Hardware Trojans

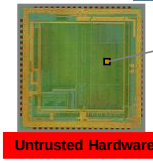
Mohammad Tehranipoor

ECE 6095: Hardware Security & Trust
University of Connecticut
ECE Department

What's Hardware Trojan?

- Hardware Trojan:
  - A malicious addition or modification to the existing circuit elements.
- What hardware Trojans can do:
  - Change the functionality
  - Reduce the reliability
  - Leak valuable information
- Applications that are likely to be targets for attackers
  - Military applications
  - Aerospace applications
  - Civilian security-critical applications
  - Financial applications
  - Transportation security
  - More

Hardware Trojan – Back Door



Antenna

Untrusted Hardware

- Adversary can send and receive secret information
- Adversary can disable the chip, blowup the chip, send wrong processing data, impact circuit information etc.

- Adversary can place an Antenna on the fabricated chip
- Such Trojan cannot be detected since it does not change the functionality of the circuit.

Time Bomb

Untrusted Hardware

- Counter
- Finite state machine (FSM)
- Comparator to monitor key data
- Wires/transistors that violate design rules

- Such Trojan cannot be detected since it does not change the functionality of the circuit.
- In some cases, adversary has little control on the exact time of Trojan action
- Cause reliability issue

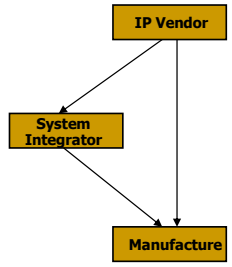
Applications and Threats

Thousands of chips are being fabricated in untrusted foundries

IC/IP Trust Problem

- Chip design and fabrication is becoming increasingly vulnerable to malicious activities and alterations with globalization.
- IP Vendor and System Integrator:
  - IP vendor may put a Trojan in the IP
  - IP Trust problem
- Designer and Foundry:
  - Foundry may put a Trojan in the layout design.
  - IC Trust problem

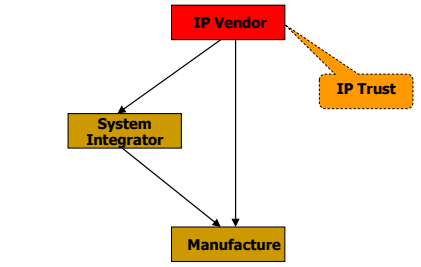
Hardware Threats Source



Any of these steps can be untrusted

7

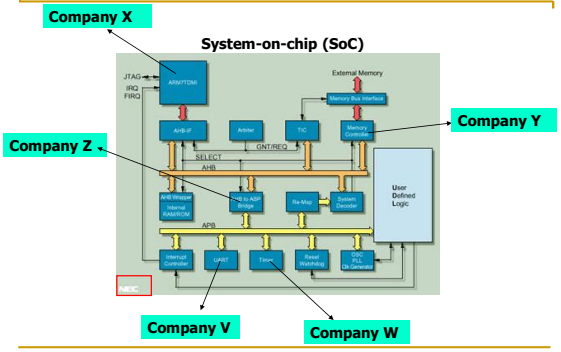
Hardware Threats Source



Untrusted

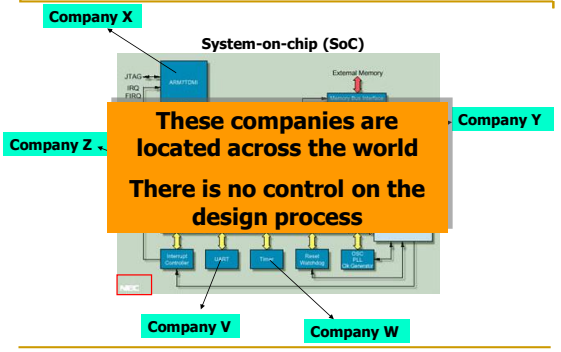
8

Issues with Third IP Design



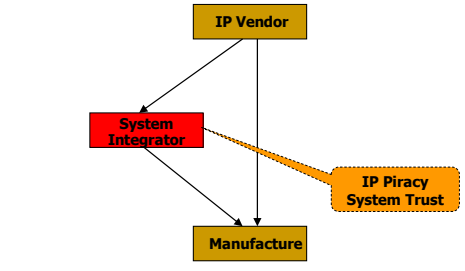
9

Issues with Third IP Design



10

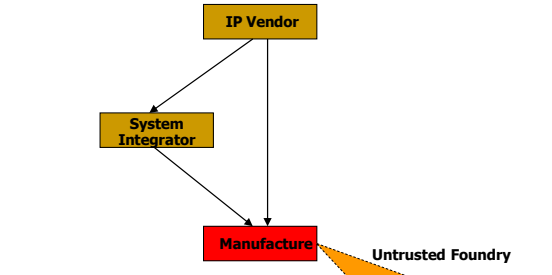
Hardware Threats Source



Untrusted

11

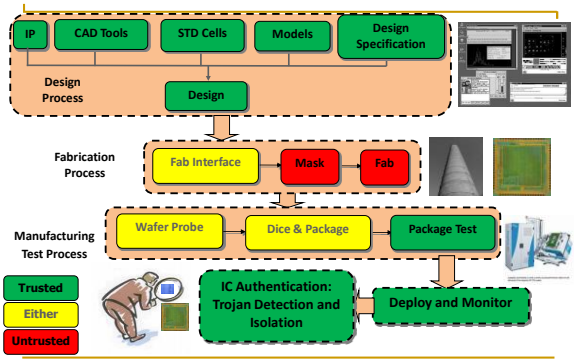
Hardware Threats Source



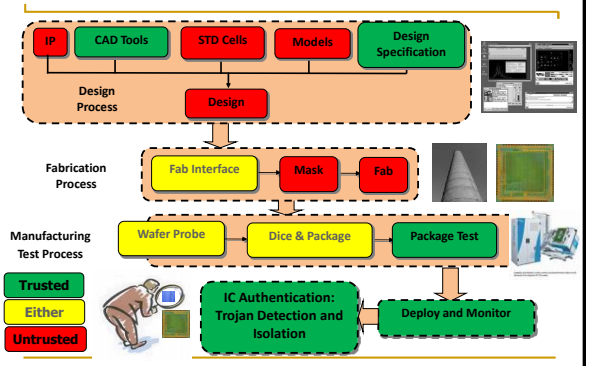
Untrusted

12

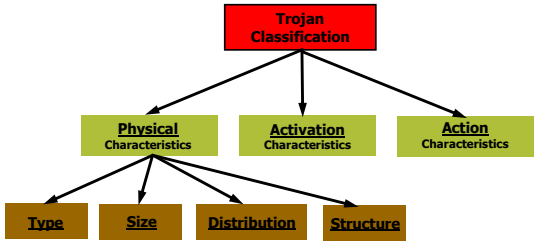
ASIC Design Process – Untrusted Foundry



Untrusted Designer and Foundry

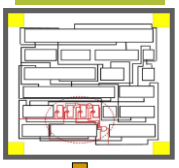


Trojan Taxonomy

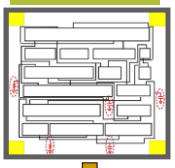


Example: Type

Functional



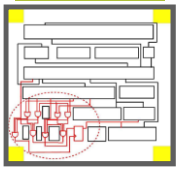
Parametric



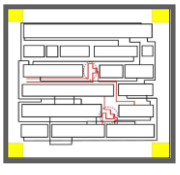
- **Functional**
  - Addition or deletion of components
  - Sequential circuits
  - Combinational circuits
  - Modification to function or no change
- **Parametric**
  - Modifications of existing components
    - Wire: e.g. thinning of wires
    - Logic: Weakening of a transistor, modification to physical geometry of a gate
    - Modification to power distribution network
  - Sabotage reliability or increase the likelihood of a functional or performance failure

Example: Size

Big



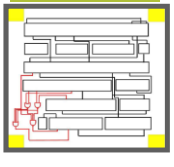
Small



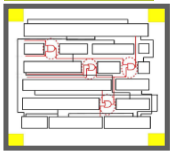
- **Size:**
  - Number of components added to the circuit
    - Small transistors
    - Small gates
    - Large gates
- **Depends on availability of:**
  - Dead spaces
  - Filler cells
  - Decap cells
  - Change in the structure

Example: Distribution

Tight



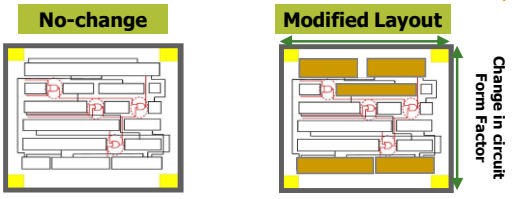
Loose



- **Tight Distribution**
  - Trojan components are topologically close in the layout
- **Loose Distribution**
  - Trojan components are dispersed across the layout of a chip

- **Distribution of Trojans depends on the availability of dead spaces on the layout**

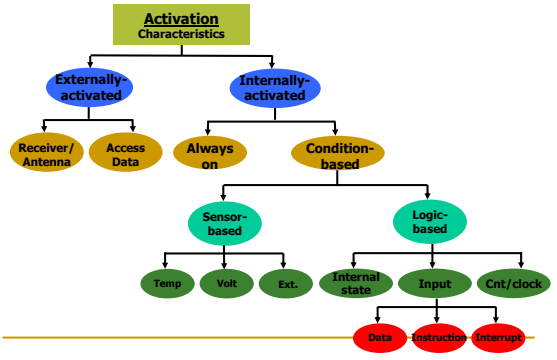
Example: Structure



- The adversary may be forced to regenerate the layout to be able to insert the Trojan, then the chip dimensions change
  - It could result in different placement for some or all the design components
- A change in physical layout can change the delay and power characteristics of chip
  - It is easier to detect the Trojan

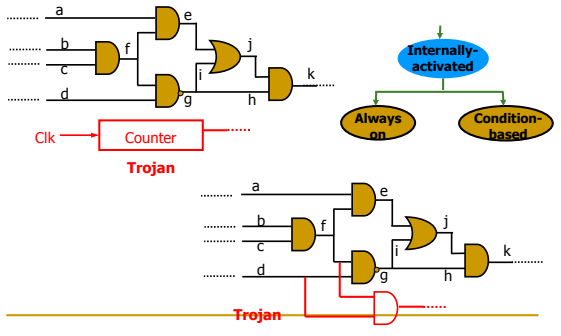
19

Trojan Taxonomy: Activation



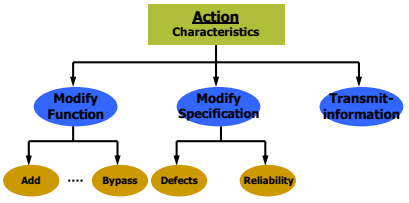
20

Activation: Internally Activated



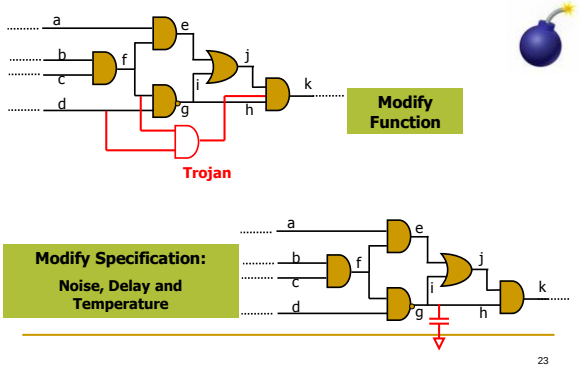
21

Trojan Taxonomy: Action



22

Example: Action



23

IP Trust & IP Security

- **IP Trust Issue**
  - Detect malicious circuits inserted by the third-party (IP designers or IP vendors)
  - Protect IP buyers
- **IP Security Issue**
  - Focus on whether IP cores are used illegally
  - Protect the ownership of IP designers and IP vendors

24

IP Trust

- IPs from untrusted vendors need to be verified for trust before use in a system design
- How can one establish that the IP does exactly as the specification, nothing less nothing more?
- IP cores: soft IP, firm IP and hard IP

- Challenges:
  - No known golden model for the IP as that for IC
  - Soft IP is just code so that we can not read its implementation
  - No side-channel information

25

Approaches For Pre-synthesis

- Formal verification
  - Property checking
  - Model checking
  - Equivalence checking

- Coverage analysis
  - Code coverage
  - Functional coverage

26

Formal Verification

- Formal verification
  - Ensuring IP core is exactly same as its specification, nothing more and nothing less
  - Three types of verification methods
    - Property checking: every requirement is defined as assertion in testbench and is checked
    - Equivalence checking: check the equivalence of RTL code, gate-level netlist and GDSII file
    - Model checking
      - System is described in a formal model (C, HDL)
      - The desired behavior is expressed as a set of properties
      - The specification is checked against the model

27

Coverage Analysis

- **Code coverage**
  - **Line coverage**
    - **Show which lines of the RTL have been executed**
  - **Statement Coverage**
    - **Spans multiple lines, more precise**
  - **FSM Coverage**
    - **Show which state can be reached**
  - **Toggle**
    - **Each Signal in gate-level netlist**
- **Function coverage**
  - **Assertion**
    - **Successful or Failure**

28

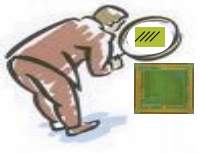
Suspicious Parts

- **If one of assertion is failed, the IP is untrusted.**
- **If coverage is not 100%, uncovered parts are suspicious.**

29

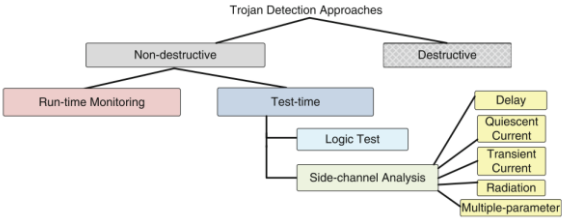
IC Trust:Trojan Detection and Isolation

- The objective is to ensure that the fabricated chip/system will carry out only our desired function and nothing more.
- Challenges:
  - Tiny: several gates to millions of gates
  - Quiet: hard-to-activate (rare event) or triggered itself (time-bomb)
  - Hard to model: human intelligence
  - Conventional test and validation approaches fail to reliably detect hardware Trojans.
    - Focus on manufacture defects and does not target detection of additional functionality in a design



30

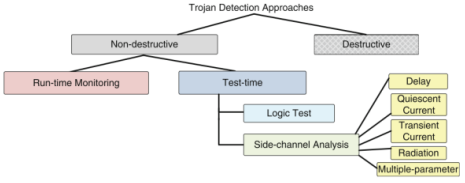
Classification of Trojan Detection Approaches



- Destructive Approach: expensive and time comsuming
  - Reverse engineering to extract layer-by-layer images by using Scanning Electron Microscope
  - Identify transistors or gates and routing elements by using a template-matching approach

Classification of Trojan Detection Approaches

- Non-destructive Approach
  - Run-time monitoring: Monitor abnormal behavior during run-time
    - Exploit pre-existing redundancy in the circuit
    - Compare results and select a trusted part to avoid an infected part of the circuit.
  - Test-time: Detect Trojans throughout test duration.
    - Logic-testing-based approaches
    - Side-channel analysis-based approaches



Logic-testing Approach

- Logic-testing approach focus on test-vector generation for
  - Activating a Trojan circuit
  - Observing its malicious effect on the payload at the primary outputs
  - Both functional and structural test vectors are applicable.
- Pros & Cons:
  - Pros: straight-forward and easy to differentiate
  - Cons:
    - The difficulty in exciting or observing low controllability or low observability nodes.
    - Intentionally inserted Trojans are triggered under rare conditions. (e.g., sequential Trojans)
    - It cannot trigger Trojans that are activated externally and can only observe functional Trojans.

Functional Test Deficiency

- Functional patterns could potentially detect a “functional” Trojan.
  - Exhaustive test would be effective
  - Not applicable for large circuits
  - E.g. 64 input adder → 2^{65} input combination (including carry in)
  - $2^{65} > 10^{18}$ – This is impractical
  - 100MHz is used → 10^{10} s → 317 years
  - Only a few and more effective patterns are used → Trojan can escape.
  - The fault coverage is low for manufacturing test
- In practice, structural tests are used.

MERO

- MERO:
  - Generate a set of test vectors that can trigger each rare node to its rare value multiple times (N times)
  - It improves the probability of triggering a Trojan activated by a rare combination of a selection of the nodes

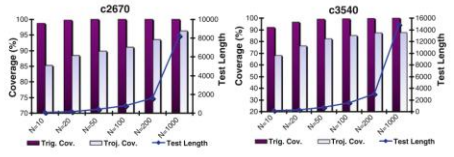


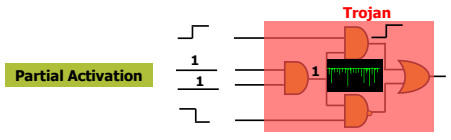
Fig. 15.6 Trigger coverage and Trojan coverage and test length for two ISCAS-85 benchmark circuits for different values of “N,” using the MERO approach [8]

Side-Channel Analysis-Based Approaches

- All the side-channel analysis are based on observing the effect of an inserted Trojan on a physical parameter such as
  - IDDQ: Extra gates will consume leakage power.
  - IDDT: Extra switching activities will consume more dynamic power.
  - Path delay: additional gates and capacitance will increase path delay.
  - EM: Electromagnetic radiation due to switching activity
- Pros & Cons
  - Pros: It is effective for Trojan which does not cause observable malfunction in the circuits.
  - Con: Large process variations in modern nanometer technologies and measurement noise can mask the effect of the Trojan circuits, especially for small Trojan.

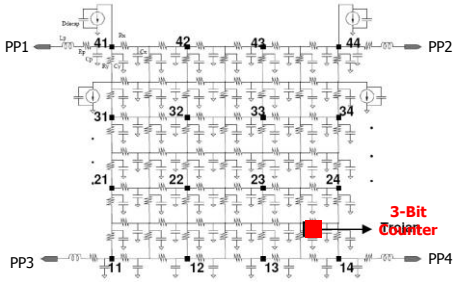
Side Channel Signal Analysis -- Power

- Hardware Trojans inserted in chip can change the power consumption characteristics.
- Partial activation of Trojan can be extremely valuable for power analysis.
- The more number of cells in Trojan is activated the more the Trojan will draw current from power grid.



37

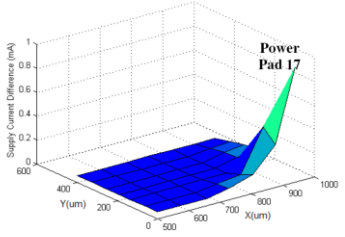
Trojan Inserted into s38417 Benchmark



PP: Power Pad

38

Power Analysis -- Locality



Current difference measured from power pad 17 (Trojan-free vs Trojan-inserted)

There is no change in layout of the circuit. Trojan was inserted in an unused space in the circuit layout.

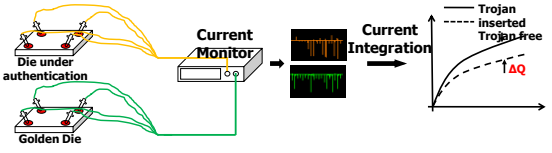
39

Current (Charge) Integration Method

- Current consumption of Trojan-free and Trojan-inserted circuits

$$Q_{trojan\text{-}free}(t) = \int I_{trojan\_free}(t) \, . \, dt$$

$$Q_{trojan\text{-}inserted}(t) = \int I_{trojan\_inserted}(t) \, . \, dt = \int (I_{trojan\_free}(t) + I_{trojan}(t)) \, . \, dt$$

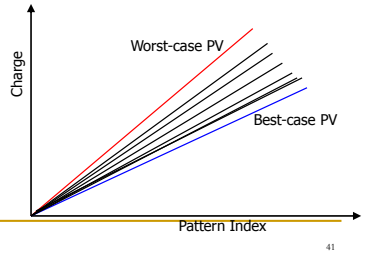


40

Process Variations

- **Worst & Best Cases:**
  - Define lower and upper bounds on current consumption
  - Determine confidence level on Trojan detection

PV:
L: Channel Length)
Vth: Threshold voltage
Tox: Oxide Thickness



41

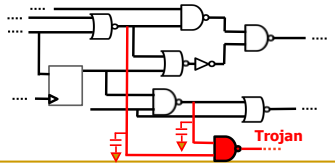
Power Analysis -- Challenges

- **Pattern Generation**
  - How to increase switching activity in Trojans?
  - How to reduce background noise?
  - Switching locality
  - Random Patterns
- **Measurement Device Accuracy**
  - Measurement noise
- **Process Variations**
  - Calibration
- **On-Chip Measurement**
  - Vulnerable to attack
- **Authentication Time**
  - Trojans can be inserted randomly

42

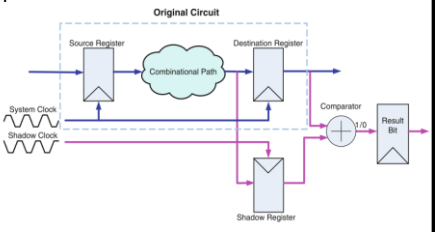
Side Channel Analysis -- Delay

- Hard to be detected using power analysis
  - Distributed Trojans
  - Hard-to-activated Trojans
- Path delay: A change in physical dimension of the wires and transistors can also change path delay.
- We are developing new methods that can detect additional delays on each path of the circuit.



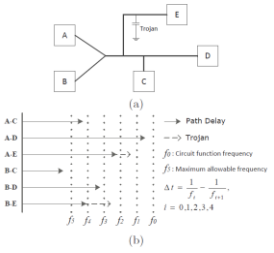
Delay-based Methods

- Shadow-register provides a possible solution for measuring internal path delay.
- From this architecture, it can be seen that the basic unit contains one shadow register, one comparator and one result register.
- Limitations:
  - PV
  - Overhead
  - S-clock
  - Output



Clock Sweeping Technique

- Clock sweeping involves applying a pattern at different clock frequencies, from a lower speed to higher speeds.
- Some paths sensitized by the pattern which are longer than the current period start to fail when the clock speed increases.
- The obtained start-to-fail clock frequency can indicate the delays of the paths sensitized by the patterns



Delay Analysis -- Challenges

- Major advantage over power analysis: No activation is required.
- **Detection and Isolation**
  - How significant is the delay inserted by Trojan?
  - It depends on Trojan size and type
  - Location: on short paths or long paths
- **Pattern Generation**
  - Delay test patterns
  - Path Coverage
- **Process Variations (V_{th}, L, T_{ox})**
  - Impact circuit delay characteristics significantly
  - Differentiate between Trojan and PV
- Trojan can have impact on multiple paths (an advantage over PV)

Trojan Detection

- **Side Channel Signal Analysis**
  - Transient Power (Current) Analysis
    - Fully activation is not necessary
    - A switching at the inputs of a Trojan and inside the Trojan can increase transient power
  - Circuit Delay Analysis
    - Trojan is not needed to be targeted
    - Trojan will impact circuit path delay
    - Target paths rather than Trojans
- **Fully Activation of Trojans**
  - Not applicable to all Trojans (Combinational and Sequential Trojans only)
  - Requires increased controllability and observability
- **Trojan Isolation**
  - Important to know adversary's intention

Trojan Detection

Trojan				Power Analysis	Delay Analysis	Fully Activation
Trojan Classification	Physical Characteristics	Type	Functional	D	P	P
			Parametric	P	D	P
		Size	Small		D	P
			Large	D	P	P
		Distribution	Tight	D	D	P
			Loose	P	D	P
		Structure	Modify Layout	P	D	
	Activation Characteristics	Always-on			D	
		Condition-based	Logic-based	D	P	P
			Sensor-based	D		
	Action Characteristics	Modify Function		D	P	
		Modify Spec.	Defects	P	D	P
			Reliability	P	P	P

P: Detection is possible D: High level of confidence

Design for Hardware Trust

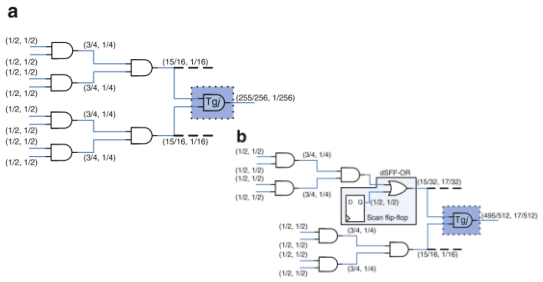
- Since detecting Trojan is extremely challenging, design for hardware trust approaches are proposed to
  - Facilitate hardware Trojan detection methods
    - Improve sensitive to power and delay
    - Rare event removal
  - Prevent hardware Trojan insertion
    - Design obfuscation

Rare Event Removal

- Intelligent attackers will choose low-frequency events to trigger the inserted Trojans.
- Improving controllability or observability can make rare events scarce, thereby facilitating detecting Trojans inside the design.
  - Design for Trojan test: inserting probing points
  - Inserting dummy scan flip-flops

Increasing Probability of Partial/Full Activation

- Inserting dummy FFS on path with very low activation probability



Increasing Probability of Partial/Full Activation

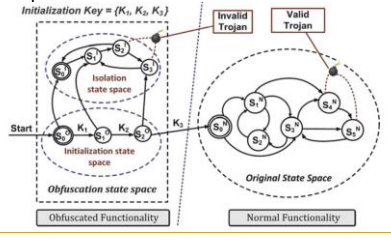
- Dummy scan flip-flops are inserted to control hard-to-excite nodes.
- Usage:
  - Full activation: increase controllability
  - Power-based: generate switching activities
  - Delay-based: activate more paths to improve coverage

Trojan Prevention-Design obfuscation

- The objective is deterring attackers from inserting Trojans inside the design.
- Design obfuscation means that a design will be transformed to another one which is functionally equivalent to the original, but in which it is much harder for attackers to obtain complete understanding of the internal logic, making reverse engineering much more difficult to perform.
- The authors propose a Trojan prevention method that obfuscates the state transition function to add an obfuscated mode on top of the original functionality (called normal mode).

Design obfuscation

- Specified pattern is able to guide the circuit into its normal mode.
- The transition arc K3 is the only way the design can enter normal operation mode from the obfuscated mode.



Question?

55