Peter Kairouz

(217) 550-2697 kairouz@google.com
4218 Stone Way N, Seattle, WA 98103 kairouzp.github.io

CURRENT POSITION

Research Scientist Seattle, WA
Research and Machine Intelligence, Google Jul. 2018 - Present
Federated, Differentially Private, and Robust Machine Learning

EXPERIENCE

Research Fellow Stanford, CA
Information Systems Laboratory, Stanford University Sep. 2016 – Jul. 2018
On-Device Artificial Intelligence and Differential Privacy

Rsearch Assistant Champaign, IL
Coordinated Science Laboratory, University of Illinois Jan. 2013 – Aug. 2016
Mathematical Foundations of Data Privacy and Anonymous Communication

Research Intern Seattle, WA
Research and Machine Intelligence, Google May 2015 – Sep. 2015
Privacy-Preserving Machine Learning Algorithms

Research Intern San Diego, CA
Qualcomm Research, Qualcomm May 2013 – Sep. 2013
Interference-Aware Rate Control for Small Cells

Research Assistant Champaign, IL
Coordinated Science Laboratory, University of Illinois Aug. 2010 – Dec. 2012
Multi-Input Multi-Output Communications over Optical Networks

Research Intern San Diego, CA
Qualcomm Research, Qualcomm May 2012 – Sep. 2012
Variable Block Length Coding for LTE Systems

Research Intern College Park, MD
Center for Automation Research, University of Maryland Jun. 2009 – Sep. 2009
Face Recognition Algorithms for Large Datasets

EDUCATION

Stanford University Stanford, CA
Postdoctoral Research Fellow Jul. 2018

University of Illinois at Urbana-Champaign Champaign, IL
Ph.D. in Electrical and Computer Engineering May 2016

University of Illinois at Urbana-Champaign Champaign, IL
Master of Science in Applied Mathematics: Optimization and Algorithms May 2016

University of Illinois at Urbana-Champaign Champaign, IL
Masters of Science in Electrical and Computer Engineering Dec. 2012

American University of Beirut Lebanon
Bachelor of Engineering in Electrical and Computer Engineering Jun. 2010

AWARDS

University of Illinois at Urbana-Champaign
Harold L. Olesen Award for Excellence in Undergraduate Teaching (Jan. 2016)

Association for Computing Machinery
Best Paper Award at ACM SIGMETRICS 2015 (Jun. 2015)

Qualcomm Incorporated
Qualcomm Innovation Fellowship Finalist Award (Dec. 2014)
The 2012 Roberto Padovani Scholarship (Dec. 2012)

American University of Beirut
Distinguished ECE Graduate Award (Jun. 2010)
Graduated with High Honors (May 2010)
Dean's Honor List for outstanding academic performance (Aug. 2006 – May 2010)
Benjamin Franklin Scholarship from the US Agency for International Development (Aug. 2006)

PUBLICATIONS

Manuscripts and Preprints:

1. Peter Kairouz, H Brendan McMahan, et al. Advances and open problems in federated learning. *arXiv preprint arXiv:1912.04977*
2. Ziteng Sun, Peter Kairouz, Ananda Theertha Suresh, and H Brendan McMahan. Can you really backdoor federated learning? *arXiv preprint arXiv:1911.07963*
3. Mario Diaz, Peter Kairouz, Jiachun Liao, and Lalitha Sankar. Theoretical guarantees for model auditing with finite adversaries. *arXiv preprint arXiv:1911.03405*
4. Peter Kairouz, Jiachun Liao, Chong Huang, and Lalitha Sankar. Learning generative adversarial representations (gap) under fairness and censoring constraints. *arXiv preprint arXiv:1910.00411*
5. Tyler Sypherd, Mario Diaz, Harshit Laddha, Lalitha Sankar, Peter Kairouz, and Gautam Dasarathy. A class of parameterized loss functions for classification: Optimization tradeoffs and robustness characteristics. *arXiv preprint arXiv:1906.02314*
6. Jayadev Acharya, Keith Bonawitz, Peter Kairouz, Daniel Ramage, and Ziteng Sun. Context-aware local differential privacy. *arXiv preprint arXiv:1911.00038*
7. H Brendan McMahan, Galen Andrew, Ulfar Erlingsson, Steve Chien, Ilya Mironov, Nicolas Papernot, and Peter Kairouz. A general approach to adding differential privacy to iterative training procedures. *arXiv preprint arXiv:1812.06210*

Workshop Papers:

1. Ziteng Sun, Peter Kairouz, Ananda Theertha Suresh, and H Brendan McMahan. Can you really backdoor federated learning? *Federated Learning for Data Privacy and Confidentiality, (NeurIPS)*, 2019
2. Wennan Zhu, Peter Kairouz, Haicheng Sun, Brendan McMahan, and Wei Li. Federated heavy hitters discovery with differential privacy. *Theory and Practice of Differential Privacy, (CCS)*, 2019
3. Jayadev Acharya, Keith Bonawitz, Peter Kairouz, Daniel Ramage, and Ziteng Sun. Context-aware local differential privacy. *Theory and Practice of Differential Privacy, (CCS)*, 2019
4. Lillian Clark, Matthew Clark, Konstantinos Psounis, and Peter Kairouz. Privacy-utility trades in wireless data via optimization and learning. *Information Theory and Applications (ITA) Workshop*, 2019

5. Tyler Sypherd, Lalitha Sankar, Mario Diaz, Peter Kairouz, and Gautam Dasarathy. A class of parameterized loss functions for classification: Optimization tradeoffs and robustness characteristics. *Information Theory and Machine Learning, (NeurIPS)*, 2019

6. Tyler Sypherd, Lalitha Sankar, Mario Diaz, Peter Kairouz, and Gautam Dasarathy. A class of parameterized loss functions for classification: Optimization tradeoffs and robustness characteristics. *Machine Learning with Guarantees, (NeurIPS)*, 2019

7. Peter Kairouz, Chong Huang, Xiao Chen, Ram Rajagopal, and Lalitha Sankar. Generative adversarial privacy. *Privacy in Machine Learning and Artificial Intelligence (ICML)*, 2018

8. Witold Oleszkiewicz, Tomasz Włodarczyk, Karol Piczak, Tomasz Trzciński, Peter Kairouz, and Ram Rajagopal. Siamese generative adversarial privatizer for biometric data. *Challenges and Opportunities for Privacy and Security (CVPR)*, 2018

9. Peter Kairouz, Sewoong Oh, and Pramod Viswanath. Differentially private multi-party computation. *Private Multi-Party Machine Learning, (NeurIPS)*, 2016

Journal Papers:

1. Huseyin A Inan, Peter Kairouz, and Ayfer Özgür. Sparse combinatorial group testing. *IEEE Transactions on Information Theory*, 2019

2. Huseyin A Inan, Peter Kairouz, Mary Wootters, and Ayfer Özgür. On the optimality of the kautz-singleton construction in probabilistic group testing. *IEEE Transactions on Information Theory*, 2019

3. Chong Huang*, Peter Kairouz*, Xiao Chen, Lalitha Sankar, and Ram Rajagopal. Context-aware generative adversarial privacy. *Entropy*, 2017

4. Peter Kairouz, Sewoong Oh, and Pramod Viswanath. The composition theorem for differential privacy. *IEEE Transactions on Information Theory*, 2017

5. Giulia Fanti*, Peter Kairouz*, Sewoong Oh, Kannan Ramchandran, and Pramod Viswanath. Hiding the rumor source. *IEEE Transactions on Information Theory*, 2017

6. Peter Kairouz, Sewoong Oh, and Pramod Viswanath. Extremal mechanisms for local differential privacy. *Journal of Machine Learning Research (JMLR)*, 2016

7. Giulia Fanti*, Peter Kairouz*, Sewoong Oh, Kannan Ramchandran, and Pramod Viswanath. Metadata-conscious anonymous messaging. *IEEE Transactions on Signal and Information Processing over Networks*, 2016

8. Quan Geng, Peter Kairouz, Sewoong Oh, and Pramod Viswanath. The staircase mechanism in differential privacy. *IEEE Journal of Selected Topics in Signal Processing*, 2015

Conference Papers:

1. Wennan Zhu, Peter Kairouz, Haicheng Sun, H Brendan McMahan, and Wei Li. Federated heavy hitters discovery with differential privacy. *International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2020

2. Sean Augenstein, H Brendan McMahan, Daniel Ramage, Swaroop Ramaswamy, Peter Kairouz, et al. Generative models for effective ML on private, decentralized datasets. *International Conference on Learning Representations (ICLR)*, 2020

3. Reihaneh Torkzadehmahani, Peter Kairouz, and Benedict Paten. DP-CGAN: Differentially private synthetic data and label generation. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 2019

4. Huseyin A Inan, Surin Ahn, Peter Kairouz, and Ayfer Özgür. A group testing approach to random access for short-packet communication. In *IEEE International Symposium on Information Theory (ISIT)*, 2019

5. Tyler Sypherd, Mario Diaz, Lalitha Sankar, and Peter Kairouz. A tunable loss function for binary classification. *IEEE International Symposium on Information Theory (ISIT)*, 2019

6. Witold Oleszkiewicz, Peter Kairouz, Karol Piczak, Ram Rajagopal, and Tomasz Trzciński. Siamese generative adversarial privatizer for biometric data. In *Asian Conference on Computer Vision (ACCV)*, 2018

7. Chong Huang, Peter Kairouz, and Lalitha Sankar. Generative adversarial privacy: A data-driven approach to information-theoretic privacy. In *Asilomar Conference on Signals, Systems, and Computers*, 2018

8. Xiao Chen, Peter Kairouz, and Ram Rajagopal. Understanding adversarial compression in privacy applications. *IEEE Conference on Decision and Control (CDC)*, 2108

9. Huseyin Inan, Peter Kairouz, and Ayfer Ozgur. Energy-limited massive random access via noisy group testing. *IEEE International Symposium on Information Theory (ISIT)*, 2018

10. Huseyin Inan, Peter Kairouz, and Ayfer Ozgur. Sparse group testing codes for low-energy massive random access. *Allerton Conference on Communications, Control, and Computing*, 2017

11. Kabir Chandrasekher, Kangwook Lee, Peter Kairouz, Ramtin Pedarsani, and Kannan Ramchandran. Asynchronous and noncoherent neighbor discovery for the IoT using sparse-graph codes. *IEEE International Conference on Communications (ICC)*, 2017

12. Peter Kairouz, Keith Bonawitz, and Daniel Ramage. Discrete distribution estimation under local privacy. *International Conference on Machine Learning (ICML)*, 2016

13. Giulia Fanti*, Peter Kairouz*, Sewoong Oh, Kannan Ramchandran, and Pramod Viswanath. Metadata-conscious anonymous messaging. *International Conference on Machine Learning (ICML)*, 2016

14. Giulia Fanti*, Peter Kairouz*, Sewoong Oh, Kannan Ramchandran, and Pramod Viswanath. Rumor source obfuscation on irregular trees. *ACM SIGMETRICS Performance Evaluation Review*, 2016

15. Peter Kairouz, Sewoong Oh, and Pramod Viswanath. Differentially private multi-party computation. *Conference on Information Sciences and Systems (CISS)*, 2016

16. Peter Kairouz, Sewoong Oh, and Pramod Viswanath. Secure multi-party differential privacy. *Advances in Neural Information Processing Systems (NeurIPS)*, 2015

17. Giulia Fanti*, Peter Kairouz*, Sewoong Oh, and Pramod Viswanath. Spy vs. spy: Rumor source obfuscation. *ACM SIGMETRICS Performance Evaluation Review*, 2015. [**Best Paper Award**]

18. Peter Kairouz, Sewoong Oh, and Pramod Viswanath. The composition theorem for differential privacy. *International Conference on Machine Learning (ICML)*, 2015

19. Peter Kairouz, Sewoong Oh, and Pramod Viswanath. Extremal mechanisms for local differential privacy. *Advances in Neural Information Processing Systems (NeurIPS)*, 2014

20. Peter. Kairouz, Ahmed Sadek, and Tamer Kadous. Interference aware rate control for bursty interference channels. *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2013

21. Peter Kairouz, Aolin Xu, Naresh Shanbhag, and Andrew Singer. A sphere decoding approach for the vector viterbi algorithm. *Asilomar Conference on Signals, Systems and Computers*, 2012

22. Andrew Bean, Peter Kairouz, and Andrew Singer. Convergence rates for cooperation in heterogeneous populations. *Asilomar Conference on Signals, Systems and Computers*, 2012

PATENTS

1. Peter Kairouz, Ahmed Kamel Sadek, Kambiz Azarian Yazdi, and Nachiappan Valliappan. Interference management in a bursty-interference environment, February 4 2016. US Patent 20,160,037,363

2. Peter Kairouz, Ahmed Kamel Sadek, Kambiz Azarian Yazdi, and Nachiappan Valliappan. Bursty-interference-aware interference management, February 4 2016. US Patent 20,160,037,364

3. Peter Kairouz, Ahmed Kamel Sadek, and Tamer Adel Kadous. Variable block length and superposition coding for hybrid automatic repeat request, September 12 2013. US Patent App. 14/025,713

SELECTED TALKS

1. *Federated Learning, Threat Models, and Differential Privacy*, Microsoft Research (Nov. 2019)

2. *Decentralized and Privacy-Preserving ML via TensorFlow Federated*, PyConDE & PyData Berlin (Oct. 2019)

3. *Federated Heavy Hitters Discovery with Differential Privacy*, Symposium on Information-Theoretic Methods for Privacy at the Simons Institute for the Theory of Computing (Apr. 2019)

4. *Evaluating Privacy and Fairness Schemes via Adversarial Threat Models*, Symposium on Information-Theoretic Methods for Privacy at the Simons Institute for the Theory of Computing (Mar. 2019)

5. *Generative Adversarial Models for Privacy and Fairness*, Symposium on Information-Theoretic Methods for Privacy at the Simons Institute for the Theory of Computing (Mar. 2019)

6. *Designing and Evaluating Privacy Mechanisms via Generative Adversarial Networks*, Qualcomm Research (Feb. 2019)

7. *Federated Learning in Practice at Google*, Applied Machine Learning Days (Jan. 2019)

8. *A Discussion on Data and Privacy*, Forbes Councils (Nov. 2018)

9. *Generative Adversarial Privacy*, Privacy in Machine Learning and Artificial Intelligence Workshop at ICML (Jul. 2018)

10. *From Differential Privacy to Generative Adversarial Privacy*, Google, University of Toronto, ETHZ, EPFL, USC, ASU, KAUST, AUB, and Stanford University (Feb. 2018 - Mar. 2018)

11. *Generative Adversarial Privacy*, Mathematical Foundations of Data Privacy at Banff International Research Station (May. 2018)

12. *Generative Adversarial Privacy*, Information Theory & Applications Workshop (Feb. 2018)

13. *Embracing Uncertainty*, Stanford SystemX IoE Workshop (May 2017)

14. *Scaling Wireless Networks to the Next Trillion Devices*, Stanford SystemX IoE Workshop (Nov. 2016)

15. *The Fundamental Limits of Statistical Data Privacy*, University of Southern California (Apr. 2016)

16. *Metadata-Conscious Anonymous Messaging*, ICML 2016 (Jun. 2016)

17. *Discrete Distribution Estimation Under Local Privacy*, ICML 2016 (Jun. 2016)

18. *The Fundamental Limits of Differential Privacy*, Information Theory & Applications Workshop (Feb. 2016)

19. *The Composition Theorem for Differential Privacy*, ICML 2015 (Jun. 2015)

20. *Spy vs. Spy: Rumor Source Obfuscation*, SIGMETRICS 2015 (Jun. 2015)

21. *Extremal Mechanisms for Local Differential Privacy*, Google (Jun. 2015)

22. *Spy vs. Spy: Rumor Source Obfuscation*, Qualcomm (Mar. 2015)

SUPERVISORY EXPERIENCE

Mr. Ziteng Sun Jun. 2019 – Present
Google Intern and PhD student at Cornell
Project: Backdoor Attacks on Federated Learning

Miss Wennan Zhu Jun. 2019 – Sep. 2019
Google Intern and PhD student at RPI
Project: Federated Analytics with Differential Privacy

Mr. Huseyin Inan Jan. 2017 – Jul. 2018
PhD student at Stanford University
Project: Sparse Combinatorial Codes for Massive Random Access

Mr. Chong Huang Jan. 2017 – Jul. 2018
PhD student at Arizona State University
Project: Generative Adversarial Privacy

Mr. Xiao (Mark) Chen Dec. 2016 – Jul. 2018
PhD student at Stanford University
Project: Privacy-Preserving Algorithms for Smart Meter Data

Miss Hawraa Salami Jun. 2012 – Sep. 2012
PhD student at University of California, Los Angeles
Project: Low Complexity Algorithms for MIMO Communication Systems

Mr. Rohan Bali Sep. 2011 – Dec. 2011
Research Engineer at Oculus Research
Project: Detection Algorithms for Multi-Mode Optical Fiber Communication

Mr. Zhiyuan Zheng Sep. 2011 – Dec. 2011
Software Engineer at Yahoo!
Project: Detection Algorithms for Multi-Mode Optical Fiber Communication

CONTRIBUTIONS TO PROPOSALS

1. *Generative Adversarial Privacy: A Data-driven Approach to Guaranteeing Privacy and Utility*, NSF CCF, Program Solicitation Number: NSF 17-571, PI: Lalitha Sankar ($500,000)
2. *Massive Wireless Random Access: Principles and Protocols*, NSF CNS, Program Solicitation Number: NSF 17-570, PI: Ayfer Ozgur ($500,000)
3. *HeimdalNet: a Radio Frequency Machine Learning System*, DARPA RFMLS program, BAA HR001117S0043, PI: Rockwell Collins (under review)
4. *Statistical Data Privacy: Fundamental Limits and Efficient Algorithms*, NSF CCF, Award Number: 1422278, PI: Pramod Viswanath ($500,000)

TEACHING EXPERIENCE

Courses Developed
ECE Department, University of Illinois

- Making Sense of Big Data (Spring 2014, Fall 2014, Spring 2016)
- Digital Signal Processing Lab (Summer 2011)

Courses Taught

ECE Department, University of Illinois

- Probabilities with Engineering Applications (Fall 2015)
- Digital Signal Processing (Summer 2011)

Teaching Assistant

ECE Department, American University of Beirut

- Computer Networks (Spring 2010)
- Communication Systems (Fall 2009)
- Introduction to Programming (Spring 2008)

PROFESSIONAL SERVICES

Workshops and Tutorials Organized

- Google Workshop on Federated Learning and Analytics (Summer 2019)
- Privacy and Fairness in Data Science: An Information-Theoretic Perspective at ISIT (Summer 2019)

Conferences Organized

- General Chair for the 10th Annual CSL Student Conference (Spring 2015)
- Media Chair for the 6th Annual CSL Student Conference (Spring 2011)

Technical Program Committee Member

- Proceedings of Privacy Enhancing Technologies (PoPETs)
- ACM Conference on Computer and Communications (CCS)
- Symposium on Theory of Computing (STOC)
- Neural Information Processing Systems (NeurIPS)
- International Conference on Machine Learning (ICML)
- International Conference on Artificial Intelligence and Statistics (AISTATS)
- Journal of Machine Learning Research (JMLR)
- Theory of Computing (ToC)
- ACM Transactions on Economics and Computation (TEAC)
- IEEE Information Theory Workshop (ITW)
- IEEE Transactions on Information Theory (TIT)
- IEEE Transactions on Knowledge and Data Engineering (TKDE)
- IEEE International Symposium on Information Theory (ISIT)

Memberships

- IEEE Member
- IEEE Information Theory Society Santa Clara Valley Chapter, Treasurer

REFERENCES

Pramod Viswanath
Professor
ECE
University of Illinois
pramodv@illinois.edu

Sewoong Oh
Professor
CS
University of Washington
sewoong@cs.washington.edu

Ayfer Özgür
Professor
EE
Stanford University
aozgur@stanford.edu

Ram Rajagopal
Professor
CEE
Stanford University
ramr@stanford.edu

Kannan Ramchandran
Professor
EECS
UC Berekely
kannanr@berkeley.edu

Brendan McMahan
Research Scientist
Google AI
Google
mcmahan@google.com

Daniel Ramage
Research Scientist
Google AI
Google
dramage@google.com

Lalitha Sankar
Assistant Professor
ECE
ASU
lsankar@asu.edu