

Lydia Zakynthinou

Curriculum Vitae
Updated August 2026

Department of Computer Science
Johns Hopkins University
lyzakynthinou@jhu.edu
lydiazakynthinou.com

Research Summary

My research develops mathematical foundations for trustworthy machine learning and statistics, with an emphasis on differential privacy, robust statistics, and algorithmic stability.

Academic Appointments

- 2025-present **Assistant Professor**, Department of Computer Science, Johns Hopkins University, Baltimore, MD
Member, Data Science and AI Institute.
- Spring 2026 **Visiting Scholar**, Simons Institute for the Theory of Computing, University of California, Berkeley
Research Program on Federated and Collaborative Learning.
- 2023-2025 **Postdoctoral Research Fellow**, Simons Institute for the Theory of Computing (ML Pod), University of California, Berkeley
Supervisor: Michael I. Jordan.
- 2022 **Research Intern**, Apple, Cupertino, CA
Summer internship. Supervisor: Audra McMillan.
- 2019, 2020 **Research Intern**, IBM Research - Almaden, San Jose, CA
Summer internships. Supervisor: Thomas Steinke.

Education

- 2017-2023 **Ph.D. in Computer Science**, Northeastern University, Khoury College of Computer Sciences
Thesis: Algorithms and frameworks for preventing privacy leakage and overfitting in machine learning. Advisors: Jonathan Ullman and Huy Le Nguyen.
- 2015-2017 **Graduate Program in Logic, Algorithms, and Computation (MPLA)**, National Kapodistrian University of Athens, Department of Mathematics
Thesis: Online facility location with switching costs. Advisor: Dimitris Fotakis.
- 2008-2015 **Diploma in Electrical and Computer Engineering**, National Technical University of Athens, School of Electrical and Computer Engineering
Thesis: The multiplicative weights update method in mechanism design. Advisor: Dimitris Fotakis.

Publications

Authors are typically listed in alphabetical order unless noted. My name is bolded.

Manuscripts

- [1] **Tukey-depth Mechanisms for Practical Private Mean Estimation**
Gavin Brown and **Lydia Zakynthinou**. In submission, 2025.

Conference Publications

- [2] **Empirical Privacy Variance**
Yuzheng Hu, Fan Wu, Ruicheng Xian, Yuhang Liu, **Lydia Zakynthinou**, Pritish Kamath, Chiyuan Zhang, and David Forsyth. *International Conference on Machine Learning*, 2025. (ICML '25; authors by contribution.)
- [3] **Dimension-free Private Mean Estimation for Anisotropic Distributions**
Yuval Dagan, Xuelin Yang, Michael I. Jordan, **Lydia Zakynthinou**, and Nikita Zhivotovskiy. *Annual Conference on Neural Information Processing Systems*, 2024. (NeurIPS '24.)
- [4] **From Robustness to Privacy and Back**
Hilal Asi, Jonathan Ullman, and **Lydia Zakynthinou**. *International Conference on Machine Learning*, 2023. (ICML '23.)
- [5] **Multitask Learning via Shared Features: Algorithms and Hardness**
Konstantina Bairaktari, Guy Blanc, Li-Yang Tan, Jonathan Ullman, and **Lydia Zakynthinou**. *Conference on Learning Theory*, 2023. (COLT '23.)
- [6] **Covariance-Aware Private Mean Estimation Without Private Covariance Estimation**
Gavin Brown, Marco Gaboardi, Adam Smith, Jonathan Ullman, and **Lydia Zakynthinou**. *Annual Conference on Neural Information Processing Systems*, 2021. (NeurIPS '21, **Spotlight**.)
- [7] **PAC-Bayes, MAC-Bayes and Conditional Mutual Information: Fast rate bounds that handle general VC classes**
Peter Grunwald, Thomas Steinke, and **Lydia Zakynthinou**. *Conference on Learning Theory*, 2021. (COLT '21.)
- [8] **Differentially Private Decomposable Submodular Maximization**
Anamay Chaturvedi, Huy Le Nguyen, and **Lydia Zakynthinou**. *AAAI Conference on Artificial Intelligence*, 2021. (AAAI '21.)
- [9] **Private Identity Testing for High-Dimensional Distributions**
Clement L. Canonne, Gautam Kamath, Audra McMillan, Jonathan Ullman, and **Lydia Zakynthinou**. *Annual Conference on Neural Information Processing Systems*, 2020. (NeurIPS '20, **Spotlight**.)
- [10] **Reasoning About Generalization via Conditional Mutual Information**
Thomas Steinke and **Lydia Zakynthinou**. *Conference on Learning Theory*, 2020. (COLT '20.)
- [11] **Efficient Private Algorithms for Learning Large-Margin Halfspaces**
Huy Le Nguyen, Jonathan Ullman, and **Lydia Zakynthinou**. *Algorithmic Learning Theory*, 2020. (ALT '20.)
- [12] **Improved Algorithms for Collaborative PAC Learning**
Huy Le Nguyen and **Lydia Zakynthinou**. *Annual Conference on Neural Information Processing Systems*, 2018. (NeurIPS '18.)

Journal Publications

- [13] **Online Facility Location in Evolving Metrics**
Dimitris Fotakis, Loukas Kavouras, and **Lydia Zakynthinou**. *Algorithms*, 14(3):73, 2021.

Grants and Funding

- 2026-2027 **Foundations of Data Science and AI Award**
Data Science and AI Institute, Johns Hopkins University
PI. Project: Privacy Beyond Independent Records: Differential Privacy for Correlated, Shared, and Sequential Data. Internal seed funding award, up to \$60,000.

Honors and Awards

- 2023 Foundations of Data Science Institute Postdoctoral Fellowship.
2023 Northeastern University Dissertation Completion Fellowship.
2022 Khoury College PhD Research Award.
2020 Meta PhD Fellowship.
2017 Khoury College Graduate Fellowship.
2017 First Honor in the Graduate Program in Logic, Algorithms, and Computation, National Kapodistrian University of Athens.

Advising and Mentoring

Doctoral Students

- Fall 2026-present **Michael Xie**, Ph.D. student, Johns Hopkins University

Research Mentoring

- Summer 2025 **Renaud Gaucher**, visiting Ph.D. student, UC Berkeley
Ph.D. student at Ecole Polytechnique and Inria; visit May-July 2025.

Degree Committees

- 2026 **Vineet Kamat**, Doctor of Engineering research proposal examination committee, Johns Hopkins University
Advisor: Yinzhi Cao.

Teaching

Instructor

- Fall 2026 **Theory of Differential Privacy (EN.601.438/638)**, Johns Hopkins University
Undergraduate and graduate course; 3 credits.

Tutorials and Outreach

- Spring 2026 **Tutorial: Privacy and Security**, Simons Institute for the Theory of Computing, UC Berkeley
Boot camp for the Semester Program on Federated and Collaborative Learning; with Adam Smith and Adria Gascon.
Fall 2024 **Tutorial: Introduction to Differential Privacy**, Australasian Summer School on Recent Trends in Algorithms
Guest lecturer; undergraduate and graduate audience.
Fall 2024 **Session on Introduction to Differential Privacy**, Berkeley Math Circle
Guest lecturer; high school audience.

Teaching Assistantships

- Fall 2022 **Advanced Algorithms (CS7800)**, Northeastern University
Instructor: Jonathan Ullman; graduate course; guest lecturer.
- Fall 2018 **Algorithms and Data (CS3000)**, Northeastern University
Instructor: Jonathan Ullman; undergraduate course; teaching assistant.
- Spring 2015-2017 **Introduction to Computer Science**, National Technical University of Athens
Instructors: Aris Pagourtzis and Stathis Zachos; undergraduate course; grader.
- Fall 2014-2016 **Computer Programming**, National Technical University of Athens
Instructors: Stathis Zachos, Dimitris Fotakis, and Nikolaos Papaspyrou; undergraduate course; lab instructor.
- Fall 2014-2016 **Algorithms and Complexity**, National Technical University of Athens
Instructor: Dimitris Fotakis; undergraduate course; teaching assistant.
- Spring 2015-2016 **Algorithms and Complexity**, MPLA
Instructor: Dimitris Fotakis; graduate course; teaching assistant.
- Spring 2016 **Algorithmic Game Theory**, MPLA
Instructor: Dimitris Fotakis; graduate course; teaching assistant.
- Spring 2015 **Social Networks**, MPLA
Instructor: Dimitris Fotakis; graduate course; teaching assistant.

Invited Talks

- March 2026 Trust in Decentralized Systems workshop, Federated and Collaborative Learning program, Simons Institute for the Theory of Computing.
- August 2025 Joint Statistical Meetings.
- June 2025 Theory and Practice of Differential Privacy (TPDP) Workshop, **keynote**.
- March 2025 Apple Workshop on Privacy-Preserving Machine Learning.
- January 2025 Information Theory and Applications Workshop (ITA).
- October 2024 Google Algorithms Seminar.
- July 2024 Workshop on Algorithms in Learning and Economics (WALE).
- June 2024 TTIC Workshop: New Frontiers in Robust Statistics.
- June 2023 Theory and Practice of Differential Privacy (TPDP) Workshop.
- January 2023 Chicago Junior Theorists Workshop.
- June 2022 Theory and Practice of Differential Privacy (TPDP), **keynote**.
- November 2021 New York Colloquium on Algorithms and Complexity (NYCAC).
- October 2020 First IBM Workshop on Information Theory.
- July 2019 Workshop on Algorithms Learning and Economics (WALE).
- November 2019 New York Colloquium on Algorithms and Complexity (NYCAC).

Seminar and Other Talks

- January 2026 Privacy Seminar, Federated and Collaborative Learning program, Simons Institute for the Theory of Computing.
- November 2025 Center for Imaging Science (CIS) and Mathematical Institute for Data Science (MINDS) Seminar, Johns Hopkins University.

November 2025 Department of Applied Mathematics and Statistics Seminar, Johns Hopkins University.

November 2025 CS Theory Seminar, Johns Hopkins University.

October 2025 Department of Electrical and Computer Engineering Seminar, Johns Hopkins University.

October 2025 Department of Statistics Seminar, Athens University of Economics and Business.

April 2025 Computer Science Department Seminar, Johns Hopkins University.

March 2025 ASSET Seminar, University of Pennsylvania.

March 2025 Cheriton School of Computer Science Department Seminar, University of Waterloo.

March 2025 ECE RISE Seminar Series: Trustworthy AI, University of Wisconsin-Madison.

January 2025 Computer Science Department Seminar, Barnard College.

January 2023 MIT Algorithms and Complexity Seminar.

October 2021 CS Theory Seminar, Johns Hopkins University.

October 2021 CS Theory Seminar, Northeastern University.

February 2019 Signal Processing, Imaging, Reasoning, and Learning (SPIRAL) Group Seminar, Northeastern University.

Professional Service

Program Committees, Area Chair Roles, and Reviewing

2027 Program Committee, Innovations in Theoretical Computer Science (ITCS).

2027 Area Chair, Algorithmic Learning Theory (ALT).

2026 NSF Panel Reviewer.

2026 Area Chair, Neural Information Processing Systems (NeurIPS).

2026 Area Chair, International Conference on Machine Learning (ICML).

2026 Area Chair, Algorithmic Learning Theory (ALT).

2026 Program Committee, IEEE Security and Privacy (S&P).

2026 Program Committee, Theory and Practice of Differential Privacy (TPDP) Workshop.

2025 Reviewer, Conference on Learning Theory (COLT).

2024 Program Committee, Theory and Practice of Differential Privacy (TPDP) Workshop.

2024 Reviewer, Conference on Learning Theory (COLT).

2024 Reviewer, Neural Information Processing Systems (NeurIPS).

2024 Reviewer, Algorithmic Learning Theory (ALT).

2023 Program Committee, ACM Conference on Fairness, Accountability, and Transparency (FAccT).

2023 Reviewer, Conference on Learning Theory (COLT).

2023 Reviewer, Neural Information Processing Systems (NeurIPS, technical and ethics).

2023 Reviewer, International Conference on Machine Learning (ICML).

2023 Reviewer, IEEE Secure and Trustworthy ML (SaTML), **outstanding reviewer distinction**.

2022 Program Committee, ACM Conference on Fairness, Accountability, and Transparency (FAccT).

2022 Program Committee, Theory and Practice of Differential Privacy (TPDP) Workshop.

- 2022 Reviewer, Neural Information Processing Systems (NeurIPS, technical and ethics).
- 2022 Reviewer, International Conference on Machine Learning (ICML).
- 2021 Program Committee, ACM Conference on Fairness, Accountability, and Transparency (FAccT).
- 2021 Program Committee, Theory and Practice of Differential Privacy (TPDP) Workshop.
- 2021 Reviewer, Neural Information Processing Systems (NeurIPS).
- 2021 Reviewer, International Conference on Machine Learning (ICML).
- 2020 Program Committee, Theory and Practice of Differential Privacy (TPDP) Workshop.
- 2020 Reviewer, Neural Information Processing Systems (NeurIPS).
- 2020 Reviewer, International Conference on Machine Learning (ICML).
- 2020 Reviewer, Algorithmic Learning Theory (ALT).
- 2020 Reviewer, AAAI Conference on Artificial Intelligence.

Organizing

- 2026 Workshops and Tutorials Chair, Conference on Learning Theory (COLT).
- 2023-2025 Mentoring Workshop Committee, Learning Theory Alliance, including Fall 2025 Workshop, COLT 2025 Event, NeurIPS 2024 Social Event, Spring 2024 Workshop, Fall 2023 Workshop, and COLT 2023 Panel.

Departmental and University Service

- 2026 Reviewer, M.S. admissions, Department of Computer Science, Johns Hopkins University.
- 2026 Member, Data Science and AI Institute Postdoctoral Research Fellows Committee, Johns Hopkins University.
- 2022-2023 Student reviewer, Ph.D. admissions, Northeastern University.
- 2021 Ph.D. representative, faculty hiring committee, Northeastern University.
- 2021 Organizer, Boston-area Differential Privacy Seminar.
- 2019-2021 Organizer, Northeastern CS Theory Seminar.
- 2019-2023 Organizer, Khoury Ph.D. Women's Group, Northeastern University.