Hardware Security and Trust

Giorgio DI NATALE

giorgio.dinatale@lirmm.fr
Motivation

- **Security** and **trust** play a critical role as computing is intimately integrated in the infrastructures we depend on.

- Hardware Security
  - dealing with (secret) data in hardware devices

- Hardware Trust
  - dealing with design and manufacturing of devices
HARDWARE SECURITY
Scenario

• How to protect a (digital) secret:
  – Secure storage of confidential data
  – Cryptographic capabilities

• Implementation:
  – Crypto algorithms integrated as hardware devices
  – E.g., smartcards, crypto-cores, crypto-processors, hardware security module
Implementation Attacks

\[ f_1(PT, Key, time) = f_2(PT, Key, time) \]
Implementation Attacks – Types of Attacks

Access to secure devices storing other parties’ secrets

- Side Channel Attacks
  - Power
  - Electromagnetic
  - Light
  - ...

- Fault Attacks
  - Laser
  - Electromagnetic
  - ...

Test Infrastructures
Implementation Attacks – Types of Attacks

Side Channel Attacks
- Power
- Electromagnetic
- Light
- ...

Fault Attacks
- Laser
- Electromagnetic
- ...

Test Infrastructures
Based on information gained from the non-primary interface of the physical implementation of a cryptosystem

- Timing information
- Power consumption
- Electromagnetic leaks
- Sound
- Light
- ...

Side-Channel Attacks
Simple Power Analysis on RSA

Input: $X, N, K=(k_{j-1}, ..., k_1, k_0)_2$
Output: $Z = X^K \mod N$

1: $Z = 1$;
2: for $i=j-1$ downto 0 {
3: \hspace{1em} $Z = Z \times Z \mod N$ //Square
4: \hspace{1em} if ($k_i==1$) {
5: \hspace{2em} $Z = Z \times X \mod N$ //Multiply
6: \hspace{1em} }
7: }

---

Key Bits

Operation

Waveform
• Actually not so simple…
  – Noise
  – Interrupts
  – Multi-core architectures
  – Peripherals
  – …
Countermeasures

• Goal: removing the correlation between processed data and the physical interface

• Methods:
  – Masking: adding randomness in the intermediate values and operations
  – Hiding: making side-channel independent of intermediate values and operations
e.g., constant power consumption
Implementation Attacks – Types of Attacks

- Side Channel Attacks
  - Power
  - Electromagnetic
  - Light
  - ...

- Fault Attacks
  - Laser
  - Electromagnetic
  - ...

Test Infrastructures
Fault Attacks

**Hypothesis**: Injection forces a ‘0’ on a single bit of the secret key

1) \( C_{OK} = E(P) \)
2) Calculate \( C' = E(P) \), while injecting a fault
3) If \( C' = C_{OK} \) \( \rightarrow \) target bit is ‘0’
   else \( \rightarrow \) target bit is ‘1’
Injection means

• To inject faults affecting critical paths
  – Under/over powering
  – Altering the clock
  – Altering the temperature

• To inject precise faults in space and time
  – Laser injections
  – Electro Magnetic injections
Countermeasures

• IC Packaging
• Fault detectors:
  – Laser/light, bulk current
  – They can generate false positives
• Error detectors, based on redundancy
Implementation Attacks – Types of Attacks

Side Channel Attacks
- Power
- Electromagnetic
- Light
- ...

Fault Attacks
- Laser
- Electromagnetic
- ...

Test Infrastructures
Manufacturing Process

- Manufacturing process of integrated circuit is not totally controlled:
  - Dust, physical mechanisms, spot defect
  - Process variability
  - Assemblage faults
Scan-based Design

Primary Inputs → Combinational Logic → Primary Outputs

Scan Enable → FF → Scan In → FF → Scan Out

Observability of all states
Controllability of all states
Scan attacks presentation

• Scan attacks:
  – Exploit observability and controllability offered by scan chains
  – Principle: switch between functional and scan modes
  – Goal: Retrieve embedded secret data
Countermeasures

• Leave the scan chain unbound
• Built-In Self-Test
• Secure Test Access Mechanism
  – Authentication (expensive)
  – No in-field debug/diagnosis
  – Not easy to integrate in design flow
• Scan Chain Encryption
Conclusions - Hardware Security

• Cryptography has +2000 years history and experience
• Hardware Security is still a young research field
HARDWARE TRUST
The Untrusted Chain
The Untrusted Chain

Design Time

Specs → Design

IP → Tools → TechLib

Manufacturing Time

Fabrication → Test
The Untrusted Chain

Design Time
- Specs
  - IP
  - Tools
  - TechLib

Design

Manufacturing Time
- Fabrication
- Test

Life Time
- Distribution
- Use Life
- Recycling
The Untrusted Chain

Design Time
- Specs
- Design
  - IP
  - Tools
  - TechLib

Manufacturing Time
- Fabrication
- Test
  - Untested
  - Discarded

Life Time
- Distribution
- Use Life
  - Recycling

- IP Theft
- Netlist / Mask Theft
- Overbuilding
- IC Piracy
- Repackaging
  - Refurbishing
The Untrusted Chain

Design Time
- Specs
- Design
  - IP
  - Tools
  - TechLib

Manufacturing Time
- Fabrication
- Test
  - Untested
  - Discarded

Life Time
- Distribution
  - IC Piracy
  - Repackaging
  - Refurbishing
- Use Life
- Recycling

Additional notes:
- IP Theft
- Netlist / Mask Theft
- Overbuilding
The Untrusted Chain

Design Time
- Specs
- Design
  - IP
  - Tools
  - TechLib

Manufacturing Time
- Fabrication
- Test
- Untested Discarded

Life Time
- Distribution
- Use Life
- Recycling

- IP Theft
- Netlist / Mask Theft
- Overbuilding
- IC Piracy
- Repackaging
- Refurbishing
The Untrusted Chain

Design Time
- Specs
- Design
- IP
- Tools
- TechLib
- IP Theft
- Netlist / Mask Theft
- Overbuilding
- IC Piracy
- Repackaging
- Refurbishing
- Untrusted
- Chain

Manufacturing Time
- Fabrication
- Test
- Untested
- Discarded

Life Time
- Distribution
- Use Life
- Recycling
Counterfeiting types

- Recycled, Defective
- Overproduced
- Cloned
- Tampered
Counterfeit types

Recycled

• Electronic component that is recovered from a system and then modified to be misrepresented as a new component

• Problems:
  – lower performance
  – shorter lifetime
  – damaged component
Counterfeit types

Overproduced

• Overproduction occurs when foundries sell components outside of contract with the design houseparts

• Problems:
  – loss in profits for the design and IP owner
  – reliability threats since they are often not subjected to the same rigorous testing as authentic part
Counterfeit types

Cloned

• A copy of a design, in order to eliminate the large development cost of a part

• Methods:
  – Reverse engineering
  – By obtaining IP illegally (also called IP theft)
  – With unauthorized knowledge transfer from a person with access to the design
Counterfeit types
Tampered – Hardware Trojan Horses

• A Hardware Trojan Horse is a malicious modification of an integrated circuit
  – Performed at any design or manufacturing step

• Examples:
  – Backdoors, time bombs

• A real threat?
Counterfeiting detection

- Cleaning, visual inspection
- Microscope & X Ray Inspections
- Side-Channel
- Testing
Counterfeiting prevention

- Aging detectors
- Hardware metering
- IC Camouflage
- IC Authentication
- HT Prevention
Counterfeiting prevention – Aging Detectors

• Sensors in the chip to capture the usage of the chip in the field
  – It relies on aging effects of MOSFETs to change a ring oscillator frequency in comparison with the golden one embedded in the chip.

• Techniques:
  – Fuse-based technology to record usage time
  – Differential measurement
Counterfeiting prevention – Hardware Metering

• A set of security protocols that enable the design house to achieve the post-fabrication control of the produced ICs to prevent overproduction
  – Post-Manufacturing Activation
  – Adding a Finite-State Machine (FSM) which is initially locked and can be unlocked only with the correct sequence of primary inputs
  – Logic Encryption
Counterfeiting prevention – IC Camouflage

- Standard-cells are re-designed not to disclose their identity
Counterfeiting prevention — IC Authentication

• Physically Unclonable Functions (PUF)
  — Able to generate random and stable responses

• After manufacturing, each device is challenged by several random inputs

• Responses are stored in a secure database

• To authenticate the device, some of the challenges are used during mission mode
• Delays of all the paths from input to output: nominally identical

• Reality: because of process variations, all different!
HW Tojans prevention – Split Manufacturing

- Front End Of Line (FEOL) layers (transistor and lower metal layers) are fabricated in an untrusted foundry.
- Back End Of Line (BEOL) in a trusted low-end fab.
- It is considered secure against reverse engineering as it hides the BEOL connections from an attacker in the FEOL foundry.
Conclusions

• Hardware Security and Trust are big challenges
• It might become even worst because of:
  – Limited resources (IoT)
  – Safety (autonomous cars)
THANK YOU