Hanshen Xiao

MIT Stata Center G890,
32 Vassar St,
Cambridge, MA, USA, 02139.

hsxiao@mit.edu
(+1) 617-682-2584
https://hanshen-xiao.github.io/

INTERESTS

Information Security and Privacy: Automatic Privacy Proof, High-Dimensional Privacy-Preservation Technology, Differential Privacy, and PAC Privacy.
Byzantine Tolerance and Robustness: (Byzantine) Robust Machine Learning, Byzantine Consensus, and Robust Statistics.
Information Theory and Signal Processing: Constrained Sampling Theory and Compressed Sensing.

EDUCATION

Massachusetts Institute of Technology — Cambridge, MA, USA
Ph.D in Computer Science — 2019 - 2024
Advisor: Prof. Srinivas Devadas

M.S. in Computer Science, GPA: 5.0/5.0 — 2017 - 2019
- ★ Thesis: Local differential privacy in decentralized optimization
- ★ Advisor: Prof. Srinivas Devadas

Tsinghua University — Beijing, China
B.S. in Mathematics (with honor) — 2013 - 2017
- ★ Thesis: On iterative collision search for LPN and proof of work (Distinguished Thesis Award)
- ★ Advisor: Prof. Jing Yang

PUBLICATION

Manuscripts

23. **Hanshen Xiao**, Jun Wan, Elaine Shi and Srinivas Devadas, On the Foundation of One-Sided Noise and Side-Channel Leakage Control.
22. **Hanshen Xiao**, Lam M. Nguyen, Marten van Dijk and Srinivas Devadas, Why Differentially-Private Local SGD - An Analysis of Biased Synchronized-Only Iterates.

Conference Papers

21. **Hanshen Xiao**, Edward Suh, and Srinivas Devadas, Formal Privacy Proof of Heuristic Obfuscation The Possibility and Impossibility of Learnable Encryption, ACM Conference on Computer and Communications Security (CCS), 2024, conditional accept.
20. Daniel Kane*, Ilias Diakonikolas*, **Hanshen Xiao***, and Sihan Liu*(randomized author order): Online Robust Mean Estimation, ACM-SIAM Symposium on Discrete Algorithms (SODA), 2024.
19. **Hanshen Xiao**, Jun Wan, and Srinivas Devadas, Geometry of Sensitivity: Twice Sampling and Hybrid Clipping in Differential Privacy with Optimal Gaussian Noise and Application to Deep Learning, ACM Conference on Computer and Communications Security (CCS), 2023.
18. **Hanshen Xiao** and Srinivas Devadas, PAC Privacy: Automatic Privacy Measurement and Control of Statistical Data Processing, Advances in Cryptology-CRYPTO, 2023. (Winner of **Capital One Research Award** 2023 and **Cisco Research University Funding** 2023)
17. **Hanshen Xiao***, Zihang Xiang*, Di Wang and Srinivas Devadas, A Theory to Instruct Differentially-Private Learning via Clipping Bias Reduction, IEEE Symposium on Security and Privacy (IEEE S&P), 2023.
16. Lijie Hu, Shuo Ni, **Hanshen Xiao**, and Di Wang. High Dimensional Differentially Private Stochastic Optimization with Heavy-tailed Data, ACM SIGMOD PODS, 2022. (**Best of PODS 2022**)

15. Jun Wan, **Hanshen Xiao**, Elaine Shi, and Srinivas Devadas. Expected constant round byzantine broadcast under dishonest majority, Theory of Cryptography Conference (TCC), 2020.
14. Jun Wan, **Hanshen Xiao**, Srinivas Devadas and Elaine Shi. Round-Efficient Byzantine Broadcast Under Strongly Adaptive and Majority Corruptions, Theory of Cryptography Conference (TCC), 2020.
13. Di Wang*, **Hanshen Xiao***, Srinivas Devadas and Jinhui Xu. On the Differentially Private Stochastic Optimization with Heavy-tailed Data, ICML, 2020.
12. Srinivas Devadas*, Ling Ren*, and **Hanshen Xiao***. On Iterative Collision Search for LPN and Subset Sum, Theory of Cryptography Conference (TCC), 2017.
11. Hari Krishna Garg and **Hanshen Xiao**. New Residue Arithmetic Based Barrett Algorithms: Modular Polynomial Computations, 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017.
10. **Hanshen Xiao**, Cas Cremers, and Hari Krishna Garg. Symmetric Polynomial & CRT Based Algorithms for Multiple Frequency Determination from Undersampled Waveforms, 2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2016.

Journal Papers

9. **Hanshen Xiao**, Yaowen Zhang, Beining Zhou and Guoqiang Xiao. On the Foundation of Sparsity Constrained Sensing (Part I): Necessary and Sufficient Sampling Theory and Robust Remaindering Problem, IEEE Trans on Signal Processing, 2023.
8. **Hanshen Xiao**, Beining Zhou, Yaowen Zhang and Guoqiang Xiao. On the Foundation of Sparsity Constrained Sensing (Part II): Diophantine Sampling with Arbitrary Temporal and Spatial Sparsity, IEEE Trans on Signal Processing, 2023.
7. **Hanshen Xiao**, Nan Du, Zhikang Wang and Guoqiang Xiao, Wrapped Ambiguity Gaussian Mixed Model with Applications in Sparse Sampling Based Multiple Parameter Estimation, Signal Processing, 2021.
6. **Hanshen Xiao** and Guoqiang Xiao. A Framework of Topology-Transparent Scheduling Based on Polynomial Ring, IEEE Wireless Communications Letters, 2019.
5. **Hanshen Xiao** and Guoqiang Xiao. On Solving Ambiguity Resolution With Robust Chinese Remainder Theorem for Multiple Numbers, IEEE Transactions on Vehicular Technology, 2019.
4. **Hanshen Xiao**, Yufeng Huang, Yu Ye and Guoqiang Xiao. Robustness in Chinese Remainder Theorem for Multiple Numbers and Remainder Coding, IEEE Transactions on Signal Processing, 2018.
3. **Hanshen Xiao** and Guoqiang Xiao. Notes on CRT-based Robust Frequency Estimation, Signal Processing, 2017.
2. Yu Ye, **Hanshen Xiao**, and Guoqiang Xiao. A Rotation-Aided Arctangent Phase Discriminator with One-Bit Quantization, IEEE Signal Processing Letters, 2016.
1. **Hanshen Xiao**, Hari Krishna Garg, Jianhao Hu, and Guoqiang Xiao. New Error Control Algorithms for Residue Number System Codes, ETRI Journal, 2016.

FELLOWSHIP & FUNDINGS

7. Mathwork Fellowship (2021-2023)
6. Tsinghua University Initiative Scientific Research Program Funds (2015-2017), 20161080166,1622S0372, PI.
5. Tsinghua Future Scholar Fellowship (2015-2017), Key Project 2015THZ0, PI.
4. Peking Scholarship of Science (2016).
3. Tsinghua 1993 Alumni Scholarship (2016).

2. Tsinghua Spark Program Fellowship (2015).
1. Israel Government Scholarship (2014).

SERVICES

Program Committee Member or Reviewer
ICLR (2024), IJCAI (2024), EuroCrypt (2023), ICML (2024, 2023, 2022, 2021), NeurIPS (2023, 2022), AsiaCrypt (2019), IEEE CDC (2019)
Journal of Machine Learning Research (JMLR)
IEEE Trans on Signal Processing (IEEE TSP)
Journal of Privacy and Confidentiality
Theoretical Computer Science
Neural Computing and Applications
IEEE Trans on Circuits and Systems I: Regular Papers

MIT PRIMES Program Mentor
Coley DuPlessie (2023-), Aidan Gao (2023-). Past students: Cathy Zhou (2020-2022, now at Stanford), Matthew Ding (2020-2022, now at UC Berkeley), Jason Yang (co-advising, 2020-2022, now at MIT), Kunal Kapoor (co-advising, 2020-2022, now at CMU).

Teaching Assistant
MIT 6.875 (Fall 2023): Foundations of Cryptography

SELECTED TALKS

1. **Learning Privacy and Privately Learning**:
   UIUC CSL (2024)
2. **High-Dimensional Sensitivity Geometry and Optimal Privacy-Preserving Randomization**:
   ACM CCS (2023)
3. **Possibility and Impossibility Results of Learnable Encryption**:
   Berkeley Security Seminar
4. **PAC Privacy: Automatic Privacy Measurement and Control of Statistical Data Processing**:
   Columbia Security Seminar, Crypto (2023), Google Algorithm Seminar, MIT CIS Seminar, UMN Machine Learning Seminar
5. **A Theory to Instruct Differentially-Private Learning via Clipping Bias Reduction**:
   IEEE S&P (2023)
6. **Towards Understanding Practical Randomness Beyond Noise: Differential Privacy and Mixup**:
   Harvard University, PPML (2020)
7. **On Iterative Collision Search for LPN and Subset Sum**:
   TCC (2017)

RESEARCH EXPERIENCE

MIT CSAIL Jun 2016 - Sep 2016
Research Intern, hosted by Prof. Srinivas Devadas
University of Oxford, Department of CS Jan 2016 - Feb 2016
Research Intern, hosted by Prof. Cas Cremers
National University of Singapore, Department of ECE Sep 2015
Visiting Student, hosted by Prof. Hari Garg
Yale University, Department of CS July 2015 - Aug 2015
Research Intern, hosted by Prof. Ruzica Piskac

REFERENCES

Srinivas Devadas
MIT, EECS Department
Email: devadas@mit.edu

Elaine Shi
CMU, Computer Science Department
Email: runting@cs.cmu.edu

Marten van Dijk
CWI & UConn, ECE Department
Email: marten.van.dijk@cwi.nl

Edward Suh
Cornell, ECE Department & Meta AI
Email: suh@ece.cornell.edu

Lam M. Nguyen
IBM Research & MIT-IBM Watson AI Lab
Email: lamng@mit.edu