CAREER: Protecting Deep Learning Systems against Hardware-Oriented Vulnerabilities

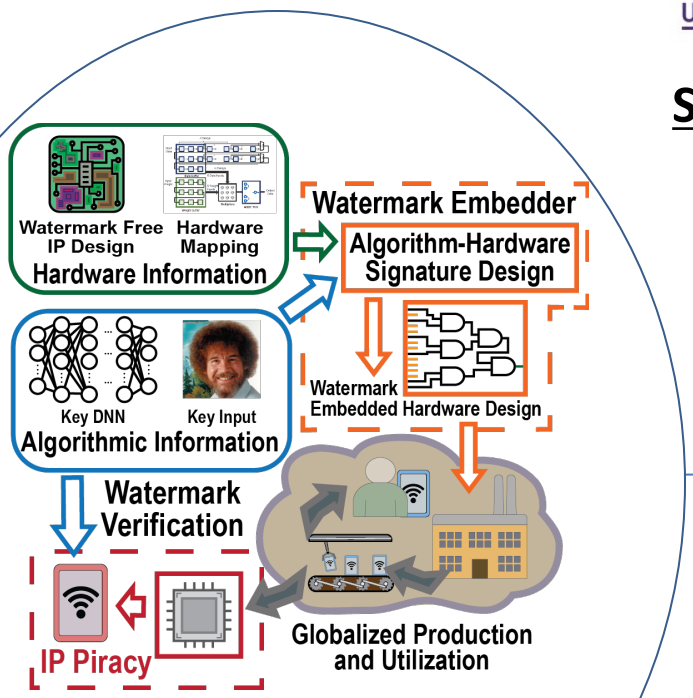
CLEMSON UNIVERSITY

Challenge:

- There is a lack of systematic studies on hardware-oriented vulnerabilities and countermeasures, which also opens up demand for AI security education.

Solution:

- Watermarking for protecting hardware intellectual property (AAAI22)
- Investigation of novel vulnerabilities and attacks (AAAI22, WACV22, ICASSP22)



DL Hardware Watermarking

Embedding a hardware watermark into deep learning accelerators.

Scientific Impact:

- Advances the understanding of hardware-oriented vulnerabilities and defenses for AI systems.
- Further validates the need to protect both algorithm and hardware for next-generation AI applications.

Broader Impact and Broader Participation:

- This project yields novel methodologies for ensuring trust in AI systems from both the algorithm and hardware perspectives to meet the future needs of commercial products and national defense.
- Results are integrated into my Creative Inquiry course "AI Security and Privacy".

Project # 2047384
Clemson University
Yingjie Lao
ylao@clemson.edu