Jalaj Upadhyay

CONTACT INFORMATION

1 Apple Park Way,
Cupertino, CA - 95050, U.S.A.

Phone: +1 (669) 294-6231
E-mail: jalaj.kumar.upadhyay@gmail.com
https://sites.google.com/view/jalajupadhyay

RESEARCH INTERESTS

I am interested in understanding fundamental questions in mathematics of data privacy.

PROFESSIONAL EXPERIENCE

Senior researcher, Apple, USA — 2019 – Present

Postdoctoral fellow in Computer Science, Johns Hopkins University, USA — 2017 – 2019
- Advisor: Prof. R. Arora and Prof. V. Braverman.

Postdoctoral fellow in Computer Science, Pennsylvania State University, USA — 2016 – 2017
- Advisor: Prof. A. Smith and Prof. S. Raskhodnikova.

PhD in Computer Science, University of Waterloo, Canada — 2010 – 2015
- Advisor: Prof. D. R. Stinson.
- Dissertation Topic: *Integrity and Privacy of Large Data*

RESEARCH GRANTS

NSF Big Data: F: Privacy in Unsupervised Learning, IIS-1838139 — $911,398.00
(PI: Raman Arora; Senior Personnel: Jalaj Upadhyay)

DARPA: Lifelong Unsupervised Learning with Streaming Algorithms — $ 112,000.00
(PI: Vladimir Braverman)

CONFERENCE PUBLICATIONS

Differential Private Analysis on Graph Streams (with R. Arora and S. Upadhyay)
In Artificial Intelligence and Statistics, 2021 (long oral presentation).

Near optimal linear algebra in the online and sliding window models (with V. Braverman, P. Drineas, C. Musco, C. Musco, D. Woodruff, and S. Zhou)
In *Foundations of Computer Science*, 2020.

On Differentially Private Graph Sparsification and its Applications (with R. Arora)
In *Neural Information Processing Systems*, 2019.

Sublinear Space Private Algorithms Under the Sliding Window Model
In *International Conference on Machine Learning*, 2019.

Differentially Private Robust PCA (with R. Arora and V. Braverman)
In *Neural Information Processing Systems*, 2018.

The Price of Privacy for Low-rank Factorization
In *Neural Information Processing Systems*, 2018.

Is Interaction Necessary for Distributed Private Learning? (with A. Smith and A. Thakurta).
In *IEEE Symposium of Security & Privacy*, 2017.

Block-wise Non-malleable Codes (with N. Chandran, V. Goyal, P. Mukherjee, and O. Pandey).
In *International Colloquium on Automata, Languages, and Programming*–ICALP, 2016.

Random Projections, Graph Sparsification, and Differential Privacy.
In *Proceedings of Advances in Cryptology*–ASIACRYPT, 2013.

Journal Publications

Multi-server Proof-of-retrievability (with M. Paterson and D. Stinson)
Journal of Mathematical Cryptology, 12(4), pages 203–220, 2018.

Is Data Possession Same as Extraction? (with D. Stinson)
Journal of Mathematical Cryptology, 8(2):189–207, 2014.

A coding theory foundation for the analysis of general unconditionally secure proof-of-retrievability schemes for cloud storage (with M. Paterson and D. Stinson).
Journal of Mathematical Cryptology, 7(3): 183–216, 2013.

On the Complexity of the Herding Attack and Some Related Attacks on Hash Functions (with S. Blackburn and D. Stinson).
Design, Codes, and Cryptography, 64 (1-2): 171–193, 2012.

Professional Service

- Organizer, Machine Learning seminar from September 2018–December 2018.
- Organizer, Lightning talks in 2018 Joint PI Meeting: NSF BIGDATA and Big Data Hubs & Spokes
- Organizer, CACR seminars from September 2013–May 2015.
- Social coordinator, Penn State Postdoc Society from February, 2016 – August, 2017.
- Reviewer for ICML 2019 – 2021, NeurIPS 2019 – 2021, COLT 2020 – 2021, ICLR 2021, PPML 2021.
- Reviewer for journals: *Journal of Mathematical Cryptology*, *Journal of Machine Learning Research*, *ACM Transactions on Information and System Security*, *Information Processing Letters*, *Transactions on Services Computing*, and *IET Information Security*.
- Sub-reviewer for conferences: SODA 2021, SoCG 2021, IJCAI 2019, SODA 2019, NeurIPS 2018, Usenix 2018, ICALP 2018, ICML 2018, STOC 2018, AISTATS 2018, LATIN 2018, SODA 2018, AISTATS 2017, STOC 2016, TCC 2016, ICALP 2014, ACISP 2014, AFRICACRYPT 2013, ESORICS 2012, SAC 2009 and SAC 2011.

Honors and Awards

Top 5% reviewer for 36th Annual ICML, 2019.
Travel Grant for 36th Annual ICML, 2019.
Travel Grant for 26th Annual PCMI, Mathematics of Data, 2016.
Recipient of 1 out of 100 travel Grant worldwide for the 1st Heidelberg Laureate Forum, 2013.
David R. Cheriton Scholarship, University of Waterloo, May 2013–April 2015.
Graduate Entrance Scholarship, University of Waterloo, September 2010–August 2011.

Selected Presentation

Towards Robust and Scalable Private Data Analysis
– Privacy Seminar, University of California – Berkeley (April, 2019)
– Machine Learning Seminar, University of Copenhagen (April, 2019)
– Theory Seminar, Johns Hopkins University (February, 2019)
– Optimization Seminar, Johns Hopkins University (February, 2019)
– MSIS Seminar, Rutgers University (February, 2019)
– CS Colloqium, Iowa State University (February, 2019)
– Privacy Seminar, University of California, Berkeley (April, 2019)

Differentially private Graph Sparsification and Applications
– Theory Seminar, University of California – Santa Cruz (April, 2019);
– Theory Seminar, Johns Hopkins University (November, 2018);
– Privacy Seminar, Boston University (May, 2018).

Differentially private Robust-PCA
– ML Seminar, Johns Hopkins University (September, 2018).

Is Interaction Necessary for Distributed Learning?
– Theory Seminar, Microsoft Research, Bangalore (June, 2017);
– Theory Seminar, Indian Institute of Technology, Delhi (June, 2017).

Fast and Space-optimal Low-rank Factorization with Application in Differential Privacy.
− Privacy Seminar, Duke University, Durham (March, 2017);
− Theory Seminar, Northeastern University, Boston (Febraury, 2017);
− Theory Seminar, University of Pennsylvania, Philadelphia (Febraury, 2017);
− Theory Seminar, Yahoo Research Labs, New York City (December, 2016);
− Theory Seminar, Johns Hopkins University(December, 2016);
− NSR Seminar, Penn State University (October, 2016);
− Theory Seminar, Purdue University (October, 2016);
− Theory Seminar, Indiana University (October, 2016);
− Tenth Annual CrySP Workshop, University of Waterloo (June, 2016).

The Johnson-Lindenstrauss Lemma: New Results and Applications.
− CACR Seminar, University of Waterloo (July, 2015);
− Indian Institute of Technology, Delhi (December, 2014).

Look-ahead Non-malleable Codes.
− PQCypto Seminar, University of Waterloo (February, 2015).

Differential Privacy in the Streaming Model.
− Contributed Talk, Sublinear Algorithms Workshop, John Hopkins University (January, 2016);
− Theory Seminar, Penn State University (April, 2015);
− Combinatorics and Optimization Seminar, University of Waterloo. (March, 2015)

Random Projections, Graph Sparsification, and Differential Privacy.
− ASIACRYPT-2013;
− Combinatorics and Optimization Seminar, University of Waterloo (January, 2014).

Random Projections and Differential Privacy.
− MMCI, Saarland University (September 2013);
− Combinatorics and Optimization Seminar, University of Waterloo (October, 2013);
− CACR Seminaar, University of Waterloo (October 2013);
− Indian Institute of Technology, Kanpur (January, 2014);
− Indian Institute of Technology, Delhi (January, 2014).