Adam Davison Smith

Curriculm vitae, updated May 11, 2022

http://cs-people.bu.edu/ads22

ads22@bu.edu

Research Interests

Data privacy, Cryptography, Information theory, Machine learning, Quantum computing, Theoretical computer science, Computer security.

Education

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

Employment

- **Professor of Computer Science**, **Boston University** — 2017–present
- Professor of Computer Science and Engineering, Pennsylvania State University — July 2016–July 2017
- Associate Professor, Pennsylvania State University — July 2010–June 2016
- 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
  Mentor: Moni Naor

Awards

- ACM **Paris Kanellakis Theory and Practice Award**, joint with A. Blum, I. Dinur, C. Dwork, F. McSherry, K. Nissim). May 2022.
- ACM Fellow. Awarded January 2021.
- Eurocrypt Test of Time Award, 2019. Awarded to *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data* (*Eurocrypt* 2004, *SICOMP* 2008)
- **Gödel Prize, 2017**. Awarded annually to an "outstanding paper in the area of theoretical computer science". Awarded for *Calibrating Noise to Sensitivity in Private Data Analysis* (*TCC* 2006, *JPC* 2016).
- Theory of Cryptography Test of Time Award, 2016. Awarded to a paper published at the TCC Conference at least eight years before the award. Awarded to *Calibrating Noise to Sensitivity in Private Data Analysis* (*TCC* 2006) "for introducing the definition of differential privacy, and providing a solid mathematical foundation for a vast body of subsequent work on private data analysis."

- ◇ Presidential Early Career Award for Scientists and Engineers (PECASE), 2009. Awarded yearly to 100 junior scientists and engineers. My award was one of 20 (across all areas of science) sponsored by the National Science Foundation.
- ◇ 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.
- ◇ 1999 Governor General's Bronze Medal (highest GPA, Faculty of Science), McGill University.

TEACHING

- ◇ Privacy in Machine Learning and Statistical Inference (`http://dpcourse.github.io`) Fall 18, Spring 2021
- ◇ Introduction to the Analysis of Algorithms (at BU) Fall 2019, Fall 2020
- ◇ Algorithms in Society Spring 2020
- ◇ Computational Tools for Data Science Spring 2018
- ◇ Adaptive Data Analysis (`http://adaptivedataanalysis.com`) Fall 2017
- ◇ Algorithms and Data Structures (undergraduate) Spring 2007, Fall 2009, Spring 2012, Spring 2017
- ◇ Analysis of Algorithms (graduate) Fall 2008, Fall 2010, Fall 2014, Fall 2015
- ◇ Computational Tools for Data Science Spring 2018
- ◇ Cryptography (graduate) Fall 2007, Spring 2009, Spring 2011, Spring 2016
- ◇ Privacy in Statistical Databases (graduate) Fall 2007, Spring 2010, Fall 2012, Spring 2015
- ◇ Probabilistic Algorithms Fall 2016
- ◇ Pseudorandomness (graduate) Fall 2011
- ◇ TCS Seminar Spring 2008, Spring 2009, Fall 2012, Fall 2015, Spring 2016
- ◇ Privacy in Statistical Databases (graduate), Weizmann Institute of Science Spring 2005

Department-level teaching awards while at Penn State

- ◇ Spring 2015 Faculty Teaching Award
- ◇ 2012-2013 Joel and Ruth Spira Award for Teaching Excellence

GRADUATE STUDENTS

- ◇ Srivatsava Ranjit Ganta (co-advised with Raj Acharya), Ph.D. October 2008. Currently at Oracle.
- ◇ Laxman Vembar, M.S. September 2008.
- ◇ Ashwinkumar Gopalrathnam, M.S. (Electrical Engineering) September 2008.
- ◇ Abhradeep Guha Thakurta, Ph.D. May 2013. Currently assistant professor at University of California, Santa Cruz, on leave at Google.
- ◇ Megan Heysham, M.S. August 2013. Currently at Hitachi.
- ◇ Ye Zhang, Ph.D. June 2015. Currently at Google.
- ◇ Om Thakkar, Ph.D. August 2019. Currently at Google.
- ◇ Jiayu Zhang, Ph.D. 2021. Currently Currently a postdoc at Caltech.

◇ Gavin Brown, Ph.D. expected 2022.

◇ Marika Swanberg, Ph.D. expected 2024.

◇ Palak Jain, Ph.D. expected 2024.

POSTDOCTORAL FELLOWS

◇ Raef Bassily, September 2012–2015. Currently: tenure-track faculty at Ohio State.

◇ Jalaj Upadhyay, September 2015–August 2017. Currently: researcher at Apple.

◇ Audra McMillan, July 2018–June 2020. Currently: researcher at Apple.

EXTERNAL FUNDING

◇ US National Science Foundation Award CNS-2120667. *Foundations for the Next Generation of Private Learning Systems*. Role: PI for BU. Other PIs: Jonathan Ullman, Roxana Geambasu, Steven Wu. BU Portion: $100,000. Total award: $500,000.

◇ Apple Faculty Award. Role: PI (50%). Co-PI: Mark Bun. Spring 2021–2023, $100,000.

◇ Google Faculty Award. Role: PI (100%). Fall 2020–2022, $50,000.

◇ US Census Bureau Collaborative Research Agreement. *Towards an End-to-end Approach to Formal Privacy for Sample Surveys.* Role: co-PI (%33 for BU). PI: Marco Gaboardi. Fall 2020–2024. BU portion: $1.5 million. Total award: $3 million.

◇ US National Science Foundation Award CCF-1763786. *AF: Medium: Foundations of Adaptive Data Analysis.* Role: PI for BU. Other PIs: Cynthia Dwork, Aaron Roth, Weijie Su, James Zou. June 2018-2021, $260,000.

◇ US Census Bureau Collaborative Research Agreement. PI for Penn State (100%), $400,000. Lead institution: Georgetown University (PI: Kobbi Nissim).

◇ Google Faculty Research Award. *Privacy-preserving Deep Learning*. Role: Co-PI (50%). PI: Vitaly Shmatikov (Cornell). Fall 2016–2018, $60,000.

◇ Sloan Foundation Research Award. Practical Algorithms for Interactive Private Data Analysis, with Applications to False Discovery Control. Role: Co-PI (50%). PI: Aaron Roth. Fall 2015–2018, $494,015.

◇ US National Science Foundation Award #1447700. *BIGDATA: F: DKA: Scalable, Private Algorithms for Continual Data Analysis*. Role: PI (50%). Co-PI: Sofya Raskhodnikova. Fall 2014–2018, $500,000.

◇ Google Faculty Research Award. Detailed Streaming Analytics: Privacy Measurement and Algorithms. Co-PI (50%). PI: Daniel Kifer. Fall 2013–2015, $256,000.

◇ US National Science Foundation Award #1057312. *Workshop on Trustworthy Computing Program* , Role: PI (50%). Co-PI: Trent Jaeger. Fall 2010–2012, $225,814.

◇ US National Science Foundation Award #0941553. *CDI Type II: Integrating Computational and Statistical Approaches to Data Privacy*, Role: Co-PI (33%). PI: Aleksandra Slavkovic. Co-PIs: John Abowd, Stephen Fienberg, Sofya Raskhodnikova. Fall 2010–2014, $1,025,626.

◇ US National Science Foundation Award #0747294. *CAREER: Rigorous Foundations for Data Privacy*, Role: PI, Fall 2008–2014, $400,000. Received *PECASE*, 2009.

◇ US National Science Foundation Award #0729171. *TF: Algorithmic and Learning-Theoretic Aspects of Data Privacy*, Role: PI (50%). Co-PI: Sofya Raskhodnikova. Fall 2007–2010, $277,000.

◇ US Army Research Laboratory Collaborative Technology Alliance Award. *Quality-of Information-Aware Networks for Tactical Applications (QUANTA)*. Role: Co-PI. PI: Thomas La Porta. Fall 2009–2014.

◇ US National Institutes of Health. *Penn State Clinical and Translational Science Institute*. Role: Senior personnel. PI: Lawrence Sinoway. June 2011–June 2013.

PROFESSIONAL ACTIVITIES

◇ Community service and outreach:

- Member, *Committee for the Advancement of Theoretical Computer Science*, 2021–present

◇ Associate editor:

– *Journal of Cryptology*, 2021–present.
– *Journal of Privacy and Confidentiality*, 2012–present.
– *IEEE Transactions on Information Theory*, 2011-2014
– Guest editor, *SIAM Journal on Computing* special issue for *STOC 2014* selected papers.

◇ Program Chair:

– *Theory of Cryptography Conference (TCC 2016-B)*, Beijing, China, November 2016 (co-chaired with Martin Hirt).
– *International Conference on Information-Theoretic Security (ICITS) 2012*, Montreal, Canada, August 2012.

◇ General chair:

– *Information-theoretic Cryptography Conference* (ITC), held virtually, June 2020.

◇ Program committee member:

– Senior program committee, *Algorithmic Learning Theory (ALT 2022)*, virtual, March 2022.
– *Conference for Failed Approaches and Insightful Losses in Cryptology (CFAIL) 2022*, August 2022.
– Area chair, *Conference on Learning Theory (COLT) 2021*, virtual, June 2021.
– *Foundations of Responsible Computing (FORC)* Conference, virtual, June 2021.
– *International Conference on Learning Representations (ICLR)*, 2021.
– NeurIPS workshop on Privacy-preserving Machine Learning (*PPML 2020*), virtual event associated with *NeurIPS 2020*.
– Area chair, *Conference on Learning Theory (COLT) 2020*, virtual.
– *Foundations of Responsible Computing (FORC) 2020* Conference, virtual.
– *Eurocrypt 2020*, Zagreb, Croatia, May 2020.
– *FAT* 2020*, Barcelona, Spain, January 2020.
– Area Chair for privacy, *ACM Symposium on Computer and Communications Security (CCS)*, 2019
– *IEEE Symposium on Security and Privacy ("Oakland")*, 2018.
– *Innovations in Theoretical Computer Science (ITCS) 2016*, Boston, MA, January 2016.
– *Theory of Cryptography (TCC) 2016-A*, Tel Aviv, Israel, January 2016.
– *16th Privacy Enhancing Technologies Symposium 2016*, July 2016.
– *15th Privacy Enhancing Technologies Symposium 2015*, July 2015.
– *Neural Information Processing Systems (NIPS) 2014*, Montreal, Canada, December 2014.
– *ACM Symposium on the Theory of Computing (STOC) 2014*, New York, NY, June 2014.
– *Theory of Cryptography Conference (TCC) 2014*, San Diego, CA, February 2014.
– *Crypto 2013*, Santa Barbara, CA, August 2013.
– *International Conference on Machine Learning (ICML) 2013*, Atlanta, GA, June 2013.

- *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.

◇ Reviewer for several journals and conferences

◇ Leader, Privacy and Security Connector, Northeast NSF Big Data Hub, 2015–2018.

◇ Co-organizer:

- Semester-long program on *Data Privacy: Foundations and Applications* at the Simons Institute for Theoretical Computer Science, UC Berkeley. `https://simons.berkeley.edu/privacy2019`
- First and Second Workshops on Adaptive Data Analysis (held at *NIPS* 2016 and 2017). `wadapt.org`
- *Institute for Applied Computational Science Symposium on Data Privacy*, Harvard University, Cambridge, MA, January 2015.
- *Charles River Privacy Day*, Hariri Institute for Computation, Boston University, November 17, 2013.
- *Charles River Workshop on Private Analysis of Social Networks*, Hariri Institute for Computation, Boston University, May 2014.
- *Workshop on Differential Privacy Across Computer Science*, Center for Discrete Mathematics and Computer Science, Rutgers Unversity, October 2012.
- *Graduate summer school on cryptography and principles of computer security*, Penn State, June 2012.
- *Workshop on Privacy and Financial Data*, Penn State, March 2012.
- *NSF Workshop on the Future of Trustworthy Computing*, Arlington, VA, October 2010.
- Workshop on *Statistical and Learning-Theoretic Challenges in Data Privacy*, Institute for Pure and Applied Mathematics, UCLA, February 2010.

LECTURE NOTES

◇ A. Smith and J. Ullman. Privacy in Machine Learning and Statistics. Spring 2021. `https://dpcourse.github.io`

◇ A. Roth and A. Smith. Algorithmic Foundations of Adaptive Data Analysis. Fall 2017. `https://adaptivedataanalysis.com/`

EDITED VOLUMES

◇ Y. Tauman Kalai, A. Smith, D. Wichs. *1st Conference on Information-Theoretic Cryptography, ITC 2020*, June 17-19, 2020, Boston, MA, USA. LIPIcs 163.

◇ M. Hirt and A. Smith, editors. *Proceedings of the Fourteenth Theory of Cryptography Conference (TCC 2016), Beijing, China, October 31–November 3, 2016,* Springer.

◇ A. Smith, editor. *Proceedings of the Sixth International Conference on Information-Theoretic Security (ICITS 2012), Montreal, QC, Canada, August 15–17, 2012.* Springer, LNCS Volume 7412, 2012.

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 ∗.)

[1] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, A. Smith. Reusable Fuzzy Extractors for Low-Entropy Distributions. *J. Cryptology*, Vol. 34, No. 1, 2021.

[2] R. Bassily, K. Nissim, A. Smith, T. Steinke, U. Stemmer, J. Ullman: Algorithmic Stability for Adaptive Data Analysis. *SIAM J. Computing*, Vol. 50, No. 3, 2021.

[3] A. Cheu, A. Smith, J. Ullman. Manipulation Attacks in Local Differential Privacy. *Journal of Privacy and Confidentiality*, Vol. 11, No. 1, 2021.

[4] * J. Lei, A.-S. Charest, A. Slavkovic, A. Smith, S. Fienberg. Differentially private model selection with penalized and constrained likelihood. *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, Vol. 181, No. 3, p. 609-–633, 2018.

[5] A. McMillan, A. Smith. When is non-trivial estimation possible for graphons and stochastic block models? *Information and Inference*, Vol. 7, No. 2, June 2018.

[6] C. Dwork, F. McSherry, K. Nissim, A. Smith. Calibrating Noise to Sensitivity in Private Data Analysis. *J. Privacy and Confidentiality*, Vol. 7, No. 3, 2016.

[7] V. Guruswami, A. Smith. Optimal-Rate Code Constructions for Computationally Simple Channels. *J. ACM*, Vol. 63, No. 4, 2016.

[8] C. Gentry, J. Groth, Y. Ishai, C. Peikert, A. Sahai, A Smith. Using Fully Homomorphic Hybrid Encryption to Minimize Non-interactive Zero-Knowledge Proofs. *J. Cryptology*, Vol. 28, No. 4, 2015.

[9] V. Karwa, S. Raskhodnikova, A. Smith, G. Yaroslavtsev. Private Analysis of Graph Structure. *ACM Trans. Database Syst.*, Vol. 39, No. 3, 2014.

[10] S. P. Kasiviswanathan, A. Smith. On the 'Semantics' of Differential Privacy: A Bayesian Formulation. *Journal of Privacy and Confidentiality*, Vol. 6, No. 1, 2014.

[11] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin, and A. Smith: Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets. *IEEE Transactions on Information Theory*, Vol. 58, No. 9, p. 6207-6222, 2012.

[12] S. P. Kasiviswanathan, H. Lee, K. Nissim, S. Raskhodnikova and A. Smith. What Can We Learn Privately? *SIAM Journal on Computing*, Vol. 40, No. 3, p. 793–826, 2011.

[13] * M. Tomamichel, R. Renner, C. Schaffner, A. Smith. Leftover Hashing Against Quantum Side Information. *IEEE Transactions on Information Theory*, Vol. 57, No. 8, p. 5524–5535, 2011.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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 $*$.)

[1] P. Jain, K. Rush, A. Smith, S. Song, A. Thakurta. Differentially Private Model Personalization. In *NeurIPS 2021*. (Spotlight presentation.)

[2] G. Brown. M. Gaboardi, A. Smith, J. Ullman, L. Zakynthinou. Covariance-aware Private Mean Estimation Without Private Covariance Estimation. In *NeurIPS 2021*. (Spotlight presentation.)

[3] S. Raskhodnikova, S. Sivakumar, A. Smith, M. Swanberg. Differentially Private Sampling from Distributions. In *NeurIPS 2021*.

[4] G. Brown, M. Bun, V. Feldman, A. Smith, K. Talwar. When is Memorization Necessary for High-Accuracy Learning? In *ACM Symposium on the Theory of Computation (STOC)*, June 2021.

[5] A. Cheu, J. Ullman, A. Smith. Manipulation Attacks in Local Differential Privacy. In *IEEE Symposium on Security and Privacy* ("Oakland"), 2021.

[6] L. Reyzin, A. Smith, S. Yakoubov. Turning HATE into LOVE: Compact Homomorphic Ad Hoc Threshold Encryption for Scalable MPC. *Cyber Security, Cryptography and Machine Learning (CSCML)*, p. 361–378, 2021.

[7] A. Smith, S. Song., A. Thakurta. The Flajolet-Martin Sketch Itself Preserves Differential Privacy: Private Counting with Minimal Space. In *NeurIPS 2020*, December 2020.

[8] R. Rogers, A. Roth, A. Smith, N. Srebro, O. Thakkar, B. E. Woodworth. Guaranteed Validity for Empirical Approaches to Adaptive Data Analysis. In *AISTATS 2020*.

[9] C. Canonne, G. Kamath, A. McMillan, A. Smith, J. Ullman. The structure of optimal private tests for simple hypotheses. In *ACM Symposium on the Theory of Computation (STOC 2019)*, p. 310-321, June 2019.

[10] R. Canetti, A. Cohen, N. Dikkala, G. Ramnarayan, S. Scheffler, A Smith. From Soft Classifiers to Hard Decisions: How fair can we be? In *ACM Fairness, Accountability and Transparency (FAT*)* 2019, p. 309-318.

[11] A. Cheu, A. Smith, J. Ullman, D. Zeber, M. Zhilyaev. Distributed Differential Privacy via Shuffling. In *EUROCRYPT 2019 (1)*, p. 375-403, April 2019.

[12] * B. E. Woodworth, J. Wang, A. Smith, B. McMahan, N. Srebro. Graph Oracle Models, Lower Bounds, and Gaps for Parallel Stochastic Optimization. In *NeurIPS 2018*, 8505–8515, December 2018. (Spotlight presentation.)

[13] J. Ullman, A. Smith, K. Nissim, U. Stemmer, T. Steinke. The Limits of Post-Selection Generalization. In *NeurIPS 2018*, 6402–6411, December 2018.

[14] C. Borgs, J. Chayes, A. Smith, I. Zadik. Revealing network structure, confidentially: Improved Rates for Node-private Graphon Estimation. In *Foundations of Computer Science (FOCS)*, October 2018.

[15] A. Smith, A. Thakurta, J. Uphadhyay. Is Interaction Necessary for Distributed Private Learning? In *IEEE Symposium on Security and Privacy*, May 2017.

[16] S. Raskhodnikova, A. Smith. High-dimensional Lipschitz Extensions and Node-Private Degree Distributions. In *Foundations of Computer Science (FOCS)*, October 2016.

[17] R. Rogers, A. Roth, A. Smith, O. Thakkar. Max-Information, Differential Privacy, and Post-Selection Hypothesis Testing. In *Foundations of Computer Science (FOCS)*, October 2016.

[18] B. Fuller, L. Reyzin, A. Smith. When are Fuzzy Extractors Possible? In *ASIACRYPT*, December 2016.

[19] R. Bassily, K. Nissim, A. Smith, T. Steinke, U. Stemmer, J. Ullman. Algorithmic Stability for Adaptive Data Analysis. In *48th Annual ACM Symposium on the Theory of Computing (STOC)*, June 2016.

[20] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, A. Smith. Reusable Fuzzy Extractors via Digital Lockers. In *Advances in Cryptology—EUROCRYPT 2016*, May 2016.

[21] C. Borgs, J. Chayes, A. Smith. Private Graphon Estimation in Sparse Graphs. In *Neural Information Processing Systems (NeurIPS)*, December 2015.

[22] C. Dwork, A. Smith, T. Steinke, J. Ullman, S. Vadhan. Robust Traceability From Trace Amounts. In *Foundations of Computer Science (FOCS)*, October 2015.

[23] R. Bassily, A. Smith. Local, Private, Efficient Protocols for Succinct Histograms. In *47th Annual ACM Symposium on the Theory of Computing (STOC)*, June 2015.

[24] A. Smith, Y. Zhang. On the Regularity of Lossy RSA: Improved Bounds and Applications to Padding-Based Encryption. In *Theory of Cryptography Conference (TCC)*, March 2015.

[25] A. Blum, J. Morgenstern, A. Sharma, A. Smith. Privacy-Preserving Public Information for Sequential Games. In *Innovations in Theoretical Computer Science (ITCS)*, January 2015.

[26] R. Bassily, A. Smith, A. Thakurta. Differentially Private Empirical Risk Minimization: Efficient Algorithms and Tight Error Bounds. In *Foundations of Computer Science (FOCS)*, October 2014.

[27] R. Bassily, A. Smith. Causal Erasure Channels. In *Symposium on Discrete Algorithms (SODA)*, January 2014

[28] R. Bassily, A. Groce, J. Katz, A. Smith. Coupled-Worlds Privacy: Exploiting Adversarial Uncertainty in Statistical Data Privacy. In *Foundations of Computer Science (FOCS)*, October 2013.

[29] A. Smith, A. Thakurta. Differentially Private Feature Selection via Stability Arguments, and the Robustness of the Lasso. In *Computational Learning Theory (COLT)*, June 2013.

[30] M. Lewko, A. O'Neill, A. Smith. Regularity of Lossy RSA and Applications. In *Advances in Cryptology — EUROCRYPT 2013*, May 2013.

[31] S. P. Kasiviswanathan, K. Nissim, S. Raskhodnikova, and A. Smith. Analyzing Graphs with Node Differential Privacy. In *Theory of Cryptography (TCC)*, p. 457-476, 2013.

[32] S. P. Kasiviswanathan, M. Rudelson, A. Smith. The Power of Linear Reconstruction Attacks. In *24th Annual ACM Symposium on Discrete Algorithms (SODA)*, January 2013.

[33] D. Kifer, A. Smith and A. Thakurta. Differentially Private Convex Optimization for Empirical Risk Minimization with Applications to High-dimensional Regression. In *25th Conference on Learning Theory (COLT 2012)*, June 2012.

[34] S. Hallgren, A. Smith, F. Song. Classical Cryptographic Protocols in a Quantum World. In *Advances in Cryptology—CRYPTO 2011*, p. 411–428, August 2011.

[35] V. Karwa, S. Raskhodnikova, A. Smith, G. Yaroslavtsev. Private Analysis of Graph Structure. In *37th International Conference on Very Large Databases (PVLDB)*, Vol. 4, No. 11, p. 1146–1157, 2011.

[36] A. Smith. Privacy-preserving Statistical Estimation with Optimal Convergence Rates. In *43nd Annual ACM Symposium on the Theory of Computing (STOC)*, 813–822, June 2011.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] $*$ 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] M. Ben-Or, C. Crépeau, 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] 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.

[64] 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.

[65] 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.

[66] A. Ambainis, A. Smith and K. Yang. Extracting Quantum Entanglement. In *17th Annual IEEE Conference on Computational Complexity (CCC)*, May 2002, pp. 103–112.

[67] 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.

[68] M. Fitzi, 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

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

◇ S. Raskhodnikova, A. Smith. Private Analysis of Graph Data. In M.-Y. Kao, *Encyclopedia of Algorithms*, 2nd edition, Springer, 2015, 6 pages.

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

Talks and Presentations

Invited Plenary Conference Presentations:

◇ *12th China International Conference on Information Security and Cryptology (INSCRYPT 2016)*, Beijing, China, November 4–6, 2016.

◇ *Cryptology and Network Security Conference 2009*, Kanazawa, Japan, December 2009.

◇ *International Conference on Information-Theoretic Security 2009*, Shizuoka, Japan, December 2009.

Invited Tutorials:

◇ *North American School on Information Theory*, Boston, MA, July 2019.

◇ *Differnetial Privacy and Multiarty Comptutation Workshop*, Boston University, June 2018
◇ *Bar-Ilan Winter School on Cryptography*, Ramat Gan, Israel, February 2017.
◇ *Park City Mathematics Institute*, Midway, UT, July 2016.
◇ *Isaac Newton Institute Workshop on Data Linkage and Anonymization*, July 2016.
◇ *DIMACS/Columbia Workshop on Cryptography and Big Data*, December 2015.
◇ *Advances in Cryptography — CRYPTO 2012*, Santa Barbara, CA, August 2012.
◇ *DIMACS Workshop on Data Privacy*, Rutgers University, February 2008.

Invited Seminar and Workshop Presentations:

◇ *Memorization in Machine Learning and Its Implications for Privacy*

- Keynote presentation, PPAI Workshop at AAAI 2022 (virtual)
- Harvard Center for Mathmatical Sciences and Applications (CMSA) Colloquium, February 2022
- Worcester Polytechnic Institute Computer Science Colloquium, November 2021.
- Keynote talk, Google workshop on privacy-preserving advertizing ecosystems, June 2021
- Keynote talk, Google workshop on federated learning, August 2021
- CMU/KAUST Seminar on Federated Learning (FLOW), January 2021.
- Virtual Seminar on the Foundations of Data Science, December 2020
- Google Seminar on Privacy in Machine Learning, November 2020

◇ Apple Workshop on Privacy-preserving Machine Learning, August 2020
◇ Google Workshop on Federated Learning, July 2020
◇ Information Theory and Applications (ITA) Workshop, San Diego, CA, February 2020
◇ Distinguished Lecture Series, George Mason University, Fairfax, VA, October 2019.
◇ Data Cooperatives Workshop, Georgetown University, Washington, DC, October 2019.
◇ Theoretical Computer Science Seminar, California Institute of Technology, Pasadena, CA, May 2019.
◇ Distinguished Lecture Series, Reed College, Portland, OR, April 2019.
◇ Simons Institute Workshop on Privacy and the Science of Data Analysis, Berkeley, CA, March 2019.
◇ Census Collaborative Agreement Workshop, Harvard University, October 2018
◇ University of Pennsylvania Warren Center Seminar, November 2018
◇ Differential Privacy Deployed Workshop, Harvard University, September 2018.
◇ Simons Institute Workshop on Adaptive Data Analysis, Berkeley, CA, July 2018.
◇ University of Illinois at Urbana-Champaign Computer Science Colloquium, May 2018.
◇ Banff Center Workshop on the Mathematical Foundations of Data Privacy, May 2018.
◇ Research on Tap, Boston Unviersity, November 2017.
◇ Simons Institute Workshop on Data Privacy, from Foundations to Applications, May 2017.
◇ *Privacy, Information, and Generalization in Adaptive Data Analysis*
- University of Maryland Computer Science Colloquium, April 2017
- McGill University Computer Science Colloquium, March 2017
- Boston University Computer Science colloquium, February 2017
- University of Michigan Computer Science colloquium, November 2016.
- International Conference on Information Security and Cryptology (INSCRYPT), November 2016.
- Johns Hopkins University Theoretical Computer Science Seminar, October 2016.
- Google Workshop on Mobile Privacy and Security, Seattle, WA, September 2016.

◇ *Discussion—Recent advances in foundations of data privacy*
- Joint Statistical Meetings, Chicago, IL,, August 1, 2016.

◇ *Algorithmic Stability in Adaptive Data Analysis*
- Penn State Stochastic Modeling and Computing Seminar, February 2016
- Penn State Probability Seminar, September 2015

◇ *Robust Traceability from Trace Amounts*
- Dagstuhl Workshop on Genomic Privacy, Wadern, Germany, October 2015
- Penn State Genomics Seminar, September 2015

◇ *Google and academic research: directions for interaction*
- Google Security Summit, Mountain View, CA, March 17, 2015

◇ *Fourier's Magnet: Better Algorithms for Finding "Needles in a Haystack"*
- Microsoft Research, Bangalore, India, January 29, 2015

◇ *Private Analysis of Graphs*
- New York Area Theory Day, Columbia University, NY, April 25, 2014
- Indian Institute of Technology, Delhi, India, February 2014
- Tata Institute for Fundamental Research, Mumbai, India, February 2014

◇ *Coding, Causality, Complexity, Cryptography*
- *Allerton Conference on Communications and Control*, Monticello, IL, October 2013

◇ *Rigorous Foundations for Privacy in Statistical Databases*
- Microsoft Research Colloquium, June 22, 2016
- University of Maryland Cybersecurity Seminar, May 18, 2016
- Institute for Statistical Sciences, Kolkata, India, January 27, 2015
- Rutgers University, New Brunswick, NJ, April 29, 2014
- Boston University, Boston, MA, November 15, 2013
- *Global Signal and Information Processing* Conference, Austin, TX, October 2013
- *Rao Prize Workshop on Statistics*, Pennsylvania State University, October 2013
- University of Texas Computer Science Colloquium, Austin, TX, October 2012
- Center for Applied Cybersecurity Research Seminar, Indiana University, Bloomington, IN, April 2012
- Brown University Computer Science Colloquium, Providence, RI, February 2012
- Northeastern University Computer Science Colloquium, Boston, MA, February 2012

◇ *Integrating Differential Privacy with Statistical Theory*
- Theoretical Computer Science Seminar, University of Pennsylvania, Philadelphia, PA, September 2011.
- Computer Science Colloquium, Cornell University, Ithaca, NY, September 2010.
- 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.

Outreach Activities (2017 and later):

◇ I have run hands-on educational activities for middle-school childern on cryptography, data privacy, and related topics, in several contexts:

- Sigma Science Camp (selective week-long camp for middle- and high-schoolers focused on hands-on scientific and mathematical investigation). August 2020 and August 2021.
- Discoll Science Solstice (hosted a half-day visit by middle schooolers from a local public school at BU), December 2018 and 2019.
- Berkeley Math Circle (selective program for students in elemntary and middle school), Berkeley CA, Spring 2019.
- GEM Seminar, Mount Nittany Middle School (after-school activity open to all students at the middle school), State College PA, 2017

◇ Hosted and ran half-day field trips by middle schoolers from Discoll School in Brookline, MA to BU's Computer Science deparmtent. Students engaged in three hour-long hands-on activities that exposed them to imporannt ideas in computer science (cryptography, AI, computer-aided fabrication). December 2018 an December 2019.