Physical Security – Embedded Systems

Part IV
IP Protection

IP Protection

- Confidentiality
- Authentication
- Integrity

IP Confidentiality

- IPs (Intellectual Properties) need to be protected
- Patents provide juridical/financial protection…
  - Authorship/Ownership
  - Legitimate use
- Illegitimate use must be proved!
- How to prove that your competitor stole your solution?
  - E.g., reverse engineering
  - Quite complex and expensive ☹
  - Sometimes impossible ☹
- Obfuscation
  - Encrypted bitstreams, …

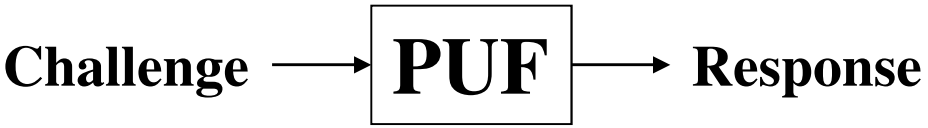
IP Authentication

- Need to identify the device efficiently and securely
  - "Fingerprint" of the device
  - Guarantee the origin of the design
  - Detect and Avoid fake products on the market
- Traditional solution
  - Embed a unique secret key in non volatile memory
  - Use crypto to authenticate the device through its secret key
- But…
  - Adversary may be able to extract the key
  - Who embeds and tests the keys? Is it trustable?
  - What if no crypto available?

[Devadas, CHES 2009]

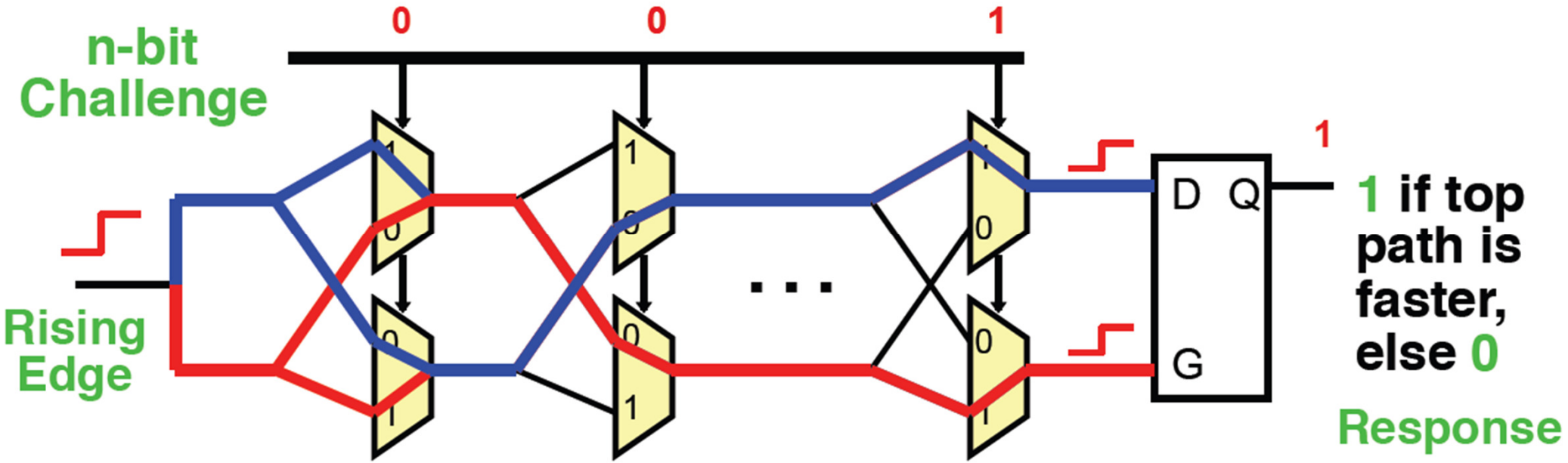
Physical Unclonable Function (PUF)

- Identification of a device, by unique physical properties
- Extract/Generate secrets from circuit of any complexity



- Process variations: no two IC are identical (even with the same layout)
  - Hard to predict
  - Intrinsic in the fabrication process
  - Future proof: relative variation increases as technology advances
- Examples
  - Path delays (Arbiter)
  - Ring-Oscillators
  - Uninitialized SRAM memory state
  - …

Simple PUF Example



- Compare two paths with an identical delay in design
  - Random process variation determines which path is faster
  - An arbiter outputs 1-bit digital response
- Multiple bits can be obtained by either duplicate the circuit or use different challenges
  - Each challenge selects a unique pair of delay paths

PUF Types

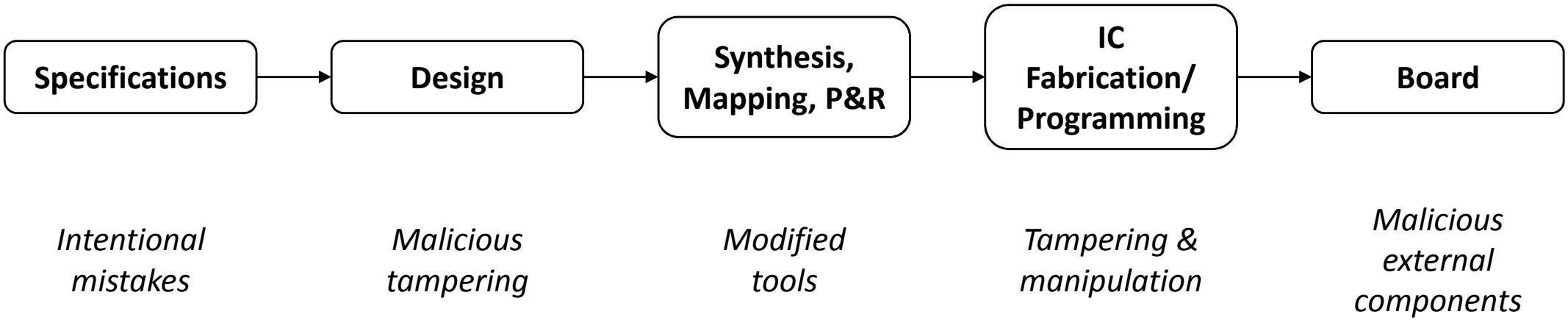
- **Strong**
  - Complex challenge/response mechanism
  - Many, many possible challenges
  - Impossible to clone
  - Impossible to map all Challenge/Response pairs
  - Hard to predict
- **Controlled**
  - Based on strong PUF, plus additional control logic
  - Control logic used to filter PUF I/O
- **Weak**
  - Very few challenges
  - Responses never meant to be used externally

PUF Applications

- **System Identification**
  - Very similar to biometrical identification systems
  - Limited security
- **Key Generation**
  - **Non volatile key storage**
  - **Unique key material**
  - **No key programming required**
- **Hardware Entangled Cryptography**
  - **Embedded integration of PUFs in crypto primitives**
  - **No digital key present at any point → Not for every application**

IP Integrity

- **Do you trust your design chain?**
  - **Several phases of IC fabrication are outsourced**



- **Circuit can modified any time by inserting unknown functionality, i.e.**

Hardware Trojan

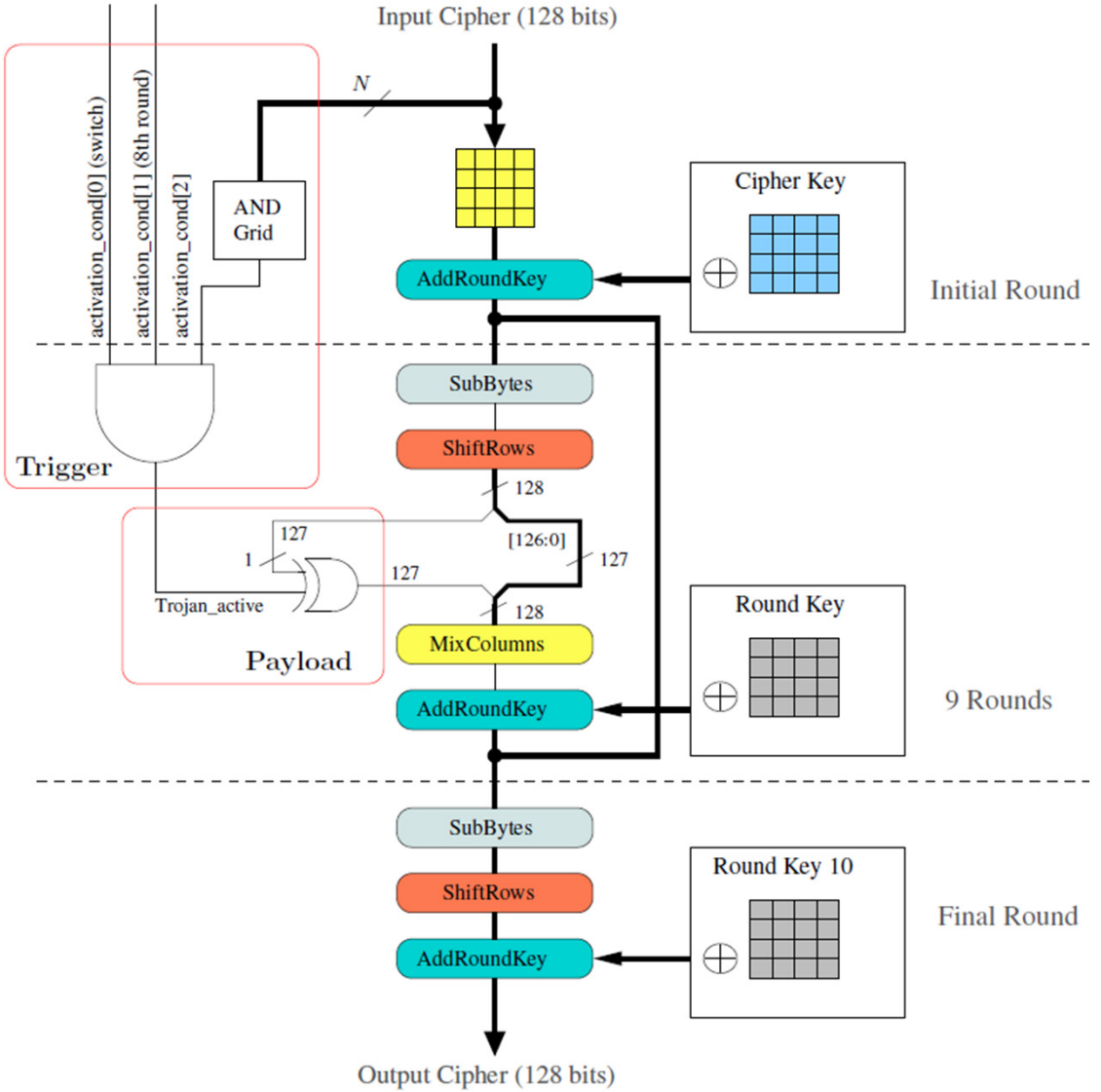
Hardware Trojan

- **Trigger**

  Activating the Trojan on a specific condition

- **Payload**

  The malicious function



[S. Bhasin et al., Hardware Trojan Horses in Cryptographic IP Cores @ FDTC2013]

HT Taxonomy (1/4)

Insertion phase

- **Specification**
- **Design**
- **Fabrication**
- **Assembly/Packaging**

HT Taxonomy (2/4)

Activation mechanism

- Always On
- Triggered
  - Internally
    - Time
    - Other physical condition
  - Externally
    - User input
    - Component output

HT Taxonomy (3/4)

Effect

- **Change functionality**
- **Degrade performance**
- **Denial of Service**
- **Information leak**

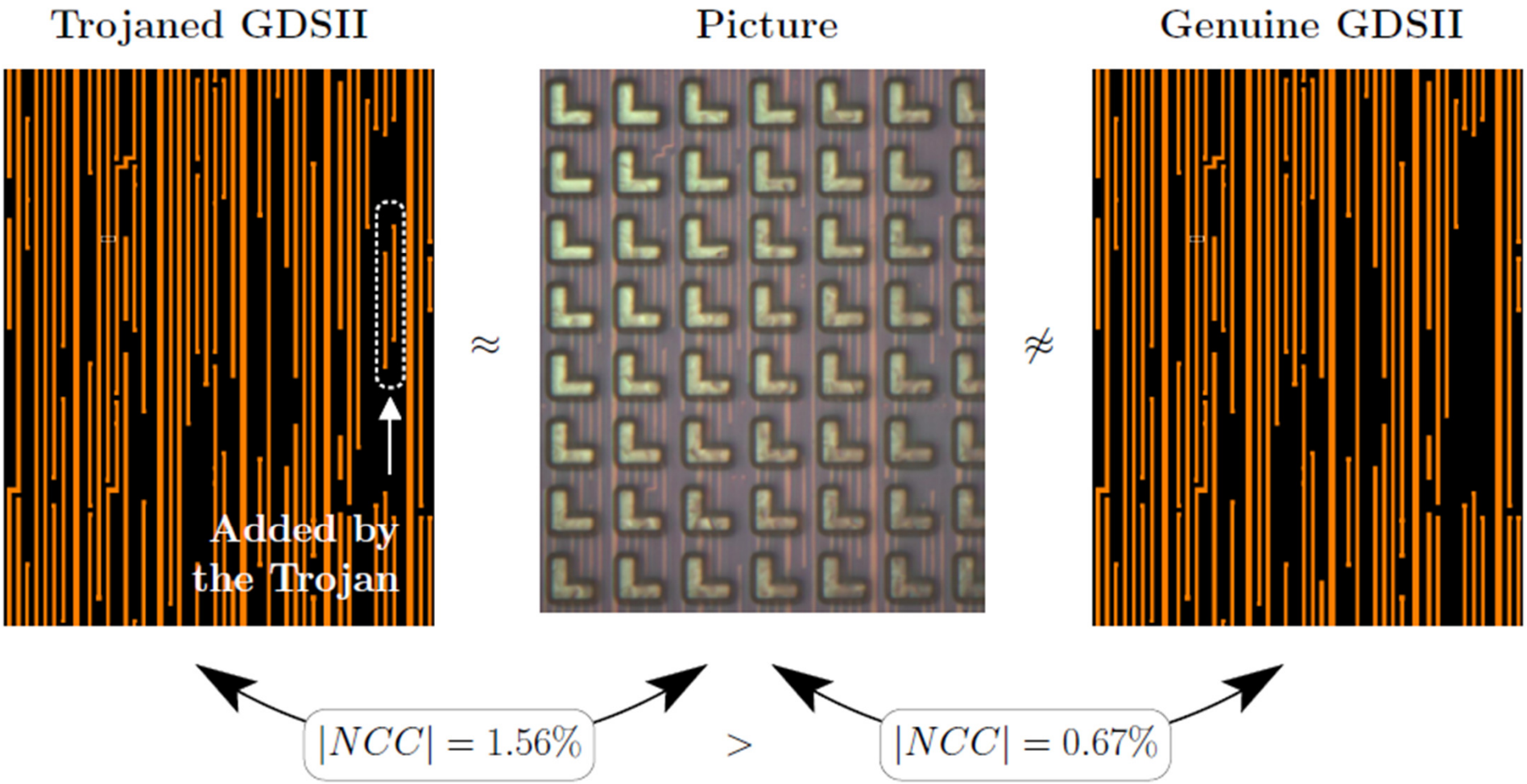
HT Taxonomy (4/4)

Other…

- **Abstraction level**
  - System, RTL, gate, layout, physical, …
- **Location**
  - CPU, memory, IO module, clock or power grid, …
- **Characteristics**
  - Distribution, size, …
  - Type parametric/functional), structure (layout)

HT Detection – Visual Inspection

Cross-correlation analysis of microscope images (invasive!)



HT Non-Destructive Detection

- Testing
  - Logic Test
- Ring Oscillators
- Gate Level Characterization
- Side Channel Analysis
  - Delay
  - Current
  - Thermal
  - Power
  - EM
  - …

HT Non-Destructive Detection

- Set Trojan-free sample as golden reference
- Characterize golden reference
- Characterize unknown sample
- Compute [dis]similarity
- Classify

- Objectives
  - Maximize *true* results (identify always Trojans infections and correct samples)
  - Minimize *false* results (e.g., missing Trojans, discarding good circuits)
  - Even without triggering the HT!

- Best dissimilarity metrics?