Lydia Zakynthinou

Curriculum Vitae

Johns Hopkins University
lzakynthinou@jhu.edu
lydiazakynthinou.com

Research Interests

Foundations of Trustworthy Machine Learning and Statistics, Differential Privacy, Algorithmic Stability

Employment History

2025-present **Assistant Professor**, Department of Computer Science, Johns Hopkins University, Baltimore, MD, USA

2023–2025 **Postdoctoral Research Fellow**, Simons Institute for the Theory of Computing (ML Pod), University of California, Berkeley, CA, USA
Supervisor: Michael I. Jordan

Summer 2022 **Research Intern**, Apple, Cupertino, CA, USA
Supervisor: Audra McMillan

Summer 2019 & 2020 **Research Intern**, IBM Research - Almaden, San Jose, CA, USA
Supervisor: Thomas Steinke

Education

2017–2023 **PhD in Computer Science**, Northeastern University, Khoury College of Computer Sciences
GPA: 3.97/4
Thesis: Algorithms and frameworks for preventing privacy leakage and overfitting in machine learning
Advisors: Jonathan Ullman and Huy Lê Nguyễn

2015–2017 **Graduate Program in Logic, Algorithms, and Computation (MPLA)**, National Kapodistrian University of Athens (NKUA), Department of Mathematics
GPA: 9.93/10
Thesis: Online facility location with switching costs
Advisor: Dimitris Fotakis

2008–2015 **Diploma in Electrical and Computer Engineering**, National Technical University of Athens (NTUA), School of Electrical and Computer Engineering
GPA: 8.28/10
Thesis: The multiplicative weights update method in mechanism design
Advisor: Dimitris Fotakis

Publications and Manuscripts (authors in alphabetical order)

Empirical Privacy Variance
Yuzheng Hu, Fan Wu, Ruicheng Xian, Yuhang Liu, Lydia Zakynthinou, Pritish Kamath, Chiyuan Zhang, David Forsyth (in order of contribution).
42nd International Conference on Machine Learning, 2025. (**ICML '25**)

Tukey-depth Mechanisms for Practical Private Mean Estimation
Gavin Brown, Lydia Zakynthinou.
In submission, 2025.

Dimension-free Private Mean Estimation for Anisotropic Distributions
Yuval Dagan, Xuelin Yang, Michael I. Jordan, Lydia Zakynthinou, Nikita Zhivotovskiy.
38th Conference on Neural Information Processing Systems, 2024. (**NeurIPS '24**)

From Robustness to Privacy and Back
Hilal Asi, Jonathan Ullman, Lydia Zakynthinou.
40th International Conference on Machine Learning, 2023. (**ICML '23**)

Multitask Learning via Shared Features: Algorithms and Hardness
Konstantina Bairaktari, Guy Blanc, Li-Yang Tan, Jonathan Ullman, Lydia Zakynthinou.
33rd Annual Conference on Learning Theory, 2023. (**COLT '23**)

Covariance-Aware Private Mean Estimation Without Private Covariance Estimation
Gavin Brown, Marco Gaboardi, Adam Smith, Jonathan Ullman, Lydia Zakynthinou.
35th Conference on Neural Information Processing Systems, 2021. (**NeurIPS '21**, **Spotlight**)

PAC-Bayes, MAC-Bayes and Conditional Mutual Information: Fast rate bounds that handle general VC classes
Peter Grünwald, Thomas Steinke, Lydia Zakynthinou.
34th Annual Conference on Learning Theory, 2021. (**COLT '21**)

Differentially Private Decomposable Submodular Maximization
Anamay Chaturvedi, Huy Lê Nguyễn, Lydia Zakynthinou.
35th AAAI Conference on Artificial Intelligence, 2021. (**AAAI '21**)

Online Facility Location in Evolving Metrics
Dimitris Fotakis, Loukas Kavouras, Lydia Zakynthinou.
Algorithms 2021, 14(3):73.

Private Identity Testing for High-Dimensional Distributions
Clément L. Cannone, Gautam Kamath, Audra McMillan, Jonathan Ullman, Lydia Zakynthinou.
34th Conference on Neural Information Processing Systems, 2020. (**NeurIPS '20**, **Spotlight**)

Reasoning About Generalization via Conditional Mutual Information
Thomas Steinke, Lydia Zakynthinou.
33rd Annual Conference on Learning Theory, 2020. (**COLT '20**)

Efficient Private Algorithms for Learning Large-Margin Halfspaces
Huy Lê Nguyễn, Jonathan Ullman, Lydia Zakynthinou.
31st International Conference on Algorithmic Learning Theory, 2020. (**ALT '20**)

Improved Algorithms for Collaborative PAC Learning
Huy Lê Nguyễn, Lydia Zakynthinou.
32nd Conference on Neural Information Processing Systems, 2018. (**NeurIPS '18**)

Honors & Awards

2023 **Foundations of Data Science Institute Postdoctoral Fellowship**, Award covering funding for one year.

2023 **Northeastern University Dissertation Completion Fellowship**, Award covering a one-semester stipend to outstanding PhD candidates who would benefit from the financial security and the freedom to focus on their final semester writing.

2022 **Khoury College PhD Research Award**, Awarded annually to a doctoral student whose research makes a significant impact in the field.

2020 **Meta PhD Fellowship**, Merit-based award covering stipend, tuition, and conference travel for two academic years.

2017 **Khoury College Graduate Fellowship**, Merit-based award covering stipend and tuition for one academic year.

2017 **First Honor in the Graduate Program in Logic, Algorithms, and Computation**, *National Kapodistrian University of Athens*, for highest GPA in the class of 2017.

Service

Reviewer, NeurIPS (2020-2024, Technical and/or Ethics Reviewer), ICML (2020-2023), COLT (2023-2025), IEEE Secure and Trustworthy ML (2023, outstanding reviewer distinction), ALT (2020, 2024), AAAI (2020), ESA (2020), SODA (2019), IEEE Transactions of Information Theory, Transactions on Machine Learning Research

Program Committee Member, IEEE Security and Privacy (2026), TPDP (2020-2022, 2024), FAccT (2021-2023)

Organizer, Learning Theory Alliance's Mentoring Workshop Committee (2023-present), Khoury PhD Women Group (2019-2023), Boston-area Differential Privacy Seminar (2021), Northeastern CS Theory Seminar (2019-2021).

Teaching Experience

Fall '24 **Tutorial on Introduction to Differential Privacy**, Australasian Summer School on Recent Trends in Algorithms, Undergraduate and Graduate
Guest Lecturer

Fall '24 **Session on Introduction to Differential Privacy**, Berkeley Math Circle, High school
Guest Lecturer

Fall '22 **Advanced Algorithms (CS7800)**, *Instructor: Jonathan Ullman*, NEU, Graduate
Guest Lecturer

Fall '18 **Algorithms and Data (CS3000)**, *Instructor: Jonathan Ullman*, NEU, Undergraduate
Teaching Assistant

Spring '15–'17 **Introduction to Computer Science**, *Instructors: Aris Pagourtzis, Stathis Zachos*, NTUA, Undergraduate
Grader

Fall '14–'16 **Computer Programming**, *Instructors: Stathis Zachos, Dimitris Fotakis, Nikolaos Papaspyrou*, NTUA, Undergraduate
Lab Instructor

Fall '14–'16 **Algorithms and Complexity**, *Instructor: Dimitris Fotakis*, NTUA, Undergraduate
Teaching Assistant

Spring '15–'16 **Algorithms and Complexity**, *Instructor: Dimitris Fotakis*, MPLA, Graduate
Teaching Assistant

Spring '16 **Algorithmic Game Theory**, *Instructor: Dimitris Fotakis*, MPLA, Graduate
Teaching Assistant

Spring '15 **Social Networks**, *Instructor: Dimitris Fotakis*, MPLA, Graduate
Teaching Assistant

Selected Invited Talks

Tukey-depth Mechanisms for Practical Private Mean Estimation, Joint Statistical Meetings (2025)

Practical Private Mean Estimation: Towards Instance - Adaptivity and Computational Efficiency, Theory and Practice of Differential Privacy (TPDP, 2025, keynote)

Dimension-free Private Mean Estimation for Anisotropic Distributions, Workshop on Algorithms in Learning and Economics (WALE, 2024), Google Algorithms Seminar (2024), Information Theory and Applications Workshop (ITA, 2025)

From Robustness to Privacy and Back, TTIC Workshop: New Frontiers in Robust Statistics (2024), Theory and Practice of Differential Privacy (TPDP, 2023)

Private Mean Estimation with Connections to Robustness, Chicago Junior Theorists Workshop (2023), Theory and Practice of Differential Privacy (TPDP, 2022, keynote)

PAC-Bayes, MAC-Bayes and Conditional Mutual Information, New York Colloquium on Algorithms and Complexity (NYCAC, 2021)

Reasoning about Generalization via Conditional Mutual Information, First IBM Workshop on Information Theory (2020)

Private Identity Testing for High-Dimensional Distributions, New York Colloquium on Algorithms and Complexity (NYCAC, 2019), Workshop on Algorithms Learning and Economics (WALE, 2019)