# Ashwinee Panda

website Email

## Education

| | |
|---|---|
| Current | PhD in Machine Learning, **Princeton University**<br>· Research Focus: Differential Privacy, Federated Learning<br>· Advisor: Prof. Prateek Mittal |
| May '20 | M.S. in Computer Science, **UC Berkeley**<br>· Research Focus: Federated Learning<br>· Advisor: Prof. Joey Gonzalez |
| May '19 | B.S. in Computer Science, **UC Berkeley** (Dean's Honors List) |
| Awards | Gordon Y.S. Wu Fellowship in Engineering |

## Work

| | |
|---|---|
| *'18 - '22.* | **CEO** at DiscreetAI *AI, Security*<br>Building open-source software for federated learning<br>1st place Y Combinator Hackathon, 1st place LAUNCH Demo Day ($26,000).<br>Founded venture backed startup for privacy preserving machine learning. Developed service enabling developers to generate insights from decentralized datasets using federated learning. Built POCs leveraging Transformer models for a range of applications: wake word detection, chatbot, TTS, forecasting, and resource allocation. Deployed on-device models across JS, iOS, and Android.<br>Investors: Samsung NEXT, Dorm Room Fund, Rough Draft Ventures<br>Clients: Ford, OhmConnect, Samsung, Ohme |

## Invited Talks

| | |
|---|---|
| April '23 | Improving the Privacy Utility Tradeoff in Differentially Private Machine Learning with Public Data<br>*Apple, USA* |
| March '23 | Google Privacy Seminar<br>*Google, USA* |
| June '22 | Challenges and Directions in Privacy Preserving Machine Learning<br>*Microsoft Research Cambridge, UK* |
| May '22 | Towards Trustworthy Machine Learning<br>*Meta AI, USA* |
| Jan '22 | Federated Learning for Forecasting<br>*Ohmconnect, USA* |
| November '21 | Building Federated Learning Systems at Scale<br>*Liftoff AI, USA* |
| November '21 | Practical Defenses Against Model Poisoning Attacks<br>*Google Federated Learning Workshop, USA* |

## Research

| | |
|---|---|
| AdvVLM | Xiangyu Qi*, Kaixuan Huang*, **Ashwinee Panda**, Mengdi Wang, Prateek Mittal<br>Introducing Vision into Large Language Models Expands Attack Surfaces and Failure Implications<br>At *40th International Conference on Machine Learning* AdvML Workshop |
| Phishing | **Ashwinee Panda**, Zhengming Zhang, Yaoqing Yang, Prateek Mittal<br>Teach GPT to Phish: Neural Phishing Attacks on Large Language Models<br>At *40th International Conference on Machine Learning* AdvML Workshop |
| DP-Diffusion | Vikash Sehwag*, **Ashwinee Panda***, Ashwini Pokle, Xinyu Tang, Saeed Mahloujifar, Mung Chiang, J Zico Kolter, Prateek Mittal<br>Differentially Private Generation of High Fidelity Samples From Diffusion Models<br>At *40th International Conference on Machine Learning* GenAI Workshop |
| DP-RandP | Xinyu Tang*, **Ashwinee Panda***, Prateek Mittal<br>Differentially Private Image Classification by Learning Priors from Random Processes<br>*Under Review at NeurIPS 2023* |
| DP-ICL | **Ashwinee Panda***, Tong Wu*, Tianhao Wang*, Prateek Mittal<br>Differentially Private In-Context Learning<br>At *NAACL 2023* TrustNLP Workshop |
| DP-Lin | **Ashwinee Panda***, Xinyu Tang*, Vikash Sehwag, Saeed Mahloujifar, Prateek Mittal<br>A New Linear Scaling Rule for Differentially Private Hyperparameter Optimization<br>*Under Review at NeurIPS 2023* |
| Neurotoxin | Zhengming Zhang*, **Ashwinee Panda***, Linyue Song, Yaoqing Yang, Prateek Mittal, Joseph Gonzalez, Kannan Ramchandran, Michael Mahoney<br>NeuroToxin: Durable Backdoors in Federated Learning<br>In *Proceedings of the 39th International Conference on Machine Learning* |
| SparseFed | **Ashwinee Panda**, Saeed Mahloujifar, Arjun Bhagoji, Supriyo Chakraborty, Prateek Mittal<br>SparseFed: Mitigating Model Poisoning Attacks in Federated Learning via Sparsification<br>In *25th International Conference on Artificial Intelligence and Statistics* |
| FetchSGD | Daniel Rothchild*, **Ashwinee Panda***, Enayat Ullah, Nikita Ivkin, Ion Stoica, Vladimir Braverman, Joseph Gonzalez, Raman Arora<br>FetchSGD: Communication-Efficient Federated Learning with Sketching<br>In *Proceedings of the 37th International Conference on Machine Learning* |
| SoftPBT | **Ashwinee Panda**, Eric Liang, Richard Liaw, Joey Gonzalez<br>SoftPBT: Leveraging Experience Replay for Efficient Hyperparameter Schedule Search<br>*Submitted to NeurIPS 2019* |

## Service

**Teaching**

| | |
|---|---|
| 2023 | Teaching Assistant for COS/ECE 432 at Princeton |
| 2019 | Course Staff for CS 189 (Machine Learning) at UC Berkeley |
| 2018 | Undergraduate Student Instructor for CS 70 (Probability and Discrete Mathematics) and Course Staff for CS 189 at UC Berkeley |
| 2017 | Course Staff for CS 70 at UC Berkeley |

**Peer Reviewing**

| | |
|---|---|
| 2023 | SATML 2023, ACL 2023, ICML 2023, NeurIPS 2023, TMLR |
| 2022 | ICML 2022, AISTATS 2022 |
| 2021 | ICML 2021, NeurIPS 2021 |
| 2020 | ICML 2020 |
| 2019 | ICLR 2019, NeurIPS 2019 |