

Ashwin Machanavajjhala

Department of Computer Science, D329 LSRC
Duke University, Durham, NC 27708
Updated June 9, 2020

ashwin@cs.duke.edu
<http://www.cs.duke.edu/~ashwin>

Research Interests

My research focuses on studying privacy and fairness aspects of living in a surveillance society and on developing practical algorithms and systems for the privacy preserving storage and analysis of sensitive data.

Education

| | |
|--|---------------------|
| Ph.D., Computer Science, Cornell University, Ithaca, NY, USA Thesis: <i>Defining and Enforcing Privacy in Data Sharing</i> Advisor: Prof. Johannes Gehrke | August 2008 |
| M.S., Computer Science, Cornell University, Ithaca, NY, USA | January 2007 |
| B.Tech., Computer Science, Indian Institute of Technology - Madras, Chennai, India | June 2002 |

Professional Positions

| | |
|--|-------------------------|
| Associate Professor, Department of Computer Science Duke University, Durham, NC | 7/2018 - current |
| President and co-founder, Tumult Labs | 7/2019 - current |
| Consultant, Center for Disclosure Avoidance Research U. S. Census Bureau | 10/2016 - 5/2019 |
| Assistant Professor, Department of Computer Science Duke University, Durham, NC | 8/2012 - 6/2018 |
| Associate Director, Information Institute @ Duke, Duke University, Durham, NC | 8/2014 - 7/2015 |
| Consultant, LEHD Program, U. S. Census Bureau | 3/2013 - 9/2016 |
| Senior Research Scientist, Yahoo! Research, Santa Clara, CA, USA | 9/2011 - 5/2012 |
| Visiting Assistant Research Scientist, University of Maryland - College Park | 8/2011 - 5/2012 |
| Research Scientist, Yahoo! Research, Santa Clara, CA, USA | 9/2008 - 8/2011 |
| Graduate Research Assistant, Cornell University, Ithaca, NY | 8/2002 - 8/2008 |
| Research Intern, Yahoo! Research, Santa Clara, CA, USA | 6/2007 - 9/2007 |
| Research Intern, IBM Almaden Research Center, San Jose, CA, USA | 5/2004 - 8/2004 |

Honors and Awards

- H-1. **2020 RAPID grant** awarded from the National Science Foundation to study privacy preserving contact tracing methodology with applications to the ongoing COVID19 pandemic.
- H-2. **2019 ACM SIGMOD Research Highlight Award** for SIGMOD 2018 paper titled "Ektelo: A Framework for Defining Differentially-Private Computations".
- H-3. **2017-2018 David and Janet Vaughan Brooks Teaching Award**, Trinity College of Arts and Sciences, Duke University, Apr 2018
- H-4. **IEEE ICDE 2017 Influential Paper Award** for paper titled "L-diversity: privacy beyond k-anonymity", that was presented at ICDE 2006.
- H-5. **Distinguished Program Committee Member** ACM SIGMOD 2017, 2019.
- H-6. **Best Demonstration Award**, PVLDB 9(13), September 2016
- H-7. **Top 5% of all undergraduate instructors for a small class** for *Quality of Course/Intellectual Stimulation*, Duke University, Spring 2013
- H-8. **Google Faculty Research Award** recipient, August 2014 and February 2013

- H-9. **NSF Faculty Early Career Development (CAREER)** Award recipient, January 2013
- H-10. **2008 ACM-SIGMOD Jim Gray Dissertation Award Honorable Mention** for Ph.D. thesis titled “Defining and Enforcing Privacy in Data Sharing”, June 2009.

Publications

Journal.

- J-1. Sameer Wagh, Xi He, *Ashwin Machanavajhala*, Prateek Mittal, “DP-Cryptography: Marrying Differential Privacy and Cryptography in Emerging Applications”, To appear CACM 2020
- J-2. Andrew Foote, Ashwin Machanavajhala, Kevin McKinney, “Releasing Earnings Distributions using Differential Privacy”, *Journal on Privacy and Confidentiality* 9(2) 2019
- J-3. Ios Kotsogiannis, Yuchao Tao, Xi He, Maryam Fanaeepour, *Ashwin Machanavajhala*, Michael Hay, Gerome Miklau, “PrivateSQL: A Differentially Private SQL Query Engine”, *PVLDB* 12(11) 2019
- J-4. Johes Bater, Xi He, William Ehrich, Ashwin Machanavajhala, Jennie Rogers, “ShrinkWrap: Differentially-Private Query Processing in Private Data Federations”, *PVLDB* 12(3) 2018
- J-5. Nisarg Raval, *Ashwin Machanavajhala*, Qiyuan Pan, “OLYMPUS: Sensor Privacy through Utility Aware Obfuscation”. *POPETS* 2019
- J-6. Ryan McKenna, Gerome Miklau, Michael Hay, *Ashwin Machanavajhala*, “Optimizing error of high-dimensional statistical queries under differential privacy”, *PVLDB* 11(10) 2018
- J-7. Yu-Hsuan Kuo, Cho-Chun Chiu, Daniel Kifer, *Ashwin Machanavajhala*, Michael Hay, “Differentially Private Hierarchical Group Size Estimation”, *PVLDB* 11(10) 2018
- J-8. Andrés F. Barrientos, Jerome P. Reiter, *Ashwin Machanavajhala*, Yan Chen, “Differentially private significance tests for regression coefficients”, To appear, *Journal of Computational and Graphical Statistics* 2018
- J-9. Andrés F. Barrientos, Alexander Bolton, Tom Balmat, Jerome P. Reiter, John M. de Figueiredo, *Ashwin Machanavajhala*, Yan Chen, Charles Kneifel, Mark DeLong, “A Framework for Sharing Confidential Research Data, Applied to Investigating Differential Pay by Race in the U. S. Government”, *Annals of Applied Statistics* 2018 and NBER Working Paper No. 23534
- J-10. Yan Chen, Andrés Barrientos, *Ashwin Machanavajhala*, Jerome Reiter, “Is My Model Any Good: Differentially Private Regression Diagnostics”, *Knowledge and Information Systems (KAIS)*, November 2017.
- J-11. Samuel Haney, *Ashwin Machanavajhala*, Bolin Ding, “Design of Policy-Aware Differentially Private Algorithms”, *PVLDB* 9(4), 2016
- J-12. Xi He, Graham Cormode, *Ashwin Machanavajhala*, Cecilia M. Procopiuc, Divesh Srivastava, “DPT: Differentially Private Trajectory Synthesis Using Hierarchical Reference Systems”, *PVLDB* 8(11), 2015
- J-13. *Ashwin Machanavajhala*, Daniel Kifer, “Designing Statistical Privacy for Your Data”, *Communications of the ACM*, 58(3) 2015
- J-14. Daniel Kifer, *Ashwin Machanavajhala*, “Pufferfish: A Framework for Mathematical Privacy Definitions”, *ACM Transactions on Database Systems TODS*, 39(1), 2014
- J-15. Hye-Chung Kum, Ashok Krishnamurthy, *Ashwin Machanavajhala*, Michael K. Reiter, Stanley C. Ahalt, “Privacy preserving interactive record linkage (PIRL)”, *Journal of the American Medical Informatics Association (JAMIA)* 21(2): 212-220, 2014
- J-16. Hye-Chung Kum, Ashok Krishnamurthy, *Ashwin Machanavajhala*, Stanley C. Ahalt, “Social Genome: Putting Big Data to Work for Population Informatics”, *IEEE Computer* 47(1): 56-63, 2014

- J-17. Theodoros Rekatsinas, Amol Deshpande, *Ashwin Machanavajjhala*, "SPARSI: Partitioning Sensitive Data amongst Multiple Adversaries", In *PVLDB*, 6(13), 2013
- J-18. *Ashwin Machanavajjhala*, Jerome. P. Reiter, "Big Privacy: Protecting Confidentiality in Big Data", In *ACM Crossroads*, 19(1), 2012.
- J-19. Michaela Goetz, *Ashwin Machanavajjhala*, Gouzhang Wang, Xiaokui Xiao, Johannes Gehrke "Publishing Search Logs - A Comparative Study of Privacy Guarantees", In *IEEE Transactions on Knowledge and Data Engineering TKDE*, 24(3), 2012.
- J-20. Nilesh Dalvi, *Ashwin Machanavajjhala*, Bo Pang, "An Analysis of Structured Data on the Web", In *PVLDB*, 5(7), 2012.
- J-21. *Ashwin Machanavajjhala*, Aleksandra Korolova, Atish Das Sarma, "Personalized Social Recommendations – Accurate or Private?", In *PVLDB*, 4(7), 2011.
- J-22. Adina Crainiceanu, Prakash Linga, *Ashwin Machanavajjhala*, Johannes Gehrke, Jayavel Shanmugasundaram, "Load Balancing and Range Queries in P2P Systems Using P-Ring." In *ACM Transactions on Internet Technology TOIT*, 10(4) 2011.
- J-23. *Ashwin Machanavajjhala*, Johannes Gehrke, Michaela Goetz, "Data Publishing against Realistic Adversaries", In *PVLDB*, 2(1), 2009.
- J-24. *Ashwin Machanavajjhala*, Daniel Kifer, Johannes Gehrke, Muthuramakrishnan Venkitasubramaniam, " ℓ -Diversity: Privacy beyond k -Anonymity", In *ACM Transactions on Knowledge Discovery from Data TKDD*, 1(1), 2007.
- J-25. *M. V. N. Ashwin Kumar*, Arun K. Singh, Ramesh Babu, "A Security Assurance Framework for Component Based Software Development", In *Informatica*, 25(4), 2001.

Peer-reviewed Conference.

- C-1. Yuchao Tao, Xi He, *Ashwin Machanavajjhala*, Sudeepa Roy, "Computing Local Sensitivities of Counting Queries with Joins", To appear *ACM SIGMOD 2020*
- C-2. Amrita Roy Chowdhury, Chenghong Wang, Xi He, *Ashwin Machanavajjhala*, Somesh Jha, "Crypte: Crypto-Assisted Differential Privacy on Untrusted Servers", To appear *ACM SIGMOD 2020*
- C-3. Satya Kuppam, Ryan Mckenna, David Pujol, Michael Hay, *Ashwin Machanavajjhala*, Gerome Miklau, "Fair Decision Making using Privacy-Protected Data", In *ACM FAT* 2020*
- C-4. Ios Kotsogiannis, Stelios Doudalis, Samuel Haney, *Ashwin Machanavajjhala*, Sharad Mehrotra, "One-sided Differential Privacy", In *ICDE 2020*
- C-5. Kamalika Chaudhuri, Jacob Imola, *Ashwin Machanavajjhala*, "Capacity Bounded Differential Privacy", In *NeurIPS 2019*
- C-6. Nisarg Raval, Ali Razeen, *Ashwin Machanavajjhala*, Landon P. Cox, Andrew Warfield, "Permissions Plugins as Android Apps", *MobiSys 2019*
- C-7. Chang Ge, Xi He, Ihab Ilyas, *Ashwin Machanavajjhala*, "APEX: Accuracy-Aware Privacy Engine for Data Exploration", To Appear *ACM SIGMOD 2019*
- C-8. Ios Kotsogiannis, Yuchao Tao, *Ashwin Machanavajjhala*, Michael Hay, Gerome Miklau, "Architecting a Differentially Private SQL Engine", To Appear *CIDR 2019*
- C-9. Dan Zhang, Ryan McKenna, Ios Kotsogiannis, Michael Hay, *Ashwin Machanavajjhala*, Gerome Miklau, " ϵ KTELO: A Framework for Defining Differentially-Private Computations", In *ACM SIGMOD 2018*
- C-10. Xi He, *Ashwin Machanavajjhala*, Cheryl Flynn, Divesh Srivastava, "Composing Differential Privacy and Secure Computation: A case study on scaling private record linkage", In *ACM CCS 2017*

- C-11. Yan Chen, *Ashwin Machanavajjhala*, Michael Hay, Gerome Miklau, "PeGaSus: Data-Adaptive Differentially Private Stream Processing", In *ACM CCS* 2017
- C-12. Samuel Haney, *Ashwin Machanavajjhala*, Mark Kutzbach, Matthew Graham, John Abowd, Lars Vilhuber, "Utility Cost of Formal Privacy for Releasing National Employer-Employee Statistics", In *ACM SIGMOD* 2017
- C-13. Ios Kotsogiannis, *Ashwin Machanavajjhala*, Michael Hay, Gerome Miklau, "Pythia: Differentially Private Algorithm Selection", In *ACM SIGMOD* 2017
- C-14. Ios Kotsogiannis, Elena Zheleva, *Ashwin Machanavajjhala*, "Directed Edge Recommendation System", In *WSDM* 2017
- C-15. Christopher Streiffer, Animesh Srivastava, Victor Orlikowski; Nisarg Raval, *Ashwin Machanavajjhala*, Landon P. Cox, Yesenia Velasco, Vincentius Martin, "ePrivateEye: To the Edge and Beyond!", In *ACM/IEEE SEC* 2017
- C-16. Yan Chen, *Ashwin Machanavajjhala*, Jerome Reiter, Andres Barrientos, "Differentially Private Regression Diagnostics", In *IEEE ICDM* 2016. **Best paper candidate** invited to special issue of KAIS journal.
- C-17. Nisarg Raval, Animesh Srivastava, Ali Razeen, Kiron Lebeck, *Ashwin Machanavajjhala*, Landon P. Cox, "What You Mark is What Apps See" In *MobiSys* 2016
- C-18. Michael Hay, *Ashwin Machanavajjhala*, Gerome Miklau, Yan Chen, Dan Zhang, "Principled evaluation of differentially private algorithms using DPBench", In *ACM SIGMOD* 2016
- C-19. Ben Stoddard, Kate O'Hanlon, Landon Cox, Ashwin Machanavajjhala, Brian Lin, " Ayumu: Efficiently capturing reading material with focused-task life-logging", *MOBICASE* 2016
- C-20. Xi He, *Ashwin Machanavajjhala*, Bolin Ding, "Blowfish privacy: tuning privacy-utility trade-offs using policies", In *Proc. SIGMOD Conference* 2014.
- C-21. Jianjun Chen, *Ashwin Machanavajjhala*, George Varghese, "Scalable Social Coordination with Group Constraints using Enmeshed Queries", In *Proc. CIDR* 2013
- C-22. Kedar Bellare, Carlo Curino, *Ashwin Machanavajjhala*, Peter Mika, Mandar Rahukar, Aamod Sane, "WOO: A Scalable and Multi-tenant Platform for Continuous Knowledge Base Synthesis", In *Proc. VLDB (Industrial Track)*, 2013
- C-23. Vibhor Rastogi, *Ashwin Machanavajjhala*, Laukik Chitnis, Anish Das Sarma, "Finding connected components in map-reduce in logarithmic rounds", In *Proc. ICDE* 2013.
- C-24. Daniel Kifer, *Ashwin Machanavajjhala*, "A rigorous and customizable framework for privacy", In *Proc. PODS* 2012.
- C-25. Anish Das Sarma, Ankur Jain, *Ashwin Machanavajjhala*, Philip Bohannon, "An Automatic Blocking Mechanism for Large-Scale De-duplication Tasks", In *Proc. CIKM* 2012.
- C-26. Aditya Pal, Vibhor Rastogi, *Ashwin Machanavajjhala*, Philip Bohannon, "Information integration over time in unreliable and uncertain environments", In *Proc. WWW* 2012.
- C-27. Daniel Kifer, *Ashwin Machanavajjhala*, "No Free Lunch in Data Privacy", In *Proc. SIGMOD* 2011.
- C-28. Nilesh Dalvi, Ravi Kumar, *Ashwin Machanavajjhala*, Vibhor Rastogi, "Sampling hidden objects using nearest-neighbor oracles.", In *Proc. KDD* 2011.
- C-29. Lorenzo Blanco, Nilesh Dalvi, *Ashwin Machanavajjhala*, "Highly Efficient Algorithms For Structural Clustering of Large Websites", In *Proc. WWW* 2011.
- C-30. *Ashwin Machanavajjhala*, Arun Iyer, Philip Bohannon, Srujana Merugu, "Collective Bayesian Extraction from Heterogeneous Web Lists", In *Proc. WSDM* 2011.

- C-31. *Ashwin Machanavajjhala*, Erik Vee, Minos Garofalakis, Jayavel Shanmugasundaram, “Scalable Ranked Publish/Subscribe”, In *Proc. VLDB* 2008.
- C-32. *Ashwin Machanavajjhala*, Daniel Kifer, John Abowd, Johannes Gehrke, Lars Vilhuber, “Privacy: Theory meets Practice on the Map”, In *Proc. ICDE* 2008.
- C-33. Adina Crainiceanu, Prakash Linga, *Ashwin Machanavajjhala*, Johannes Gehrke, Jayavel Shanmugasundaram, “P-Ring: An Efficient and Robust P2P Range Index Structure”, In *Proc. SIGMOD* 2007.
- C-34. David Martin, Daniel Kifer, *Ashwin Machanavajjhala*, Johannes Gehrke, Joseph Halpern, “Worst Case Background Knowledge”, In *Proc. ICDE* 2007.
- C-35. *Ashwin Machanavajjhala*, Johannes Gehrke, “On the Efficiency of Checking Perfect Privacy”, In *Proc. ACM PODS* 2006.
- C-36. *Ashwin Machanavajjhala*, Johannes Gehrke, Daniel Kifer, Muthuramakrishnan Venkitasubramaniam, “ ℓ -Diversity: Privacy beyond k -Anonymity”, In *Proc. ICDE* 2006.
- C-37. *M. V. N. Ashwin Kumar*, Pranava. R. Goundan, K. Srinathan, C. Pandu Rangan, “On Perfectly Secure Communication over Arbitrary Networks”, In *Proc. ACM PODC* 2002.
- C-38. K. Srinathan, *M. V. N. Ashwin Kumar*, C. Pandu Rangan, “Asynchronous Secure Communication tolerating Mixed Adversaries”, In *Proc. ASIACRYPT* 2002, LNCS, Springer Verlag.
- C-39. *M. V. N. Ashwin Kumar*, K. Srinathan, C. Pandu Rangan, “Asynchronous Perfectly Secure Computation tolerating Generalized Adversaries”, In *Proc. ACISP* 2002, LNCS, Springer Verlag.
- C-40. Pranava. R. Goundan, K. Srinathan, *M. V. N. Ashwin Kumar*, R. Nandakumar, C. Pandu Rangan, “Theory of Equal-Flows in Networks”, In *Proc. COCOON* 2002, LNCS, Springer Verlag.

Peer-reviewed Workshop.

- W-1. Ios Kotsogiannis, Yuchao Tao, Xi He, *Ashwin Machanavajjhala*, Michael Hay, Gerome Miklau, “PrivateSQL: A Differentially Private SQL Query Engine”, In Privacy Preserving Machine Learning (NeurIPS Workshop) 2019
- W-2. Amrita Roy Chowdhury, Chenghong Wang, Xi He, *Ashwin Machanavajjhala*, Somesh Jha, “Crypte: Crypto-Assisted Differential Privacy on Untrusted Servers”, In Privacy Preserving Machine Learning (NeurIPS Workshop) 2019
- W-3. Jennie Rogers, Johes Bater, Xi He, *Ashwin Machanavajjhala*, Madhav Suresh, Xiao Wang, “Privacy Changes Everything”, Privacy, Security and/or Policy Issues for Heterogenous Data (VLDB Workshop) 2019
- W-4. Yikai Wu, David Pujol, Ios Kotsogiannis, “Answering Summation Queries for Numerical Attributes under Differential Privacy”, In Theory and Practice of Differential Privacy (TPDP) Workshop 2019
- W-5. Maryam Fanaeepour, *Ashwin Machanavajjhala*, “PrivStream: Differentially Private Event Detection on Data Streams”, In CODASPY 2019
- W-6. Kamalika Chaudhuri, *Ashwin Machanavajjhala*, “Capacity Bounded Differential Privacy”, In Privacy Preserving Machine Learning (NeurIPS Workshop) 2018
- W-7. Ryan McKenna, Gerome Miklau, Michael Hay, *Ashwin Machanavajjhala*, “Optimizing error of high-dimensional statistical queries under differential privacy”, In Theory and Practice of Differential Privacy (TPDP) Workshop 2018
- W-8. Johes Bater, Xi He, William Ehrich, *Ashwin Machanavajjhala*, Jennie Rogers, “ShrinkWrap: Differentially-Private Query Processing in Private Data Federations”, In Theory and Practice of Differential Privacy (TPDP) Workshop 2018

- W-9. Dan Zhang, Ryan McKenna, Ios Kotsogiannis, Gerome Miklau, Michael Hay, *Ashwin Machanavajjhala*, "Ektelo: A Framework for Defining Differentially-Private Computations", In Theory and Practice of Differential Privacy (TPDP) Workshop 2017
- W-10. Nisarg Raval, *Ashwin Machanavajjhala*, Landon P. Cox, "Protecting Visual Secrets Using Adversarial Nets", In CVPR Workshop, COPS 2017
- W-11. Stelios Doudalis, Samuel Haney, *Ashwin Machanavajjhala*, Sharad Mehrotra, "Releasing True Data with Formal Privacy Guarantees", In SIGIR Workshop on Privacy-preserving IR, 2016
- W-12. Samuel Haney, *Ashwin Machanavajjhala*, John Abowd, Matthew Graham, Mark Kutzbach and Lars Vilhuber "The Cost of Provable Privacy: A Case Study on Linked Employer-Employee Data", In Theory and Practice of Differential Privacy (TPDP) Workshop 2016
- W-13. Michael Hay, *Ashwin Machanavajjhala*, Gerome Miklau, Yan Chen, Dan Zhang, "Principled evaluation of differentially private algorithms using DPBench", In Theory and Practice of Differential Privacy (TPDP) Workshop 2016
- W-14. Nisarg Raval, Animesh Srivastava, Kiron Lebeck, Landon Cox, *Ashwin Machanavajjhala*, "MarkIt: Privacy Markers for Protecting Visual Secrets ", Workshop on Usable Privacy & Security for wearable and domestic ubiquitous DEvices (UPSIDE), UbiComp 2014
- W-15. Eunsu Ryu, Yao Rong, Jie Li, *Ashwin Machanavajjhala*, "curso: protect yourself from curse of attribute inference: a social network privacy-analyzer", In *Proc. DBSocial* 2013
- W-16. Adam Silberstein, *Ashwin Machanavajjhala*, Raghu Ramakrishnan, "Feed Following: The Big Data Challenge in Social Applications", In *Proc. DBSocial* 2011 (*invited paper*).
- W-17. Muthuramakrishnan Venkitasubramaniam, *Ashwin Machanavajjhala*, David Martin, Johannes Gehrke, "Trusted CVS", In *ICDE Workshops - STD3S* 2006.

Books.

- B-1. Bee-Chung Chen, Daniel Kifer, Kristen Lefevre, *Ashwin Machanavajjhala* "Privacy-Preserving Data Publishing", In *Foundations and Trends in Databases*, 2(1-2), 2009.

Book Chapters.

- BC-1. Xi He, *Ashwin Machanavajjhala*, "Analyzing Your Location Data with Provable Privacy Guarantees", Chapter in *Springer Handbook on Mobile Data Privacy*, To appear 2017
- BC-2. Johannes Gehrke, *Ashwin Machanavajjhala*, "E-Privacy", Chapter in *Encyclopedia of Cryptography and Security* (2nd Ed.) 424-426, 2011
- BC-3. *Ashwin Machanavajjhala*, Johannes Gehrke, "Randomization Methods to Ensure Data Privacy", Chapter in *Encyclopedia of Database Systems*, Springer, 2009.

Posters and Demos.

- O-1. Zhiqi Huang, Ryan McKenna, George Bissias, Gerome Miklau, Michael Hay, *Ashwin Machanavajjhala*, "PSynDB: Accurate and Accessible Private Data Generation", (Demo) *PVLDB* 12(12)
- O-2. Sameera Ghayyur, Yan Chen, Roberto Yus, *Ashwin Machanavajjhala*, Michael Hay, Gerome Miklau, Sharad Mehrotra, "IOT-DETECTIVE: Analyzing IoT Data Under Differential Privacy", (Demo) *ACM SIGMOD* 2018
- O-3. Ios Kotsogiannis, *Ashwin Machanavajjhala*, Michael Hay, Gerome Miklau, "DIAS: Differentially Private Interactive Algorithm Selection using Pythia", (Demo) *ACM SIGMOD* 2017
- O-4. Stylianos Doudalis, Ios Kotsogiannis, *Ashwin Machanavajjhala* and Sharad Mehrotra, "One-sided Privacy", (Poster) *Theory and Practice of Differential Privacy (TPDP) Workshop* 2017

- O-5. Xi He, Nisarg Raval, *Ashwin Machanavajjhala*, “A Demonstration of VisDPT: Visual Exploration of Differentially Private Trajectories” (Demo) PVLDB 9(13), 2016, **awarded best demo**
- O-6. Xi He, *Ashwin Machanavajjhala*, Cheryl Flynn, Divesh Srivastava, “Composing Differential Privacy and Secure Multiparty Computation for Efficient Private Record Linkage”, (Poster) Theory and Practice of Differential Privacy (TPDP) Workshop 2016
- O-7. Michael Hay, *Ashwin Machanavajjhala*, Gerome Miklau, Yan Chen, Dan Zhang, George Bissias, “Exploring Privacy-Accuracy Tradeoffs using DPComp”, (Demo) SIGMOD Conference 2016
- O-8. Nisarg Raval, Animesh Srivastava, Ali Razeen, Kiron Lebeck, *Ashwin Machanavajjhala*, Landon P. Cox, “Demo: What You Mark is What Apps See”, (Demo) MobiSys 2016
- O-9. *Ashwin Machanavajjhala*, Daniel Kifer, Johannes Gehrke, “Beyond k -Anonymity: New Schemes for Privacy Preserving Data Publishing”, (Poster) **Best Visionary Poster** In *DB/IR Day*, April, 2005.
- O-10. Adina Crainiceanu, Prakash Linga, *Ashwin Machanavajjhala*, Johannes Gehrke, Jayavel Shanmugasundaram, “An Indexing Framework for P2P Systems”, (Demo) In *Proc. SIGMOD* 2004.
- O-11. Adina Crainiceanu, Prakash Linga, *Ashwin Machanavajjhala*, Johannes Gehrke, Jayavel Shanmugasundaram, “A Storage and Indexing Framework for P2P Systems”, (Poster) In *Proc. WWW* 2004.

Other Manuscripts

- M-1. Amol Deshpande and *Ashwin Machanavajjhala*, “Privacy Challenges in the Post-GDPR World: A Data Management Perspective”, SIGMOD Blog, October 2018
- M-2. John Abowd, Lorenzo Alvisi, Cynthia Dwork, Sampath Kannan, *Ashwin Machanavajjhala*, Jerome Reiter, “Privacy-Preserving Data Analysis for the Federal Statistical Agencies”, CoRR abs/1701.00752, 2017
A white paper prepared for the Computing Community Consortium committee of the Computing Research Association.
- M-3. Yan Chen, *Ashwin Machanavajjhala*, “On the Privacy Properties of Variants on the Sparse Vector Technique”, CoRR abs/1508.07306, 2015
- M-4. Ben Stoddard, Yan Chen, *Ashwin Machanavajjhala*, “Differentially Private Algorithms for Empirical Machine Learning”, CoRR abs/1411.5428, 2014

Tutorials & Bootcamps

- T-1. “Differential Privacy BootCamp: for Employees of the US Federal Statistical Agencies” with Gerome Miklau, Michael Hay and Daniel Kifer, Bureau of Labor Statistics, Sep 2019
- T-2. “Differential Privacy BootCamp: for Employees of the US Census Bureau” with Gerome Miklau, Michael Hay and Daniel Kifer, National Academies of Sciences, June 2019
- T-3. “Differential Privacy in the Wild: A tutorial on current practices & open challenges.” with Xi He and Michael Hay, ACM SIGMOD, 2017
- T-4. “Differential Privacy in the Wild: A tutorial on current practices & open challenges.” with Xi He and Michael Hay, PVLDB 9(13), 2016
- T-5. “Entity Resolution for Big Data”, with Lise Getoor, ACM SIGKDD Conference, 2013
- T-6. “Entity Resolution: Theory, Practice & Open Challenges” with Lise Getoor, PVLDB 5(12), 2012
- T-7. “Entity Resolution: Theory, Practice and Open Challenges” with Lise Getoor, AAAI Conference, 2012
- T-8. “Privacy in Data Publishing” with Johannes Gehrke and Daniel Kifer, IEEE ICDE, 2010

T-9. "Models and Methods for Disclosure Limitation" with Johannes Gehrke, IEEE Security and Privacy, 2009

Patents

- P-1. Srjana Merugu, Philip Bohannon, Pedro DeRose, *Ashwin Machanavajhala*, "System for Opinion Reconciliation," US Patent # 7,895,149.
- P-2. Erik Vee, Minos Garofalakis, Jayavel Shanmugasundaram, *Ashwin Machanavajhala*, "System and/or Method for Processing Events," US Patent # 7,890,494.
- P-3. Sathya K. Selvaraj, Philip L. Bohannon, Mridul Muralidharan, Cong Yu, *Ashwin Machanavajhala*, Arun S. Iyer and Sundararajan Sellamanickam, "Large Scale Entity-Specific Resource Classification", US Patent Publication 20110264651
- P-4. Srjana Merugu, Arun Shankar Iyer, *Ashwin Machanavajhala*, Sathya Keerthi Selvaraj, and Philip L. Bohannon "Opinion Aggregation System", US Patent Publication 20110264651
- P-5. Jayavel Shanmugasundaram, Minos Garofalakis, Erik Vee, *Ashwin Machanavajhala*, "Method for Generating Score-Optimal R-Trees," US Patent Publication 20100036865
- P-6. Adam Silberstein, *Ashwin Machanavajhala*, "User Behavior-Driven Background Cache Refreshing," US Patent Publication 20130159274.

Funding

- F-1. Ashwin Machanavajhala (co-PI), with Kartik Nayak (PI), Jun Yang (co-PI) and Lavanya Vasudevan (co-PI)
"RAPID: Poirot: From Contact Tracing to Private Exposure Detection"
NSF SaTC RAPID, May 2020 – April 2021, \$200,00.00
- F-2. Ashwin Machanavajhala (co-I), with Jun Yang (co-PI) (subaward of a grant led by UT Arlington)
"Convergence Accelerator Phase I (RAISE): Credible Open Knowledge Network"
NSF C-Accel Pilot, Sep 2019 – May 2020, \$999,870.00
(\$90,000 for expenditures at Duke)
- F-3. Ashwin Machanavajhala (co-PI), with Lavanya Vasudevan (PI), Geeta Swamy (co-PI), Jun Yang (co-PI)
"Vaccine misinformation and its link to vaccine hesitancy and uptake in Durham"
Duke Bass Connections Project, July 2018 – June 2019. \$25,000
- F-4. Ashwin Machanavajhala (co-PI), with Gerome Miklau (PI, UMass Amherst), Michael Hay (Colgate)
"System P: A Data Analytics Engine With Customizable Privacy and Optimized Utility"
DARPA Brandeis Program, Oct 2015 – Apr 2020. \$2,746,504
(\$1.2 million for expenditures at Duke)
- F-5. Ashwin Machanavajhala (co-PI), with Jerome Reiter (PI), John de Figueiredo (co-PI)
"An Integrated System for Public/Private Access to Large-scale, Confidential Social Science Data"
NSF CIF21 DIBBS, Jan 2015 – Dec 2017. \$1,498,683
- F-6. Ashwin Machanavajhala (PI), with Gerome Miklau (lead PI, UMass Amherst), Michael Hay (PI, Colgate)
"ReDP: Realistic Data Mining Under Differential Privacy"
NSF Secure and Trustworthy Computing, Aug 2014 – July 2018. \$449,999
- F-7. Ashwin Machanavajhala (co-PI), with Landon Cox (PI) "Protecting Visual Secrets with PrivateEye"
Google Faculty Research Award Oct 2014 – Sep 2015. \$53,098

- F-8. Ashwin Machanavajhala (PI) "PROTEUS: A Practical and Rigorous Toolkit for Privacy"
NSF Faculty Early Career Development (CAREER) Program, Feb 2013 – Jan 2018. \$520,219
- F-9. Ashwin Machanavajhala (PI) "PROTEUS: A Practical and Rigorous Toolkit for Privacy"
Google Faculty Research Award, Jun 2013 – May 2014. \$53,032
- F-10. Ashwin Machanavajhala (PI), with Bernard Fuemmeler (co-I), F. Joseph McClernon (co-I), Lavanya Vasudevan (co-I), Sohayla Pruitt (co-I), Lisa P. Davis (co-I), Marie Lynn Miranda
"CHARM: Community Health and Resource Mapping Project"
Information Initiative at Duke Research Incubator Award, Jul 2013 – Jun 2014. \$50,000

Media Coverage

- M-1. "New Tools Safeguard Census Data About Where You Live And Work"
by Robin. A Smith, Duke Today May 18, 2017
- M-2. "Duke Researchers Develop New Video Privacy Software" (Radio Interview)
by Eddie Garcia WFDD Public Radio for the Piedmont, NC. July 5, 2016
- M-3. "Video privacy software lets you select what others can see"
by Robin. A Smith, Duke Today and Phys.org. June 28, 2016
- M-4. "UMass Amherst Computer Scientists Receive Grant to Enhance Data Privacy."
by Janet Lathrop, UMass Amherst News Service. October 15, 2015.
- M-5. "The Fundamental Limits of Privacy For Social Networks."
A View from Emerging Technology from the arXiv, MIT Technology Review, May 5, 2010

Selected Talks

- T-1. Vancouver BC, Canada, "Fair Decision Making using Privacy-Protected Data", December 2019
Invited Talk, Privacy Preserving Machine Learning (PriML, NeurIPS Workshop) 2019
- T-2. Washington DC, "Moving from research to practice: How to maximize the impact of SaTC projects",
October 2019
Panel, NSF SaTC PI Meeting 2019
- T-3. Durham NC, "Architecting a Differentially Private SQL Engine", October 2019
Invited Talk, Triangle Area Privacy and Security Day (TAPS) 2019
- T-4. National Academies of Science, Washington DC, "Privately Releasing Statistics", June 2019
Panel on Current Capabilities of Differential Privacy, CNStat Privacy Workshop
- T-5. UC Santa Cruz, "Differential Privacy for Relational Data", Invited Talk, Privacy in Graphs Workshop,
October 2018
- T-6. Harvard University, "Deploying Differential Privacy U.S. Census Bureau", Invited Talk, DP Deployed
Workshop, September 2018
- T-7. Boston University, "Data Science with Provable Privacy Guarantees", Colloquium, April 2018
- T-8. Dallas, TX, "Differential Privacy & Internet of Things", November 2017
Panelist, ACM CCS Workshop on Multimedia Privacy and Security
- T-9. Rutgers University, "Differential Privacy & Relational Databases: A case study on Census Bureau Data",
October 2017, Invited Talk, DIMACS/Northeast Big Data Hub Workshop on Overcoming Barriers to
Data Sharing including Privacy and Fairness

- T-10. University of Wisconsin, Madison, "Differential Privacy & Relational Databases", October 2017, Invited Talk, Database Seminar, Department of Computer Science
- T-11. San Diego, CA, " ℓ -diversity: The Last Decade", May 2017
IEEE ICDE Influential Paper Award Talk
- T-12. University of California, Irvine, "Utility Cost of Provable Privacy: A case study on US Census Bureau Data", May 2017, Invited Talk, CS Seminar Series, Department of Computer Science
- T-13. Emory University, "Utility Cost of Provable Privacy: A case study on US Census Bureau Data", March 2017, Invited Talk, Department of Mathematics and Computer Science
- T-14. Harvard University, "Utility Cost of Provable Privacy: A case study on US Census Bureau Data", March 2017, Invited Talk, Center for Research on Computation and Society (CRCS)
- T-15. Washington DC, "Building differentially private systems: opportunities and challenges.", Jan 2017
Moderator, Breakout Session, NSF SaTC PI Meeting 2017
- T-16. Washington DC, "Providing public and private access to confidential social science data", Dec 2016
Invited Talk, Federal Committee for Statistical Methodology (FCSM) Policy Conference 2016
- T-17. Pisa, Italy, "Differential Privacy in the Wild", July 2016
Keynote Talk, PrivacyPreserving IR Workshop at SIGIR 2016
- T-18. Indiana University Bloomington, "Provable Privacy in the Wild", April 2015
CACR Security Seminar
- T-19. Indian Institute of Technology - Bombay, "Small Devices, Big Data and Individual Privacy", Dec 2014
Invited Talk
- T-20. Boston, MA, "Differential Privacy in the Wild: Challenges and Open Questions", May 2014
Invited Talk, Charles River Workshop: Privacy & Social Networks
- T-21. Duke University, "Big-data and Individual Privacy", Apr 2014
Invited Talk, mHealth@Duke Conference
- T-22. U.S. Census Bureau, "Tuning Privacy-Utility Tradeoffs in Statistical Databases Using Policies", Aug 2013
Center For Statistical Research & Methodology Seminar
- T-23. M.I.T., "No Free Lunch and the Pufferfish approach to privacy", Jun 2013
Invited Talk, MIT Big Data Privacy Workshop
- T-24. Rutgers University "Pufferfish: A Semantic Approach to the Privacy of Correlated Data", Oct 2012
Invited Talk, DIMACS Workshop on Differential Privacy across Computer Science
- T-25. University of California, San Diego, "Pufferfish: A Semantic Approach to the Privacy of Correlated Data", Sep 2012, Invited Talk, iDASH Privacy Workshop
- T-26. Maui, HI, "Challenges in Enabling Social Applications at Scale" Oct 2012
Keynote Talk, International Workshop on Cloud Data Management at CIKM 2012
- T-27. University of Colorado, Denver, "No Free Lunch in Data Privacy", 2012
Keynote Talk, CRISP Workshop on Information Security & Privacy

Teaching

- T-1. "Privacy and Fairness in Data Science", Compsci 590, **Fall 2018**
- T-2. "Everything Data", CompSci 216, **Spring 2019, 2018, 2017, 2015, 2014**

T-3. “Design of Stable Algorithms for Privacy and Learning”, Compsci 590, **Fall 2016**

T-4. “Algorithms for Big Data”, CompSci 590, **Fall 2015, Spring 2013**

T-5. “Privacy in a Mobile-Social World”, CompSci 590, **Fall 2013, 2012**

Top 5% of all undergraduate instructors for a small class for *Quality of Course/Intellectual Stimulation*, 2013

Students & Mentoring

Graduated Ph.D. Students

Ios Korsogiannis, August 2018

▷ First Employment: Snap Inc

Nisarg Raval, May 2018

▷ First Employment: LinkedIn

Xi He, August 2018

▷ Department of Computer Science **Outstanding Ph.D. Thesis Award winner**, 2018

▷ **Google PhD Fellowship in Privacy & Security**, 2017

▷ First Employment: Asst. Prof., Cheriton School of Computer Science, University of Waterloo

Yan Chen, May 2018

▷ First Employment: Google

Graduated Masters Students

Benjamin Stoddard, M.S 2017

▷ First Employment: Google

Bharat Chelepalli, M.S 2013

▷ Department of Computer Science **Outstanding M.S. Award winner**, 2013

▷ First Employment: Amazon

Current PhD Students

Yuchao Tao, expected graduation 2022

Chenghong Wang, expected graduation 2023

David Pujol, expected graduation 2023

Shweta Patwa, expected graduation 2023

Dissertation Committees

Dept. of Computer Science, Duke: Junyang Gao, Caitlin O’ Hanlon, Samuel Haney, Prajakta Kalmegh, Brett Walenz (graduated 2018), Risi Thonangi (graduated 2015), You (William) Wu (graduated 2015), Albert Yu (graduated 2013)

Dept. of Stat. Sci., Duke: Lan Wei (graduated 2016), David McClure (graduated 2016), Monika Jingchen HU (graduated 2015)

Dept. of Math and CS, Emory: Yonghui Xiao (graduated 2017)

Dept. of Computer Science, UIUC: Bolin Ding (graduated 2011)

Other Supervised Students

Yahoo! Summer Internship Mentor: Aditya Pal (University of Minnesota, Twin Cities, 2011), Lorenzo Blanco (Università degli Studi Roma, 2010), Aleksandra Korolova (Stanford University, 2009), Kedar Bellare (University of Massachusetts, Amherst, 2009), Ioannis Antonellis (Stanford University, 2009)

Service

Organizing Activities

Co-Chair, First Annual Triangle Privacy & Security Day (TAPS) 2019
 Local Arrangements Chair, ACM Conference on Management of Data (SIGMOD), 2017
 Publicity Chair, ACM Conference on Management of Data (SIGMOD), 2014
 Co-Chair, Third ACM Workshop on Databases & Social Networks, 2013

Program Committees & Panels

PC Member, ACM Conference on Management of Data (SIGMOD), 2009, 2012-19
 ▷ **Distinguished PC Member**, SIGMOD 2017, 2019
 Review Board, Proceedings of the VLDB Endowment (PVLDB), 2012-16, 2018-19
 PC Member, ACM Conference on Computer and Communications Security (CCS), 2015, 2019
 PC Member, ACM Conference on Principles of Database Systems (PODS), 2019
 PC Member, Proceedings on Privacy Enhancing Technologies (PoPETS), 2015, 2018-19
 PC Member, International Conference on Data Engineering (ICDE), 2012, 2014-15, 2017-18
 Panel Member, National Science Foundation, 2012, 2013, 2014, 2015
 PC Member, ACM Conference on Knowledge Discovery and Data Mining (KDD), 2013-14, 2016
 PC Member, International Conference on Database Theory (ICDT), 2017
 PC Member, ACM Symposium on Cloud Computing (SOCC), 2014
 PC Member, ACM Conference on World Wide Web (WWW), 2013
 PC Member, ACM Conference on Information and Knowledge Management (CIKM), 2013, 2019
 PC Member, IEEE International Conference on Big Data, 2013
 PC Member, Workshop on Privacy in Electronic Society (WPES), 2012-14
 PC Member, Conference on Very Large Databases (VLDB), 2010

Reviewer.

Reviewer, Proceedings of the National Academy of Sciences
 Reviewer, Journal of ACM
 Reviewer, Journal on Very Large Databases
 Reviewer, Transactions on Database Systems
 Reviewer, Journal of Machine Learning Research
 Reviewer, Transactions on Knowledge and Data Engineering
 Reviewer, Transactions on Information and Systems Security
 Reviewer, Journal of Computer and System Sciences
 Reviewer, Journal of Privacy and Confidentiality
 Reviewer, International Journal on Knowledge and Information Systems

Department & University Service

Director of Graduate Studies, Duke CS, 2018-2019
 Member, Graduate Admissions Committee, Duke CS, 2012-2013, 2019-current
 Member, Faculty Search Committee, Duke CS, 2014-2015, 2016-2017, 2017-2018
 Member, Communications Committee, Duke CS, 2017-2018
 Member, Graduate Program Committee, Duke CS, 2017-2018
 Member, Information Initiative @ Duke Infrastructure Committee, 2013-2014