Trust Issues in the Semiconductor Industry

Junghhee Lee
j_lee@korea.ac.kr
Your Speaker

• Education
  – Ph.D  Georgia Institute of Technology (2013)
  – B.S.  Seoul National University (2000)

• Appointments
  – Assistant/Associate Professor
    Korea University (2019-Present)
  – Assistant Professor
    University of Texas at San Antonio (2014-2019)
  – Engineer
    Samsung Electronics (2003-2008)

• Research area
  – Hardware security (processor, memory, non-volatile memory, storage, dedicated hardware)
Trust vs Security

Not implemented as designed

Not used as intended
Globalization

http://proutglobe.org/2013/12/three-tier-business-model-semiconductor-industry/
Typical Design Flow

Automation Tool → Design → Synthesis → Layout → Manufacturing

IP

Soft IP → Firm IP → Hard IP
Untrusted Foundry

Recycling

Counterfeit

Overproduction
IC Recycling

Collect discarded ICs

Replace the marking

Sell as new
Overproduction

Design House

Order 1M

Foundry

Return 1M

Extra 1M

Distributor

Sell Extra 1M
Counterfeit

• Recycling
• Overproduction
• Forged documents
• Defective parts
Countermeasures

- Detection
  - Inspection
    - Physical
    - Electrical
  - Passive metering
    - Non-functional identification
    - Functional identification
- Prevention
  - Active metering
  - Secure split testing
    - Internal control
    - External control
Untrusted Design House

- **Automation Tool**
- **Automation Tool**
- **Automation Tool**

**IP**

- **Design**
- **Synthesis**
- **Layout**

- **Soft IP**
- **Firm IP**
- **Hard IP**

**Manufacturing**
Piracy

- Unlicensed usage
- Reverse engineering
Countermeasures

Detection

Watermarking
- Constraint-based
- Test-based
- Don't care condition
- Power analysis
- Place-and-route

Prevention

Obfuscation
- State space (FSM)
- Logic

Protection of watermark
- Watermark obfuscation
- Multiple small watermark
- Parity in watermark
Untrusted IP

IP

Design

Synthesis

Layout

Manufacturing

Automation Tool

Automation Tool

Automation Tool

Soft IP

Firm IP

Hard IP
Hardware Trojan

• A hidden malicious circuit
• It does
  – Lead to malfunction
  – Leak information
• Motivation
  – Military
  – Financial
Trojan Structure

- Trigger
  - Combinational
  - Sequential

- Payload
  - Change signals
  - Leak information
  - Downgrade performance
Countermeasures

Detection
  - Pre-silicon
    - Destructive
    - Run-time
      - Logic test
      - Side-channel
  - Post-silicon
    - Non-destructive
      - Test-time
        - Obfuscation
        - Functional filler cells
  - Prevention
    - Split manufacturing
Summary

• Globalization of semiconductor industry
• Untrusted parties
• Counterfeit, piracy, Trojan, ...
• Technical countermeasures