Yvonne Zhou
Rockville, MD 20855
skyzhou@umd.edu | 301-326-7877

RESEARCH INTERESTS

Privacy-Preserving Machine Learning, Fully Homomorphic Encryption, Differential Privacy, Secure & Trustworthy AI, Cryptography, Synthetic Data, Encrypted Optimization

---

EDUCATION

University of Maryland, College Park
Ph.D. in Computer Science (Anticipated Aug 2027) | GPA: **3.975**
Aug 2022 – Present
- Completed computer science coursework towards a Master's degree before transiting to the PhD program(Aug 2020 – May 2022)
- Core focus: Privacy-Preserving ML, Fully Homomorphic Encryption, Differential Privacy

B.S. in Mechanical Engineering, Minor in **Project Management**
Dec 2011 | GPA: **3.925**

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 (ICML 2024), PMLR, Jul 2024.

RESEARCH EXPERIENCE

Graduate Research Assistant — University of Maryland | *Aug 2022 – Present*
Private Machine Learning under Fully Homomorphic Encryption (FHE) (Ongoing)
- Designing a scalable, FHE-compatible differentially private training algorithm enabling optimization directly over encrypted data
- Establishing convergence guarantees for approximate gradient descent under cipher-text constraints
- Developing guidance for optimal polynomial approximations selection for training
- Proposing data-independent hyperparameter tuning strategies for secure ML pipelines

Model Parameter Extraction Defense (Ongoing)
- Designing Differential Privacy (DP)-based defenses against model parameter

extraction and reconstruction attacks
- Evaluating robustness under adaptive adversarial query strategies across multiple ML architectures

Differential Privacy via Synthetic Data (Completed)
- Derived tight theoretical bounds on excess empirical risk for linear models trained on marginal-preserving DP synthetic datasets
- Validated theoretical guarantees through controlled experimental evaluation

XR-Based Secure Authentication System (Completed)
- Developed a secure XR authentication system ("Memory Palace") in Unity
- Implemented SHA-256–based encryption and integrated MongoDB for encrypted credential storage

---

TECHNICAL SKILLS

Programming: Python, C++, MATLAB
Security & ML: Differential Privacy, Fully Homomorphic Encryption, Privacy-Preserving ML, Secure Optimization
Tools: LaTeX, Unity, CAD, WordPress, Axure, Microsoft Office

INDUSTRY EXPERIENCE (CONDENSED)

Product Manager — United Bus Technology | *Jul 2016 – Dec 2019*
- Led cross-functional engineering teams through design, development, testing, and deployment of large-scale IoT and mobile systems
- Oversaw telemetry, GPS tracking, fleet management, and secure device integration
- Implemented Zoho CRM/ERP and built the company's full e-commerce infrastructure

---

ADDITIONAL ENGINEERING EXPERIENCE

Project Engineer — Solar Solution LLC | *Oct 2012 – Feb 2016*
- Designed solar PV systems and prepared full technical documentation (proposals, permitting, O&M manuals)

QC Engineer — Hangzhou Aihua Instruments Co., Ltd. | *Jun 2012 – Oct 2012*
Associate Engineer (Co-Op) — Scantek, Inc. | *Spring 2011*

LANGUAGES

English (Fluent), Mandarin (Fluent)