

# Ashwinee PANDA

SCHOLAR LINKEDIN GITHUB EMAIL INTERESTS

## EDUCATION

---

CURRENT	PhD in Machine Learning, <b>Princeton University</b> , GPA: 3.8 · Research Focus: Differential Privacy, Federated Learning · Advisor: Prof. Prateek Mittal
MAY '20	M.S. in Computer Science, <b>UC Berkeley</b> , GPA: 4.0 · Research Focus: Federated Learning · Advisor: Prof. Joey Gonzalez
MAY '19 AWARDS	B.S. in Computer Science, <b>UC Berkeley</b> , GPA: 3.9 ( <a href="#">Dean's Honors List</a> ) Gordon Y.S. Wu Fellowship in Engineering

## WORK

---

'18 - '22.	<b>CEO at <a href="#">DISCREETAI AI, Security</a></b> Building open-source software for federated learning 1 <sup>st</sup> place Y Combinator Hackathon, 1 <sup>st</sup> place <a href="#">LAUNCH Demo Day</a> (\$26,000). 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. Investors: <a href="#">Samsung NEXT</a> , <a href="#">DORM ROOM FUND</a> , <a href="#">Rough Draft Ventures</a> Clients: <a href="#">Ford</a> , <a href="#">OhmConnect</a> , <a href="#">Samsung</a> , <a href="#">Ohme</a>
------------	--

## INVITED TALKS

---

APRIL '23	Improving the Privacy Utility Tradeoff in Differentially Private Machine Learning with Public Data <i>Apple, USA</i>
MARCH '23	<a href="#">Google Privacy Seminar</a> <i>Google, USA</i>
JUNE '22	Challenges and Directions in Privacy Preserving Machine Learning <i>Microsoft Research Cambridge, UK</i>
MAY '22	Towards Trustworthy Machine Learning <i>Meta AI, USA</i>
JAN '22	Federated Learning for Forecasting <i>Ohmconnect, USA</i>
NOVEMBER '21	Building Federated Learning Systems at Scale <i>Liftoff AI, USA</i>
NOVEMBER '21	Practical Defenses Against Model Poisoning Attacks <i>Google Federated Learning Workshop, USA</i>

## RESEARCH

---

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

## 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