Albert Cheu

ac2305@georgetown.edu
github.com/albertcheu

Research Goals

My research focuses on distributed differentially private (DP) protocols for statistics. I study how much noise these protocols need to introduce to guarantee privacy, as well as how much their guarantees are impacted by dishonest participants. Although theoretical in nature, the work I do is motivated by real-world questions of trust, security, and efficiency.

Education

Khoury College of Computer Sciences, Northeastern University	Boston, Massachusetts
Ph.D. in Computer Science, advised by Jonathan Ullman	2016–2021
Tandon School of Engineering, New York University	New York City, New York
B.S. in Computer Science	2012–2016

Publications and Preprints

1. Albert Cheu and Maxim Zhilyaev. *Differentially Private Histograms in the Shuffle Model from Fake Users.* To appear in the 43rd IEEE Symposium on Security and Privacy (S&P 2022). San Francisco, California, USA. 22-26 May 2022.

2. Albert Cheu, Matthew Joseph, Jieming Mao, and Binghui Peng. *Shuffle Private Stochastic Convex Optimization.* Tenth International Conference on Learning Representations (ICLR 2022). Virtual. 25-29 April 2022.

3. Albert Cheu, Chao Yan. *Pure Differential Privacy from Secure Intermediaries.* arXiv preprint. December 2021.

4. Albert Cheu and Jonathan R. Ullman. *The Limits of Pan Privacy and Shuffle Privacy for Learning and Estimation.* 53rd ACM Symposium on Theory of Computing (STOC 2021). Virtual. 21-25 June 2021.

5. Victor Balcer and Albert Cheu and Matthew Joseph and Jieming Mao, *Connecting Robust Shuffle Privacy and Pan-Privacy.* 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA 2021). Virtual. 10-13 January 2021.

6. Raef Bassily and Albert Cheu and Shay Moran and Aleksandar Nikolov and Jonathan R. Ullman and Zhiwei Steven Wu. *Private Query Release Assisted by Public Data.* Thirty-seventh International Conference on Machine Learning (ICML 2020). Virtual. 13-18 July 2020.

7. Victor Balcer and Albert Cheu. *Separating Local & Shuffled Differential Privacy via Histograms.* 1st Conference on Information-Theoretic Cryptography (ITC 2020). Virtual. 17-19 June 2020.

8. Albert Cheu and Adam D. Smith and Jonathan R. Ullman. *Manipulation Attacks in Local Differential Privacy.* 42nd IEEE Symposium on Security and Privacy (S&P 2021). Virtual. 23-27 May 2021.

9. Albert Cheu and Adam D. Smith and Jonathan R. Ullman and David Zeber and Maxim Zhilyaev. *Distributed Differential Privacy via Shuffling.* 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2019). Darmstadt, Germany. 19-23 May 2019.

10. Albert Cheu and Ravi Sundaram and Jonathan R. Ullman. *Skyline Identification in Multi-Arm Bandits.* 2018 IEEE International Symposium on Information Theory (ISIT 2018). Vail, Colorado, USA. 17-22 June 2018.

Talks and Presentations

Conferences and Workshops

- *How to Perform Statistics without Breaching Privacy* 5 May 2022
  Georgetown University Annual Postdoc Symposium (poster session).
- *Differentially Private Histograms in the Shuffle Model from Fake Users* 23 July 2021
  Theory and Practice of Differential Privacy workshop. Virtual.
- *The Limits of Pan Privacy and Shuffle Privacy for Learning and Estimation* 24 June 2021
  Symposium on Theory of Computing. Virtual.
- *Differential Privacy in the Shuffle Model* 17 December 2020
  2020 Junior Theorists Workshop, Northwestern University. Virtual.
- *Private Query Release Assisted by Public Data* 15 July 2020
  International Conference on Machine Learning. Virtual.
- *Manipulation Attacks in Local Differential Privacy* 11 November 2019
  Theory and Practice of Differential Privacy workshop. London, UK.
- *Distributed Differential Privacy via Shuffling* 19 May 2019
  EUROCRYPT. Darmstadt, Germany.
- *Skyline Identification in Multi-armed Bandits* 19 June 2018
  International Symposium on Information Theory. Vail, Colorado.

Invited Talks at Seminars and Reading Groups

- *Differential Privacy in the Shuffle Model* 14 April 2022
  Cryptography Reading Group, University of Maryland
- *The Limits of Pan Privacy and Shuffle Privacy for Learning and Estimation* 25 September 2020
  Differential Privacy Group, Boston University
- *Distributed Differential Privacy via Shuffling* 9 November 2018
  Privacy Tools Group, Harvard University

Experience

Georgetown University Washington, D.C.
Postdoctoral Fellow Sept. 2021 - present

- Supervised by Kobbi Nissim

University of Maryland College Park, Marland
Member of a Research Experience for Undergraduates (REU) program Summer 2015

- Advised by William Gasarch and Clyde Kruskal
- Programmed software to play a game inspired by Van der Waerden numbers

Professional Activities

Program Committee & Reviewer

- *Workshop on Privacy Enhancing Technologies for the Homeland Security Enterprise (PETS4HSE)* 2022
- *ACM Conference on Computer and Communications Security (CCS)* 2021, 2022
- *Theory and Practice of Differential Privacy (TPDP) workshop* 2020, 2021

Other

- *Weekly Theory Seminar Organizer at Northeastern University* 2018

Teaching

- ***Teaching Assistant** at Northeastern University* Fall 2017
  Advanced Algorithms (≈ 30 students, graduate level)
  Grading and Recitation section
- ***Teaching Assistant** at New York University* Fall 2015
  Design and Analysis of Algorithms (≈ 25 students, graduate level)
  Grading and Recitation section

Scholarships and Awards

- PhD Research Award, Khoury College of Computer Sciences 2021
- Graduate Fellowship, Northeastern University 2016–2017
- Pearl Brownstein Junior and Senior Award, New York University 2015–2016
- Tandon School of Engineering Promise Scholarship, New York University 2012–2016