

EDUCATION

•University of Warwick	2023-2027
PhD of Engineering	U.K.
•Beijing Language and Culture University	2016-2023
Bachelor’s and Master’s Degrees of Computer Science	China

PUBLICATIONS

•PRBench: A Standardized Probabilistic Robustness Benchmark	<u>KDD 2026</u>	<u>Paper</u>
Yi Zhang, Z Wang, Z Chen, W Ruan, Q Guo, S Khastgir, C Maple, X Zhao. Proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining		
•Adversarial Training for Probabilistic Robustness	<u>ICCV 2025</u>	<u>Paper</u>
Yi Zhang, Y Chen, Z Chen, W Ruan, X Huang, S Khastgir, X Zhao. Proceedings of the IEEE/CVF International Conference on Computer Vision		
•ProTIP: Probabilistic Robustness Verification on Text-to-Image Diffusion Models against Stochastic Perturbation	<u>ECCV 2024</u>	<u>Paper</u>
Yi Zhang, Y Tang, W Ruan, X Huang, S Khastgir, P Jennings, X Zhao The European Conference on Computer Vision		
•Trustworthy Text-to-Image Diffusion Models: A Timely and Focused Survey	<u>Information Fusion</u>	<u>Paper</u>
Yi Zhang, Z Chen, C Cheng, W Ruan, X Huang, D Zhao, D Flynn, S Khastgir, X Zhao Information Fusion		
•Probabilistic Robustness in Medical Image Classification	<u>FSEM 2026</u>	<u>Paper</u>
Yi Zhang, S Khastgir, X Zhao Early Career Researcher Symposium, University of Warwick		
•Advancing Probabilistic Robustness via Algorithmic Stability	<u>Preprint 2026</u>	<u>Paper</u>
Yi Zhang, Z Wang, S Khastgir, X Zhao Under-review		
•Enhancing Probabilistic Robustness Under Natural Corruptions via Data Augmentation	<u>Preprint 2026</u>	<u>Paper</u>
Yi Zhang, Z Wang, X Zhang, S Khastgir, X Zhao Under-review		
•Adversarial Fine-Tuning Reduces Memorization and Privacy Risk in Text-to-Image Diffusion Models	<u>Preprint 2026</u>	<u>Paper</u>
Yi Zhang, Z Wang, C Zhen, W Ruan, S Khastgir, X Zhao Under-review		
•Long-term Memory for Large Language Models through Topic-based Vector Database	<u>IALP 2023</u>	<u>Paper</u>
Yi Zhang, Z Yu, W Jiang, Y Shen, J Li. 2023 International Conference on Asian Language Processing		
•Non-Parametric Probabilistic Robustness: A Conservative Metric with Optimized Perturbation Distributions	<u>ICML 2026</u>	<u>Paper</u>
Z Wang, Yi Zhang, S Khastgir, C Maple, X Zhao Proceedings of the 43rd International Conference on Machine Learning		
•Fragile by Design: On the Limits of Adversarial Defenses in Personalized Generation	<u>AAAI 2026</u>	<u>Paper</u>
Z Chen, Yi Zhang, X Yin, C Qin, X Zhao, X Huang, W Ruan The Annual AAAI Conference on Artificial Intelligence		
•TARP-VP: Towards Evaluation of Transferred Adversarial Robustness and Privacy on Label Mapping Visual Prompting Models	<u>NeurIPS 2024</u>	<u>Paper</u>
Z Chen, Yi Zhang, F Wang, X Zhao, X Huang, W Ruan The Annual Conference on Neural Information Processing Systems		

WORK EXPERIENCE

•OpenDOC	Algorithm Lead Engineer	Hangzhou, China	Feb–Sep 2023
•ByteDance AI Lab	Algorithm Project Engineer Intern	Beijing, China	Apr–Aug 2022
•DiDi Global	Algorithm Project Engineer Intern	Beijing, China	Sep–Mar 2021

AWARDS

•The Best Paper Award	FSEM Early Career Researcher Symposium	Jul. 2026
•The Warwick Star Award	Postgraduate Research Student Award	Jul. 2025
•NVIDIA Academic Grant Program	Accelerating Innovation in Academia	Dec. 2024

INVITED TALKS

Journal of Reliability Science and Engineering	Reliability of AI Systems	Apr. 2026
FSEM 2026: Warwick’s Early Career Researcher Symposium	Probabilistic Robustness in Trustworthy AI	Jul. 2026