fellowship*, 2003-2004.
- ◇ *NTT Entrance Fellowship*, Massachusetts Institute of Technology, 1999-2000.
- ◇ *1999 Governor General's Bronze Medal* (best cumulative GPA in Faculty of Science), McGill University.
- ◇ Scholarships while at McGill University: 1999 Edward Rosenthal Mathematics Prize, 1998 SHL Systemhouse President's Award, 1998 and 1997 Corporate Software & Technology Scholarships, 1998 H.J. Brennan Mathematics Scholarship, 1997 Edward Beatty Memorial Mathematics Scholarship, 1996 Edwards Woods Entrance Scholarship.

TEACHING EXPERIENCE

Instructor for

- ◇ Algorithms and Data Structures (undergraduate), Penn State Spring 2007, Fall 2009
- ◇ Cryptography (graduate), Penn State Fall 2007, Spring 2009, Spring 2011
- ◇ Analysis of Algorithms (graduate), Penn State Fall 2008, Fall 2010
- ◇ Theoretical Computer Science Seminar, Penn State Spring 2008, Spring 2009
- ◇ Privacy in Statistical Databases, Penn State Fall 2007, Spring 2010
- ◇ Privacy in Statistical Databases, Weizmann Institute of Science Spring 2005

Teaching Assistant for

- ◇ Cryptography, Massachusetts Institute of Technology Fall 2000
- ◇ Advanced Calculus, Algebra, Programming Languages, McGill University Fall 1997–Spring 1999

STUDENT ADVISING

- ◇ Srivatsava Ranjit Ganta (co-advised with Raj Acharya), Ph.D. October 2008.
- ◇ Laxman Vembar, M.S. September 2008.
- ◇ Ashwinkumar Gopalrathnam, M.S. (Electrical Engineering) September 2008.
- ◇ Abhradeep Guha Thakurta, Ph.D. expected May 2012.

PROFESSIONAL ACTIVITIES

- ◇ Conference organization
 - Organizer, Workshop on *Statistical and Learning-Theoretic Challenges in Data Privacy*, Institute for Pure and Applied Mathematics, UCLA, February 2010.
- ◇ Program committee chair for
 - *Information-theoretic Security (ICITS) 2012*, Montreal, Canada, August 2012.
- ◇ Program committee member for
 - *Foundations of Computer Science (FOCS) 2011*, Palm Springs, CA, October 2011.
 - *Crypto 2011*, Santa Barbara, CA, August 2011.
 - *Information-theoretic Security (ICITS) 2011*, Amsterdam, The Netherlands, May 2011.
 - *Privacy-Enhancing Technologies (PETS) 2011*, Waterloo, Canada, July 2011.
 - *IEEE Security and Privacy 2010*, Oakland, CA, May 2010.
 - *Theory of Cryptography Conference (TCC) 2010*, Zurich, Switzerland, February 2010.
 - *Crypto 2009*, Santa Barbara, CA, August 2009.
 - *Cryptography and Network Security 2009*, Santa Barbara, CA, August 2009.
 - *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, January 2009.
 - *SCN 2008*, Amalfi, Italy, September 2008.
 - *Crypto 2008*, Santa Barbara, CA, August 2008.
 - *RSA Conference, Cryptographer's Track (CT-RSA) 2008*, San Francisco, CA, February 2008.
 - *Crypto 2007*, Santa Barbara, CA, August 2007.
 - *ACM Conference on Electronic Commerce (EC) 2007*, San Diego, CA, June 2007.

- *RSA Conference, Cryptographer’s Track (CT-RSA) 2007*, San Francisco, CA, February 2007.
- *Formal and Computational Cryptography Workshop (FCC) 2006*, Venice, Italy, June 2006.
- *Theory of Cryptography Conference (TCC) 2006*, New York, NY, March 2006.
- *Crypto 2005*, Santa Barbara, CA, August 2005.

- ◇ Associate editor, *Journal of Privacy and Confidentiality*.
- ◇ Reviewer for several journals and conferences: *Journal of the ACM*, *Journal of Cryptology*, *SIAM Journal on Computing*, *SIAM Journal on Discrete Mathematics*, *Journal of Quantum Information and Computing*, *Journal of Privacy Technology*, *ACM Transactions on Algorithms*, *Physics Letters A*, *IEEE Transactions on Information Theory*, *FOCS*, *STOC*, *Crypto*, *Eurocrypt*, *SODA*, *TCC*, *Random*.

EXTERNAL FUNDING

- ◇ US National Science Foundation Award #0941553. *CDI Type II: Integrating Computational and Statistical Approaches to Data Privacy*, co-PI, Fall 2010–2014, \$2,000,000.
- ◇ US National Science Foundation Award #0747294. *CAREER: Rigorous Foundations for Data Privacy*, PI, Fall 2008–2013, \$400,000. Received *PECASE*, 2009.
- ◇ US National Science Foundation Award #0729171. *TF: Algorithmic and Learning-Theoretic Aspects of Data Privacy*, PI, Fall 2007–2010, \$277,000.
- ◇ U.S Army Research Laboratory Collaborative Technology Alliance Award. *Quality-of Information-Aware Networks for Tactical Applications (QUANTA)*, co-PI, Fall 2009–2014, \$16,755,800.

PUBLICATIONS IN REFEREED JOURNALS (Note: By default, authors are listed in alphabetical order. Papers where the author order is based on contribution are marked with *.)

- ◇ S. P. Kasiviswanathan, H. Lee, K. Nissim, S. Raskhodnikova and A. Smith. What Can We Learn Privately? Accepted to *SIAM Journal on Computing*, 2009.
- ◇ S. Raskhodnikova, D. Ron, A. Shpilka and A. Smith. Strong Lower Bounds for Approximating Distribution Support Size and the Distinct Elements Problem. *SIAM Journal on Computing*, Vol. 39, No. 3, pp. 813–842, 2009.
- ◇ M. Naor, G. Segev and A. Smith. Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models. *IEEE Transactions on Information Theory*, Vol. 54, No. 6, pp. 2408–2425, 2008.
- ◇ Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM Journal on Computing*, Vol. 38, No. 1, 2008.
- ◇ J. Katz, J. S. Shin, A. Smith. Parallel and Concurrent Security of the HB and HB+ Protocols. *Journal of Cryptology*, Vol. 23, No. 3, p. 402–421, 2010.
- ◇ * M. Tomamichel, R. Renner, C. Schaffner, A. Smith. Leftover Hashing Against Quantum Side Information. Accepted to *IEEE Transactions on Information Theory*, 2011.

PUBLICATIONS IN REFEREED CONFERENCES (Note: By default, authors are listed in alphabetical order. Papers where the author order is based on contribution are marked with *.)

- ◇ S. Hallgren, A. Smith, F. Song. Classical Cryptographic Protocols in a Quantum World. In *Advances in Cryptology—CRYPTO 2011*, p. 295–313, August 2011.

- ◇ V. Karwa, S. Raskhodnikova, A. Smith, G. Yaroslavtsev. Private Analysis of Graph Structure. In *37th International Conference on Very Large Databases (PVLDB)*, August 2011.
- ◇ A. Smith. Privacy-preserving Statistical Estimation with Optimal Convergence Rates. In *43rd Annual ACM Symposium on the Theory of Computing (STOC)*, June 2010.
- ◇ V. Guruswami, A. Smith. Codes for Computationally Simple Channels: Explicit Constructions with Optimal Rate. In *51st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, p. 723–732, October 2010.
- ◇ E. Kiltz, A. O’Neill, A. Smith. Instantiability of RSA-OAEP under Chosen-Plaintext Attack. In *Advances in Cryptology—CRYPTO 2010*, p. 295–313, August 2010.
- ◇ R. Bhaskar, S. Laxman, A. Smith, A. G. Thakurta. Discovering Frequent Patterns in Sensitive Data. In *16th ACM SIGKDD Symp. Knowledge Discovery and Data Mining (KDD)*, p. 503–512, July 2010.
- ◇ S. Kasiviswanathan, M. Rudelson, A. Smith, J. Ullman. The Price of Privately Releasing Contingency Tables and the Spectra of Random Matrices with Correlated Rows. In *42nd Annual ACM Symposium on the Theory of Computing (STOC)*, p. 775–784, June 2010.
- ◇ Y. Dodis, J. Katz, A. Smith and S. Walfish. Composability and On-Line Deniability of Authentication. In *Theory of Cryptography Conference (TCC)*, p. 146–162, March 2009.
- ◇ S. P. Kasiviswanathan, H. Lee, K. Nissim, S. Raskhodnikova and A. Smith. What Can We Learn Privately? In *48th Annual Symposium on Foundations of Computer Science (FOCS)*, p. 531–540, October 2008.
- ◇ I. Damgård, Y. Ishai, M. Krøigaard, J. B. Nielsen, A. Smith: Scalable Multiparty Computation with Nearly Optimal Work and Resilience. In *Advances in Cryptology — CRYPTO 2008*, p. 241–261, August 2008.
- ◇ S. R. Ganta, S. P. Kasiviswanathan and A. Smith. Composition Attacks and Auxiliary Information in Data Privacy. In *14th ACM International Conference on Knowledge Discovery and Data Mining (KDD)*, p. 531–540, August 2008.
- ◇ V. Goyal, P. Mohassel and A. Smith. Efficient Two- and Multi-party Computation Protocols for Covert Adversaries. In *Advances in Cryptology — EUROCRYPT 2008*, p. 289–306, April 2008.
- ◇ * W. Enck, K. Butler, T. Richardson, P. McDaniel and A. Smith. Defending Against Attacks on Main Memory Persistence. In *24th Annual Computer Security Applications Conference (ACSAC)*, p. 65–74, December 2008.
- ◇ S. Raskhodnikova, D. Ron, A. Shpilka and A. Smith. Strong Lower Bounds for Approximating Distribution Support Size and the Distinct Elements Problem. In *47th Annual Symposium on Foundations of Computer Science (FOCS)*, p. 559–569, October 2007.
- ◇ S. Raskhodnikova, D. Ron, R. Rubinfeld and A. Smith. Sublinear Algorithms for Approximating String Compressibility. In *11th International Workshop on Randomization and Computation (RANDOM)*, August 2007.
- ◇ K. Nissim, S. Raskhodnikova and A. Smith. Smooth Sensitivity and Sampling in Private Data Analysis. In *39th Annual ACM Symposium on Theory of Computing (STOC)*, June 2007, pp. 75–84.
- ◇ A. Smith. Scrambling Errors Using Few Random Bits: Optimal Information Reconciliation and Better Private Codes. In *18th Annual ACM Symposium on Discrete Algorithms (SODA)*, January 2007, pp. 472–479.
- ◇ M. Ben-Or, C. Crpeau, D. Gottesman, A. Hassidim, and A. Smith. Secure Multiparty Quantum Computation with (Only) a Strict Honest Majority. In *47th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, October 2006, pp. 249–260.

- ◇ M. Naor, G. Segev and A. Smith. Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models. In *Advances in Cryptology — CRYPTO 2006*, August 2006, Springer LNCS 4117, pp. 214–231.
- ◇ Y. Dodis, J. Katz, L. Reyzin and A. Smith. Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets. In *Advances in Cryptology — CRYPTO 2006*, August 2006, Springer LNCS 4117, pp. 232–250.
- ◇ C. Dwork, F. McSherry, K. Nissim and A. Smith. Calibrating Noise to Sensitivity in Private Data Analysis. In *Theory of Cryptography 2006*, March 2006, Springer LNCS 3876, pp. 265–284.
- ◇ X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky and A. Smith. Secure Remote Authentication Using Biometrics. In *Advances in Cryptology — EUROCRYPT 2005*, May 2005, Springer LNCS 3494, pp. 147–163.
- ◇ S. Chawla, C. Dwork, F. McSherry, A. Smith and H. Wee. Toward Privacy in Public Databases. In *Theory of Cryptography Conference (TCC)*, Cambridge, MA, February 2005, Springer LNCS 3378, pp. 363–385.
- ◇ C. Crépeau, D. Gottesman and A. Smith. Approximate Quantum Error-Correcting Codes and Secret-Sharing Schemes. In *Advances in Cryptology — EUROCRYPT 2005*, Springer LNCS 3494, May 2005, pp. 285–301.
- ◇ Y. Dodis and A. Smith. Correcting Errors Without Leaking Partial Information. In *37th Annual ACM Symposium on Theory of Computing (STOC)*, May 2005, pp. 654–663.
- ◇ Y. Dodis and A. Smith. Entropic Security and the Encryption of High Entropy Messages. In *Theory of Cryptography 2005*, Cambridge, MA, February 2005, Springer LNCS 3378, pp. 556–577.
- ◇ A. Ambainis and A. Smith. Small Pseudo-Random Families of Matrices: Derandomizing Approximate Quantum Encryption. In *8th International Workshop on Randomization and Computation (RANDOM)*, August 2004, Springer LNCS 3122, pp. 249–260.
- ◇ Y. Dodis, L. Reyzin and A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *Advances in Cryptology — EUROCRYPT 2004*, May 2004, Springer LNCS 3027, pp. 523–540. Updated version available as IACR Eprint 2003/235.
- ◇ C. Dwork, R. Shaltiel, A. Smith and L. Trevisan. List-Decoding of Linear Functions and Analysis of a Two-Round Zero-Knowledge Argument. In *Theory of Cryptography 2004*, February 2004, Springer LNCS 2951, pp. 101–120.
- ◇ R. Ostrovsky, C. Rackoff and A. Smith. Efficient Consistency Proofs for General Queries on a Committed Database. In *31st International Colloquium on Automata, Languages and Complexity (ICALP)*, Turku, Finland, July 2004, Springer LNCS 3142, pp. 1041–1053.
- ◇ J. Katz, R. Ostrovsky, and A. Smith. Round Efficiency of Multi-party Computation with a Dishonest Majority. In *Advances in Cryptology — EUROCRYPT 2003*, May 2003, Springer LNCS 2656, pp. 578–595.
- ◇ C. Peikert, A. Shelat and A. Smith. Lower Bounds for Collusion-Secure Fingerprinting. In *14th Annual ACM Symposium on Discrete Algorithms (SODA)*, January 2003, pp. 472–479.
- ◇ A. Ambainis, A. Smith and K. Yang. Extracting Quantum Entanglement. In *17th Annual IEEE Conference on Computational Complexity (CCC)*, May 2002, pp. 103–112.
- ◇ H. Barnum, C. Crépeau, D. Gottesman, A. Smith and A. Tapp. Authentication of Quantum Messages. In *42nd Annual Symposium on Foundations of Computer Science (FOCS)*, November 2002, pp. 449–458.
- ◇ M. Fitz, D. Gottesman, M. Hirt, T. Holenstein and A. Smith. Detectable Byzantine Agreement Secure Against Faulty Majorities. In *21st Annual ACM Symposium on Principles of Distributed Computing (PODC)*, July 2002, pp. 118–126.

- ◇ C. Crépeau, D. Gottesman and A. Smith. Secure Multi-party Quantum Computation. In *34th Annual ACM Symposium on Theory of Computing (STOC)*, May 2002, pp. 643–652.
- ◇ G. Di Crescenzo, J. Katz, R. Ostrovsky and A. Smith. Efficient and Non-interactive Non-malleable Commitment. In *Advances in Cryptology — EUROCRYPT 2001*, May 2001, Springer LNCS 2045, pp. 40–59. Also available as IACR Eprint 2001/032.
- ◇ Y. Dodis, A. Sahai and A. Smith. On Perfect and Adaptive Security in Exposure-Resilient Cryptography. In *Advances in Cryptology — EUROCRYPT 2001*, May 2001, Springer LNCS 2045, pp. 301–324.
- ◇ M. Liskov, A. Lysyanskaya, S. Micali, L. Reyzin and A. Smith. Mutually Independent Commitments. In *Advances in Cryptology — ASIACRYPT 2001*, December 2001, Springer LNCS 2248, pp. 385–401.

NON-REFEREED INVITED PAPERS

- ◇ A. Smith. What Can Cryptography Do for Coding Theory? In *International Conference on Cryptography and Network Security (CANS)*, December 2009.
- ◇ A. Smith. Integrating Differential Privacy with Statistical Theory. In *International Conference on Information-theoretic Security (ICITS)*, December 2009.

BOOK CHAPTERS

- ◇ Y. Dodis, L. Reyzin and A. Smith. Fuzzy Extractors. In P. Tuyls, editor, *Security with Noisy Data*, Springer-Verlag, 2008.

TALKS AND PRESENTATIONS

Invited Conference (Plenary) Presentations:

- ◇ *Cryptography and Network Security Conference 2009*, Kanazawa, Japan, December 2009.
- ◇ *International Conference on Information-Theoretic Security 2009*, Shizuoka, Japan, December 2009.

Invited Tutorials:

- ◇ *Pinning Down Privacy*
- DIMACS Workshop on Data Privacy, Rutgers University, February 2008.

Invited Seminar and Workshop Presentations:

- ◇ *Integrating Differential Privacy with Statistical Theory*
- Computer Science Colloquium, Cornell University, Ithaca, NY, September 2011.
- Department of Statistics Colloquium, Carnegie-Mellon University, Pittsburgh, PA, March 2010.
- Computer Science Colloquium, University of Massachusetts at Amherst, March 2010.
- Eastern Great Lakes Workshop on Theoretical Computer Science, Buffalo, NY, October 2009.
- ◇ *Codes for Computationally Simple Channels*
- *Information Theory Workshop (ITW)*, Dublin, Ireland, September 2010.
- ◇ *Lower Bounds on Data Privacy*
- Algorithms & Combinatorics Seminar, Carnegie Mellon University, September 2009.

- ◇ *Pinning Down Privacy*
 - Steklov Institute, Saint-Petersburg, Russia, June 2009. - DIMACS Workshop on Internet Privacy: Facilitating Seamless Data Movement with Appropriate Controls, Rutgers University, September 2008.
 - Google Research, New York, NY, March 2008.
 - Department of Statistics Colloquium, Penn State, January 2008.
 - Workshop on Data Privacy, Weizmann Institute of Science, Israel, July 2006.
- ◇ *What Can We Learn Privately?*
 - MIT Cryptography and Information Security Seminar, February 2008.
 - Microsoft-CMU Mindswap on Data Privacy, Pittsburgh, PA, October 2007.
- ◇ *Calibrating Noise to Sensitivity in Private Data Analysis*
 - C.S.-Statistics Workshop on Privacy and Confidentiality, Bertinoro, Italy, July 2005.
 - Tel Aviv University, Israel, January 2006.
 - Simon Fraser University, Canada, February 2006.
 - Federal Institute of Technology (ETH), Zürich, Switzerland, March 2006.
 - Harvard University, March 2006.
 - Massachusetts Institute of Technology, March 2006.
 - California Institute of Technology, December 2006.
 - Penn State University, January 2007.
 - Carnegie Mellon University, April 2007.
- ◇ *Cryptography with Quantum Data*
 - IPAM Workshop on Foundations of Zero-Knowledge and Multi-party Computation, UCLA, November 2006.
 - Perimeter Institute for Theoretical Physics, Canada, June 2007.
- ◇ *Interaction and Local Storage in Private Data Analysis*
 - IPAM Workshop on Locally Decodable Codes and Privacy-Preserving Data Mining, UCLA, October 2006.
- ◇ *Cryptography with Noisy Secrets*
 - Microsoft Research SVC, Mountain View, CA, May 2005.
 - University of British Columbia, Canada, February 2006.
 - Penn State University, February 2006.
 - Bell Labs (Lucent Technologies), NJ, March 2006.
 - University of Waterloo, Canada, March 2006.
 - University of Michigan, Ann Arbor, March 2006.
 - SRI (Stanford Research Institute) International, Menlo Park, CA, March 2006.
- ◇ *Evolving Notions of Security for Quantum Protocols* (tutorial presentation)
 - Classical and Quantum Information Security Workshop, Pasadena, CA, December 2005.
- ◇ *Correcting Errors without Leaking Partial Information*
 - Haifa University, Haifa, Israel, March 2005.
 - Technion (Israel Institute of Technology), Haifa, Israel, March 2005.
 - Weizmann Institute of Science, Rehovot, Israel, April 2005.
 - Princeton University, May 2005.
- ◇ *Toward Privacy in Public Databases*
 - Workshop on Secure Multiparty Protocols, Amsterdam, The Netherlands, October 2004.
 - Ben-Gurion University, Israel, November 2004.
 - Tel-Aviv University, Israel, November 2004.

- Hebrew University of Jerusalem, Israel, January 2005.
- Boston University, February 2005.
- New York University, February 2005.
- ◇ *Fuzzy Extractors: Generating Strong Keys from Biometric Data*
 - University of Waterloo, Canada, February 2004.
 - Toyota Technological Institute, Chicago, IL, March 2004.
 - Intel Research, Berkeley, CA, March 2004.
 - University of Victoria, Canada, March 2004.
 - DIMACS Workshop on Data Privacy, March 2004.
 - Tel-Aviv University, Israel, April 2004.
 - University of Montreal, Canada, May 2004.
 - University of Toronto, Canada, May 2004.
 - Bar-Ilan University, Israel, March 2005.
- ◇ *Secrecy of High-Entropy Sources — Protecting All Partial Information*
 - MIT Cryptography and Information Security Seminar, September 2003.
 - McGill University, October 2003.
 - Weizmann Institute of Science, Israel, November 2003.
 - Hebrew University of Jerusalem, Israel, November 2003.
 - Tel-Aviv University, Israel, November 2003.
- ◇ *Round Efficiency of Multi-party Computation with a Dishonest Majority*
 - Massachusetts Institute of Technology, December 2002.
- ◇ *List-Decoding and Two-Round Zero-Knowledge*
 - Microsoft Research SVC, Mountain View, CA, August 2002.
- ◇ *Detectable Byzantine Agreement Secure Against a Faulty Majority*
 - Microsoft Research SVC, Mountain View, CA, July 2002.
- ◇ *Secure Multi-party Quantum Computation,*
 - *Workshop on Quantum Cryptography*, NEC Research, Princeton, NJ, December 1999.
 - *Quantum Information Processing*, Yorktown Heights, NY, January 2002.
 - *Barbados Workshop on Quantum Cryptography*, Barbados, May 2002.
- ◇ *Efficient and Non-Interactive Non-Malleable Commitment*
 - McGill University, December 2001.
- ◇ *Range Queries on a Committed Database*
 - Telcordia Technologies, NJ, August 2000.
- ◇ *On Perfect and Adaptive Security in Exposure-Resilient Cryptography.*
 - Telcordia Technologies, NJ, July 2000.
- ◇ *Quantum and Classical Secret-Sharing*
 - Massachusetts Institute of Technology, December 1999.

Conference Presentations:

- ◇ *Privacy-preserving Statistical Estimators with Optimal Convergence Rates*
 - *STOC 2011*, San Jose, CA, 2011.
- ◇ *Codes for Computationally Simple Channels*
 - *FOCS 2010*, Las Vegas, NV, 2010.
- ◇ *Integrating Differential Privacy with Statistical Theory*
 - *American Statistical Association Joint Statistical Meetings*, Washington, DC, 2009.

- ◇ *Strong Lower Bounds for Distribution Support Size and String Compressibility*
- *IEEE Symposium on the Foundations of Computer Science (FOCS) 2007*, Providence, RI, October 2007.
- ◇ *Scrambling Adversarial Errors Using Few Random Bits*
- *ACM-SIAM Symposium on Discrete Algorithms*, New Orleans, LA, January 2007.
- ◇ *Calibrating Noise to Sensitivity in Private Data Analysis*
- *Theory of Cryptography Conference (TCC) 2006*, New York, NY, March 2006.
- ◇ *Correcting Errors without Leaking Partial Information*
- *ACM Symposium on the Theory of Computing (STOC)*, Baltimore, MD, May 2005.
- ◇ *Entropic Security and the Encryption of High Entropy Messages*
- *Theory of Cryptography Conference (TCC) 2005*, Cambridge, MA, February 2005.
- ◇ *Small Pseudo-Random Families of Matrices and Approximate Quantum Encryption*
- *8th International Workshop on Randomization and Computation (RANDOM)*, August 2004.
- ◇ *List-Decoding of Linear Codes and Two-Round Zero-Knowledge Arguments*
- *Theory of Cryptography Conference (TCC) 2004*, Cambridge, MA, February 2004.
- ◇ *Round Efficiency of Multi-party Computation with a Dishonest Majority*
- *Advances in Cryptology — Eurocrypt 2003*, May 2003.
- ◇ *Detectable Byzantine Agreement Secure Against a Faulty Majority*
- *ACM Symposium on the Principles of Distributed Computing (PODC)*, July 2002.
- ◇ *Secure Multi-party Quantum Computation*,
- *ACM Symposium on the Theory of Computing (STOC)*, May 2002.
- ◇ *On Perfect and Adaptive Security in Exposure-Resilient Cryptography*
- *Advances in Cryptology — Eurocrypt 2001*, May 2001.