Mengdi Zhu, Ph.D. **(she/her)**
Postdoctoral Researcher
zhum@ufl.edu | 386-627-3859 | LinkedIn | GitHub

Education

University of Florida — Gainesville, FL
Ph.D. in Electrical and Computer Engineering, concentration on CV and ML — *May 2020 – Aug. 2025*
M.S. in Electrical and Computer Engineering, GPA: 3.39/4.0 — *Aug. 2017 – May 2019*

Purdue University — West Lafayette, IN
B.S. in Aeronautical and Astronautical Engineering, GPA: 3.55/4.0 — *Jan. 2012 – Dec. 2015*

Publications

Multi-modal
"Towards Intelligent Hardware Assurance: Human-in-the-loop Error Localization and Resolution with Vision-Language Models", NeurIPS 2025
"Lyapunov-Stable Adaptive Control for Multimodal Concept Drift", NeurIPS 2025
ML & Generative AI
"Genetic Algorithm-Assisted Golden-Free Standard Cell Library Extraction from SEM Images",2025 26th International Symposium on Quality Electronic Design (ISQED), San Francisco, CA, USA, 2025, pp. 1-8, doi: 10.1109/ISQED65160.2025.11014403.
"MaGNIFIES: Manageable GAN Image Augmentation Framework for Inspection of Electronic Systems", J Hardw Syst Secur 8, 44–59 (2024). https://doi.org/10.1007/s41635-024-00145-7
"REFICS: Assimilating Data-Driven Paradigms Into Reverse Engineering and Hardware Assurance on Integrated Circuits", IEEE Access, vol. 9, pp. 131955-131976, 2021, doi: 10.1109/ACCESS.2021.3114360.
"Is this real? Susceptibility to deepfakes in machines and humans", doi: 10.31219/osf.io/etxzw, 2024
"Kin-Wolf: Kinship-established Wolfs in Indirect Synthetic Attack", 2024 IEEE International Joint Conference on Biometrics (IJCB), Buffalo, NY, USA, 2024, pp. 1-9, doi: 10.1109/IJCB62174.2024.10744495.
Reinforcement Learning
"LfRLD: Learning From Reinforcement Learning Demonstrations", doi: 10.36227/techrxiv.172927301.18452996/v1, 2024.

Large Language Models (LLM)
"Is the Digital Forensics and Incident Response Pipeline Ready for Text-Based Threats in LLM Era?", ArXiv, abs/2407.17870.

Projects and Research Experience

Multimodal Adaptive System — Mar. 2025 – present
Florida Institute for National Security (FINS)
- Designed and implemented a **scalable data pipeline** to streamline ingestion, preprocessing, and integration of multimodal datasets, enabling efficient training of complex models
- Researched and optimized **VLM algorithms** for an adaptive multimodal system, innovating resource-efficient training techniques that enabled large-scale model training on constrained hardware

Automated Reverse Engineering for Integrated Circuits — Sep. 2022 – present
Florida Institute for National Security (FINS)
- Currently developing **a recommendation system** to resolve data corruptions by providing top-N possible identities of corrupted standard cells for quick resolution
- Designed and implemented a **multimodal ML algorithm** to enhance data assurance and improve algorithmic robustness to noise across diverse tasks, while integrating human-in-the-loop feedback to guide data collection and refinement

- Built a **computer vision pipeline** to extract design rules with high precision, achieving an error rate below 0.01μm; this work represents the first known attempt at automated design rule extraction from layout images
- Developed an **image processing pipeline** to transform IC layout images into pseudo-language encodings, enabling faster imaging data processing and facilitating the application of multimodal algorithms to IC layout data
- Developed an **unsupervised Genetic Algorithm-based method** for golden-free standard cell extraction from IC layouts, reducing manual effort by 90% and introducing a novel approach to standard cell identification without reference data

Human Study with Deepfakes May 2021 – Present

Florida Institute for National Security (FINS)

- Engineered **StyleGAN-based** media synthetic pipelines to support recognition research, deploying high-accuracy detection models that achieved over 95% performance
- Conducted **performance analysis** and **interpretability assessment** of ML models, benchmarking results against human-level performance

Evaluation of Deepfake Generation & Detection May 2020 – Mar. 2022

Florida Institute for Cybersecurity (FICS)

- Implemented and fine-tuned 7 **GAN-based deepfake generation models** leveraging 3 open-source media datasets to advance synthetic media research and innovation
- Deployed, and benchmarked 13 **deepfake detection models (CNNs, RNNs)** across 7 synthetic media datasets, achieving over 85% accuracy and evaluating robustness

Machine Learning-based Smart Fuzzing May 2021 – Oct. 2022

Florida Institute for Cybersecurity (FICS)

- Developed and trained **ML classifiers (SVM, MLP, Naive Bayes)** to identify test cases most likely to trigger hardware Trojans, achieving 100% accuracy in distinguishing triggering from non-triggering patterns

Specialized Skills

Machine Learning: PyTorch, Tensorflow, scikit-learn
Python: Numpy, Pandas, SciPy
Computer Vision: OpenCV, CNN architectures
Tools: Git, Linux, Slurm, VSCode, PyCharm