

Yvonne Zhou

7613 Tarpley Dr., Rockville, MD USA 20855

skyzhou@umd.edu 301-326-7877

EDUCATION

University of Maryland, College Park, MD

Ph.D. in Computer Science, August 2022 – August 2027 (Anticipated) (GPA: 3.975)

Completed computer science coursework towards a Master's degree before transitioning to the PhD program. August 2020 – May 2022

B.S. in Mechanical Engineering, Minor in Project Management, December 2011 (GPA: 3.925)

RESEARCH EXPERIENCE

Graduate Research Assistant, *University of Maryland, August 2022 – Present*

- **Convergent Approximate Gradient Descent under FHE (Ongoing)**: Establishing theoretical convergence guarantees for ML training under *Fully Homomorphic Encryption (FHE)*. Developed a scalable, FHE-compatible differentially private training algorithm, including convergence analysis, optimal polynomial approximation, and data-independent hyperparameter tuning guidelines.
- **Model Parameter Extraction Defense (Ongoing)**: Designing defenses against model parameter extraction attacks by applying *Differential Privacy (DP)* techniques to safeguard model confidentiality.
- **Differential Privacy ML using DP Synthetic Data (Completed)**: Investigated DP-ML using marginal-preserving synthetic datasets; derived tight bounds for excess empirical risk and validated findings through experimental evaluation.
- **XR-Based Authentication System (Completed)**: Developed a secure XR login system (*Memory Palace*) in Unity, implementing SHA-256-based encryption and integrating MongoDB for encrypted data storage.

PUBLICATIONS

- Zhou, Y., Liang, M., Brugere, I., Dervovic, D., Polychroniadou, A., Wu, M., Dachman-Soled, D. *Bounding the Excess Risk for Linear Models Trained on Marginal-Preserving, Differentially-Private, Synthetic Data*. Proceedings of the 41st International Conference on Machine Learning, volume 235 of Proceedings of Machine Learning Research, pages 61979–62001. PMLR, 21–27 Jul 2024.

WORKING EXPERIENCE

Product Manager, *United Bus Technology, July 2016 – Dec 2019*

- Led cross-functional teams through product design, development, testing, and deployment for large-scale IoT and mobile applications
- Implemented *Zoho CRM/ERP* systems, built the company's online store, and coordinated post-launch support.
- Managed daily product operations and collaborated with cross-departmental teams on major projects, including: MegaTrac (fleet management), ShiELD (E-logbook), NetBox (media server), EasternBus App, GPS sensors, and security cameras.

Project Engineer, *Solar Solution LLC, Oct 2012– Feb 2016*

- Modeled solar installations using **SketchUp**, designed structural/electrical layouts in **Visio**, and prepared full project documentation (proposals, O&M manuals).
- Processed building permits, delivered technical support, and trained associate engineers.

QC Engineer, *Hangzhou Aihua Instruments Co., Ltd., June – Oct 2012*

Associate Engineer (Co-Op), *Scantek, Inc., Spring 2011*

SKILLS

Programming & Tools: Python, C++, MATLAB, LaTeX, CAD, Unity, WordPress, Axure, Microsoft Office Suite

Research Areas: Cryptography, Fully Homomorphic Encryption, Differential Privacy, Privacy-Preserving Machine Learning

Languages: English (Fluent), Mandarin (Fluent)