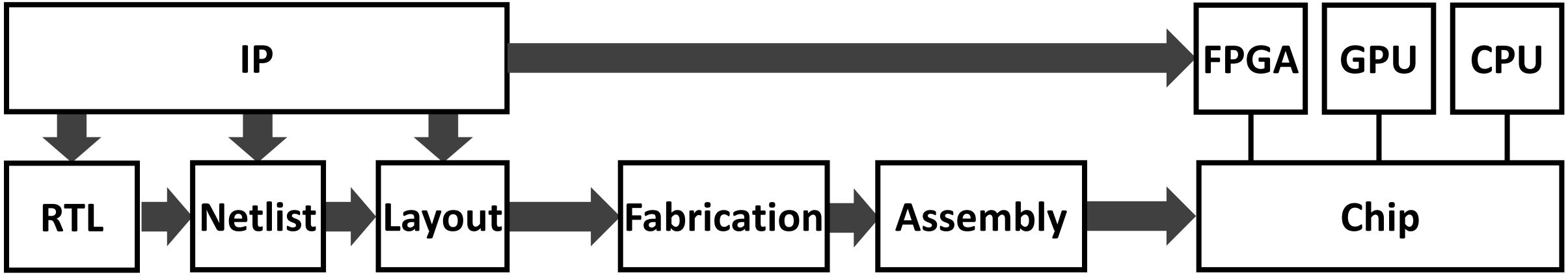
Global Electronic Supply Chain Security: What Can Asian Pacific Region Do About it?

Security Challenges of AI Processor

Xiaowei Li

State Key Laboratory of Computer Architecture
Institute of Computing Technology
Chinese Academy of Sciences

Supply Chain and Our Researches



Hardware Trojan

- Design
- Detection
- Defense

Physical Unclonable Function

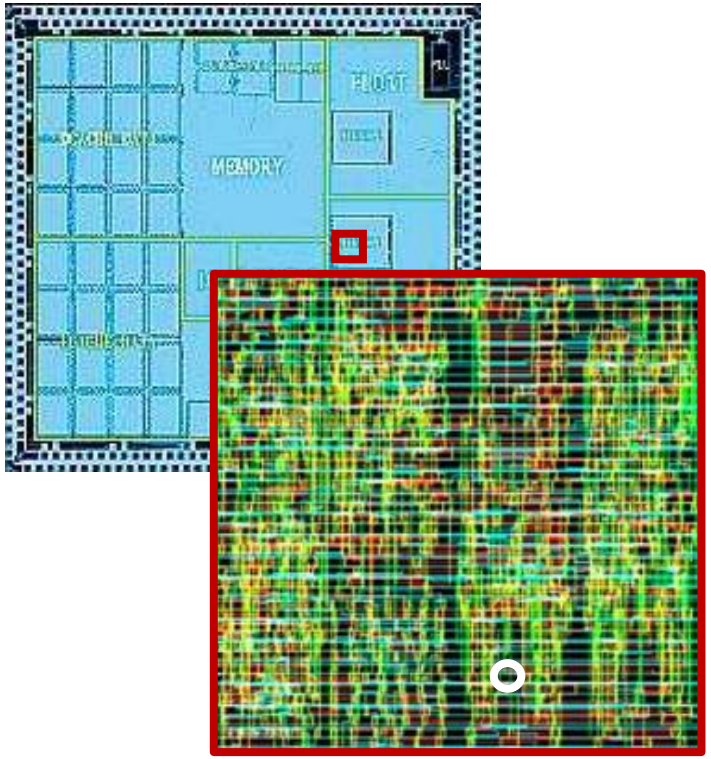
- Design

IP Protection

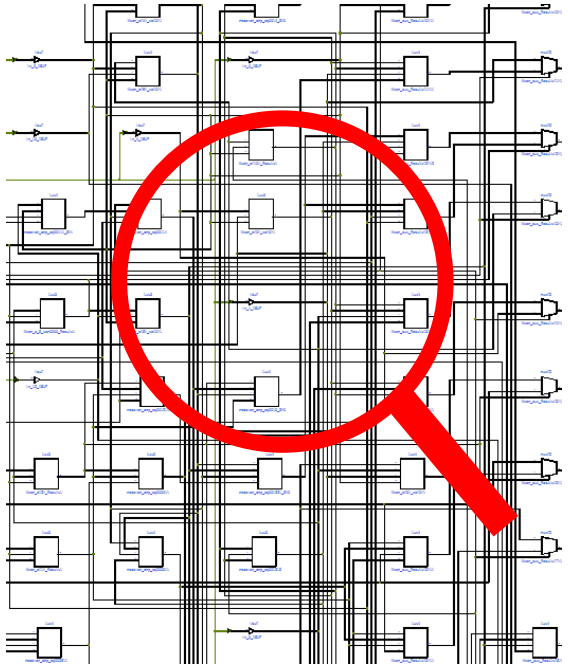
- Test
- Attack

Some Observations (Main Challenges)

High Integration vs. Tiny Malicious Circuit

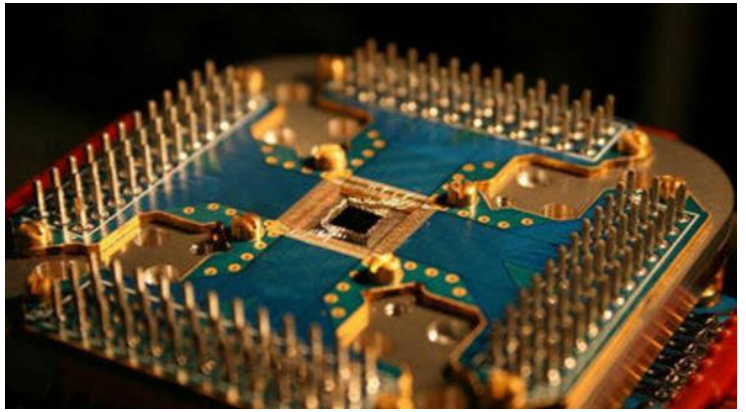


IP Protection vs. Vulnerability Detection

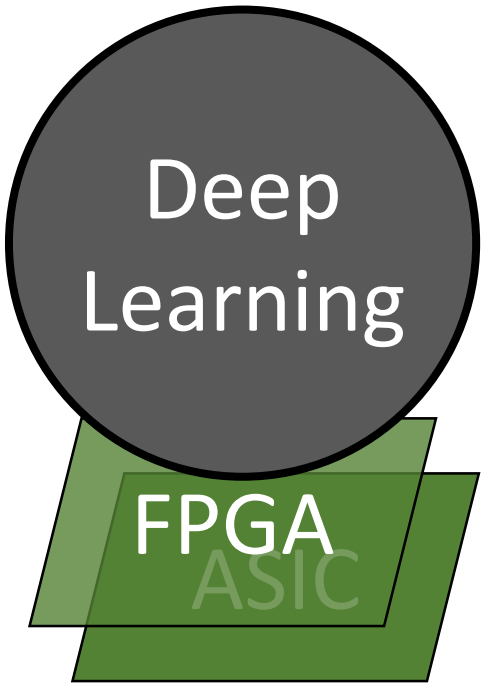


Cracking Complexity vs. High Performance Computation

Quantum Computer



Security Challenges in Deep Learning Systems



- Autonomous Driving
  - Camera, Laser, …
- Automatic Speech Recognition
  - Microphone, …
- Unmanned Aerial Vehicle
  - Camera, Gyroscope, …
- … …

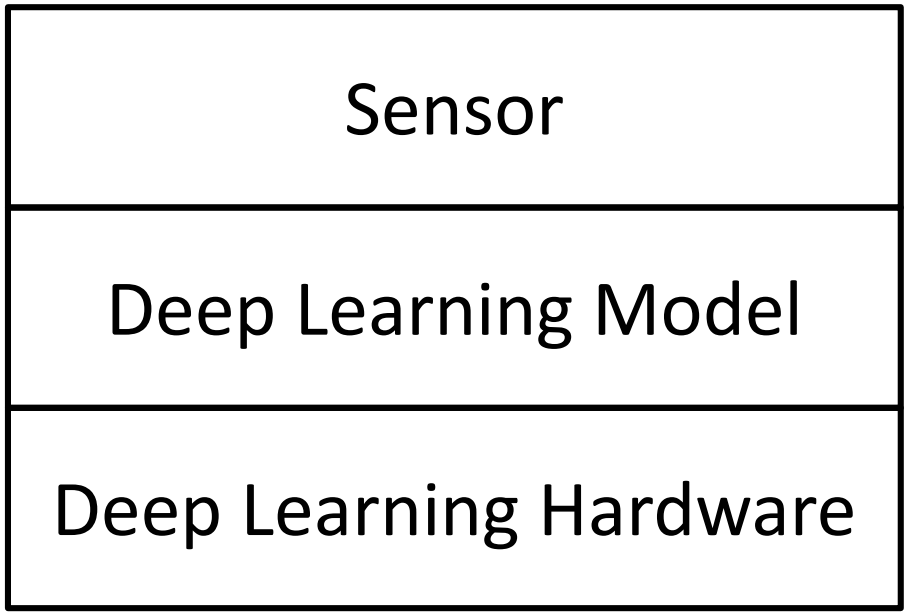
Sensors

- Figures with special patterns
- Sound wave with special frequencies
- …

- Control prediction accuracy
- …

The sensor based deep-learning system could be one of the platforms where the IC security vulnerabilities explode

What Can We Do? (Security Challenges of AI Processor)



Add defend layer between the sensor and the hardware to process the sensor data

Analyze the bias of deep learning model to reduce design vulnerabilities

Adopt more sensors and more IPs to tolerate malicious behaviors

Analyze abnormal behaviors to find the root causes

What's More?