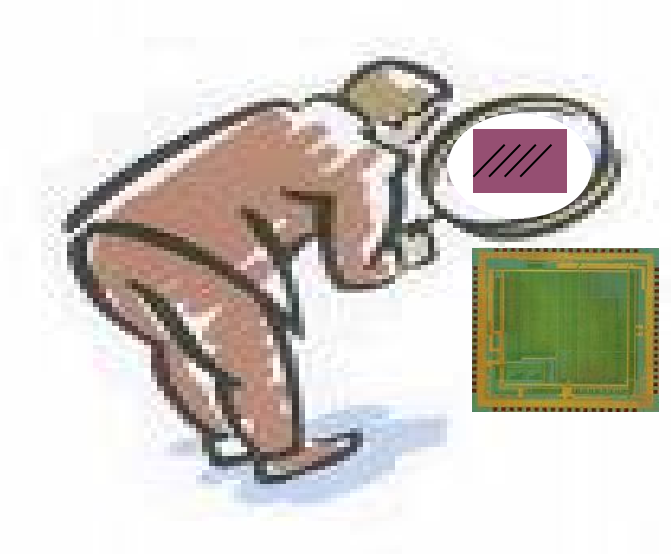
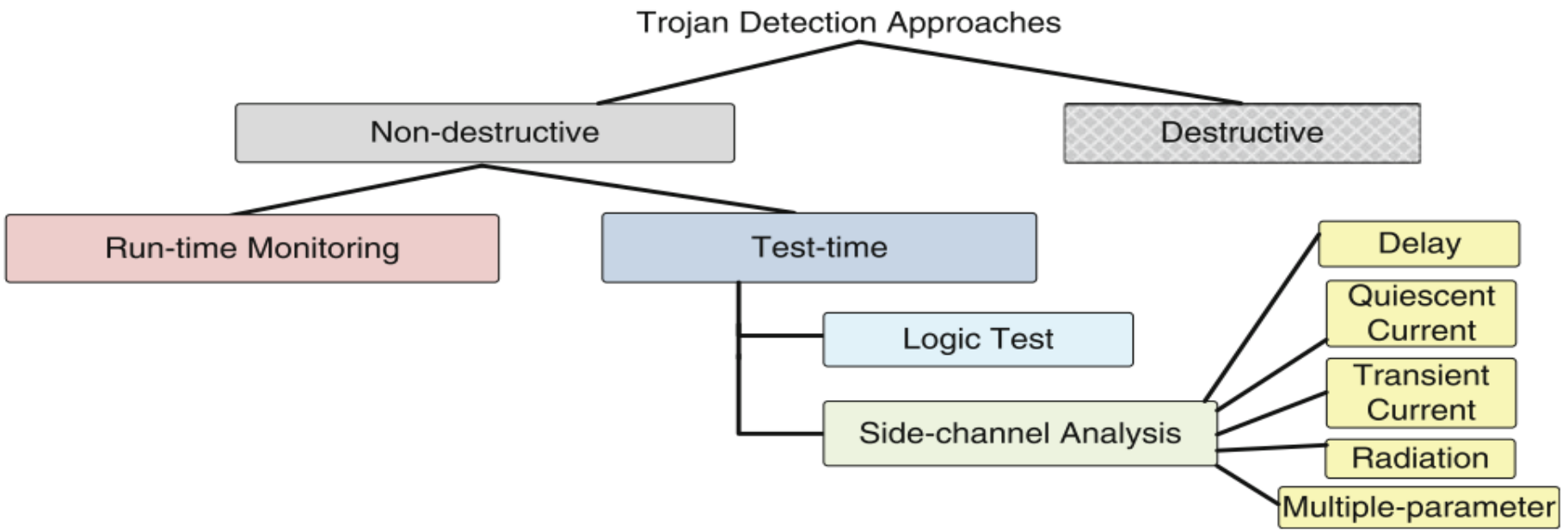
IC (System) Trust

- **Objective**:
  - 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



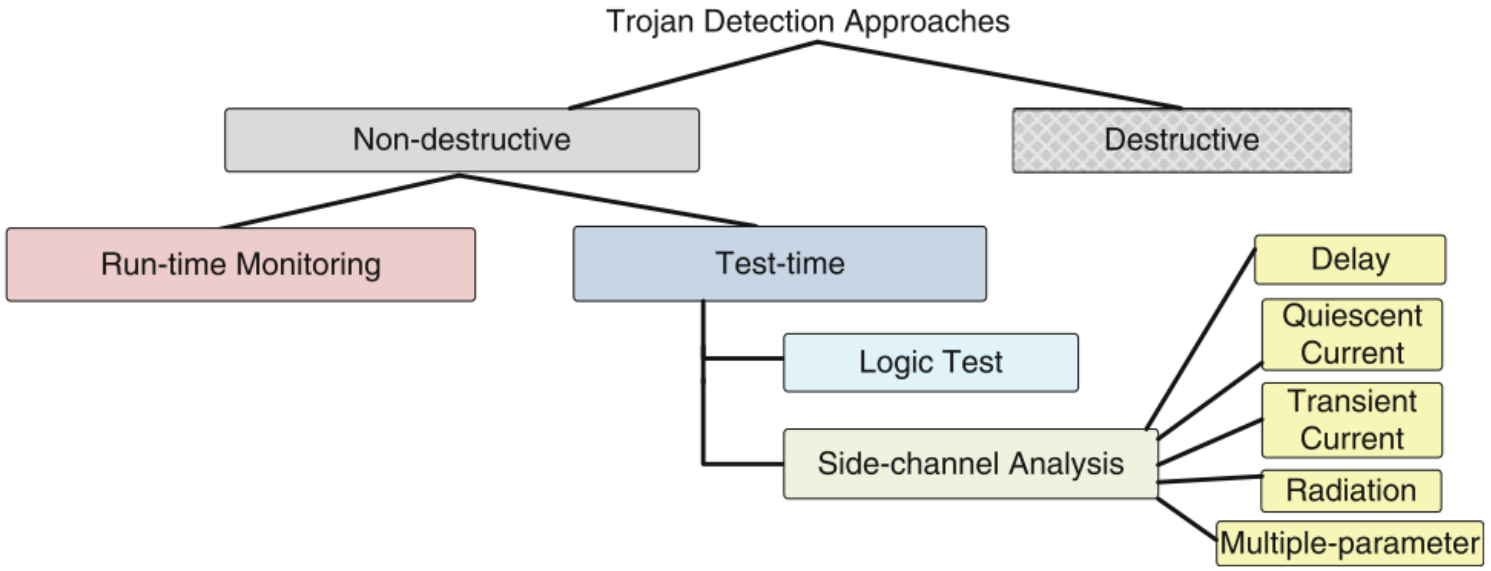
Classification of Trojan Detection Approaches



- **Destructive Approach**: Expensive and time consuming
  - Reverse engineering to extract layer-by-layer images by using delayering and Scanning Electron Microscope
  - Identify transistors, gates and routing elements by using a template-matching approach – **needs golden IC/layout**

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 Authentication**: Detect Trojans throughout test duration.
    - Logic-testing-based approaches
    - Side-channel analysis-based approaches



Hardware Trojan Benchmarks

- A set of **trust benchmarks** for researchers in academia, industry, and government is needed to
  - Provide a baseline for examining diverse methods developed
  - Establishing a sound basis for the hardness of each benchmark instance
  - Help increase reproducibility of results by others who intend to employ certain methodologies in their design flow
- See NSF supported **Trust-Hub** website (www.trust-hub.org)
  - Complete taxonomy of Trojans
  - More than 120 trust benchmarks available which were designed at different abstraction levels, triggered in several ways, and have different effect mechanisms
  - More than 300 publications used these benchmarks

Logic Testing Approach

- **Logic-testing approach** focuses 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, but certainly 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.

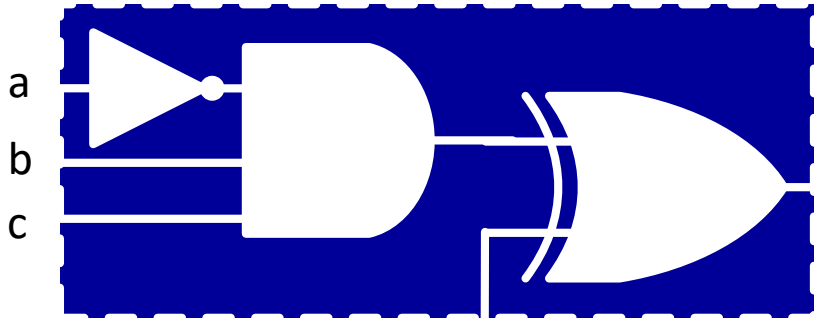
Functional Testing

Feasible Trojan space inordinately large!

Deterministic test generation infeasible

A statistical approach is, more effective

- **MERO: Multiple Excitation of Rare Occurrence: A Statistical Approach**
  - Find the rare events in the circuit
  - Generate vectors to trigger each rare node ***N times***
  - Provides high confidence in detecting unknown Trojans!



From original circuit

Trojan Trigger Condition

a=0, b=1, c=1

MERO

- **MERO**:
  - Generates 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
  - One-time trigger cannot ensure the Trojan will be activated.
  - Proposed to increase the test coverage.
  - It is still effective for sequential Trojans.
  - The Trojan detection coverage increases for higher values of “N”, at the cost of increased test length.

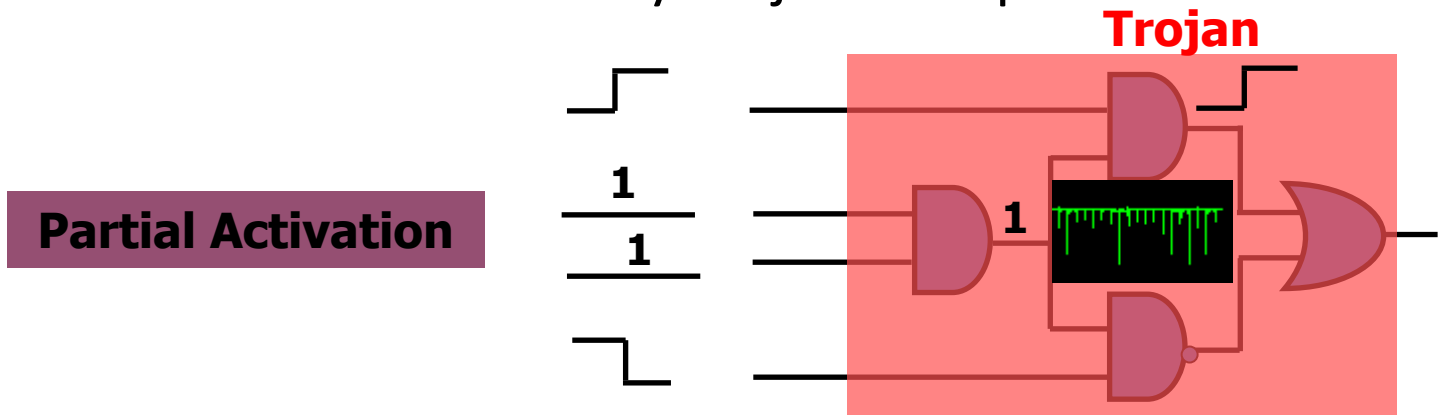
- **Challenge:** Triggering each net N times in a large circuit is challenging

Side-Channel Trojan Detection

- Side-Channel Approach for Trojan Detection relies on observing Trojan effect in physical side-channel parameter, such as switching current, leakage current, path delay, electromagnetic (EM) emission
- Due to process variations, it is extremely challenging to detect the Trojan by considering F_{max} or I_{DDT} (the transient current from the power supply) individually.

Side Channel Signal Analysis -- Power

- Hardware Trojans inserted in a 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.
- An example of IDDT (transient current) Trojan detection method is presented.
- Extra transient current is induced by Trojan with partial activation.



Golden chip required!

Side-channel Signals

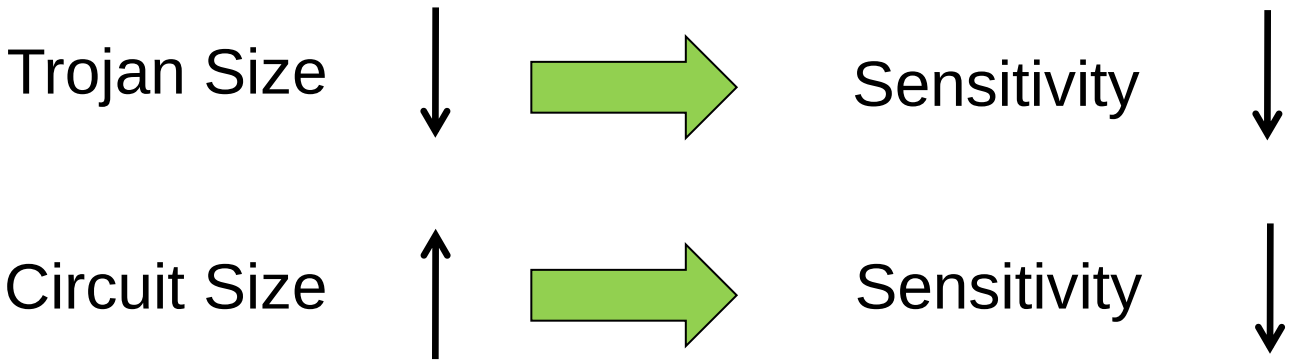
- All the side-channel analyses are based on observing the effect of an inserted Trojan on a physical parameter such as
  - **IDDQ**: Extra gates will consume leakage power.
  - **IDDT**: Extra switching activities will consume more dynamic power.
  - **Path Delay**: Additional gates and capacitance 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.
  - **Cons**: Large process variations in modern nanometer technologies and measurement noise can mask the effect of the Trojan circuits, especially for small Trojan.

Golden chip required!

Sensitivity Metric

- **Improving Detection Sensitivity**



$$Sensitivity = \frac{I_{tampered} - I_{original}}{I_{original}} \times 100\%$$

Comparing Approaches

	Logic Testing	Side-Channel Analysis
Pros	● Robust under process noise ● Effective for ultra-small Trojans	● Effective for large Trojans ● Easy to generate test vectors
Cons	● Difficult to generate test vectors ● Large Trojan detection challenging	● Vulnerable to process noise ● Ultra-small Trojan Det. challenging

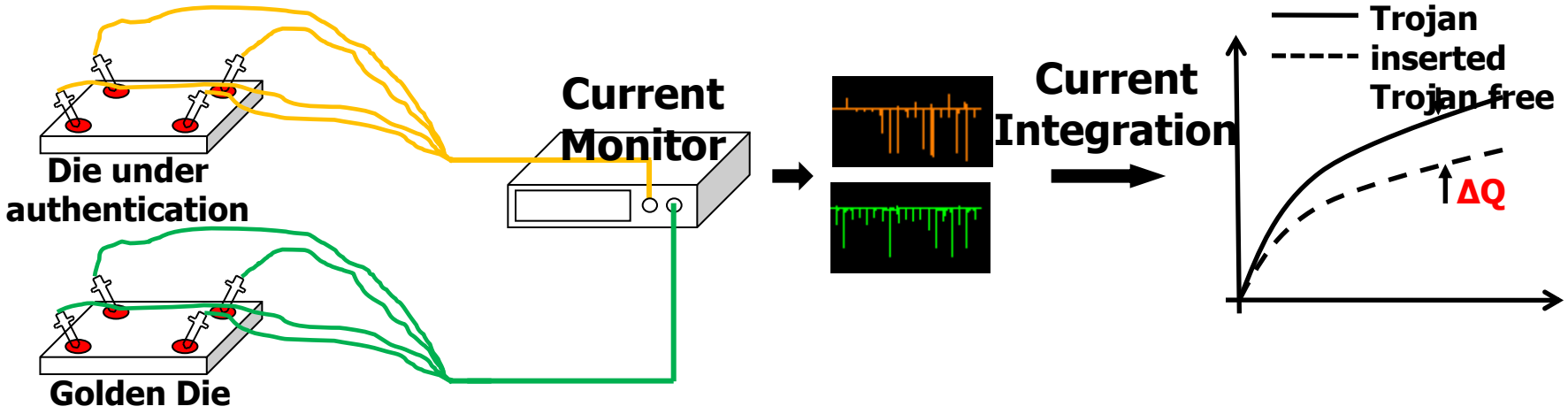
- **A combination of logic testing & side-channel analysis could provide the good coverage!**
- **Online validation approaches can potentially provide a second layer of defense!**

Current (Charge) Integration Method

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

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

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

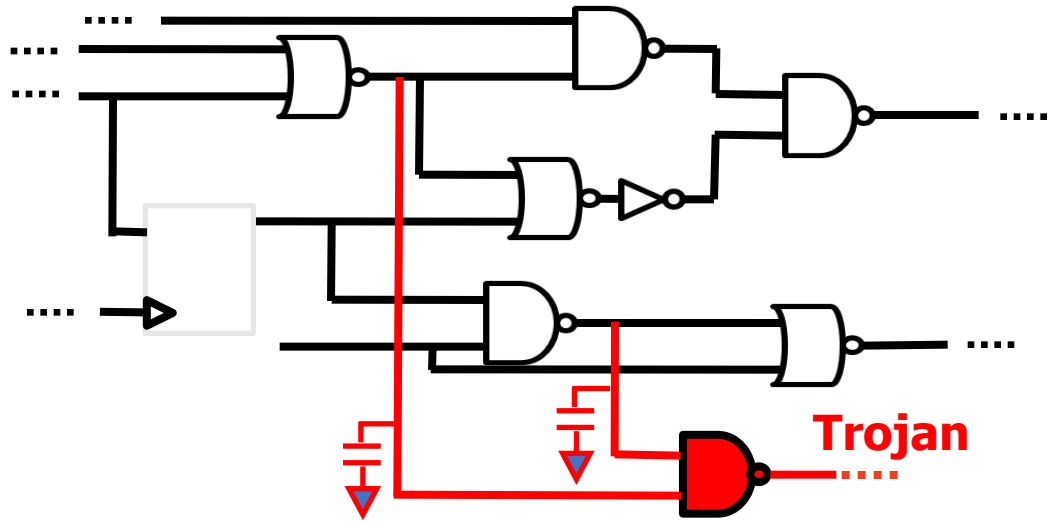


Power Analysis -- Challenges

- **Pattern Generation**
  - How to increase switching activity in Trojans?
  - How to reduce background noise?
  - Switching locality
  - Random Patterns
    - No observation is necessary , Similar to test-per-clock
- **Measurement Device Accuracy**
  - Measurement noise
- **Process Variations**
  - Calibration
- **On-Chip Measurement**
  - Vulnerable to attack
- **Authentication Time**
  - Trojans can be inserted randomly

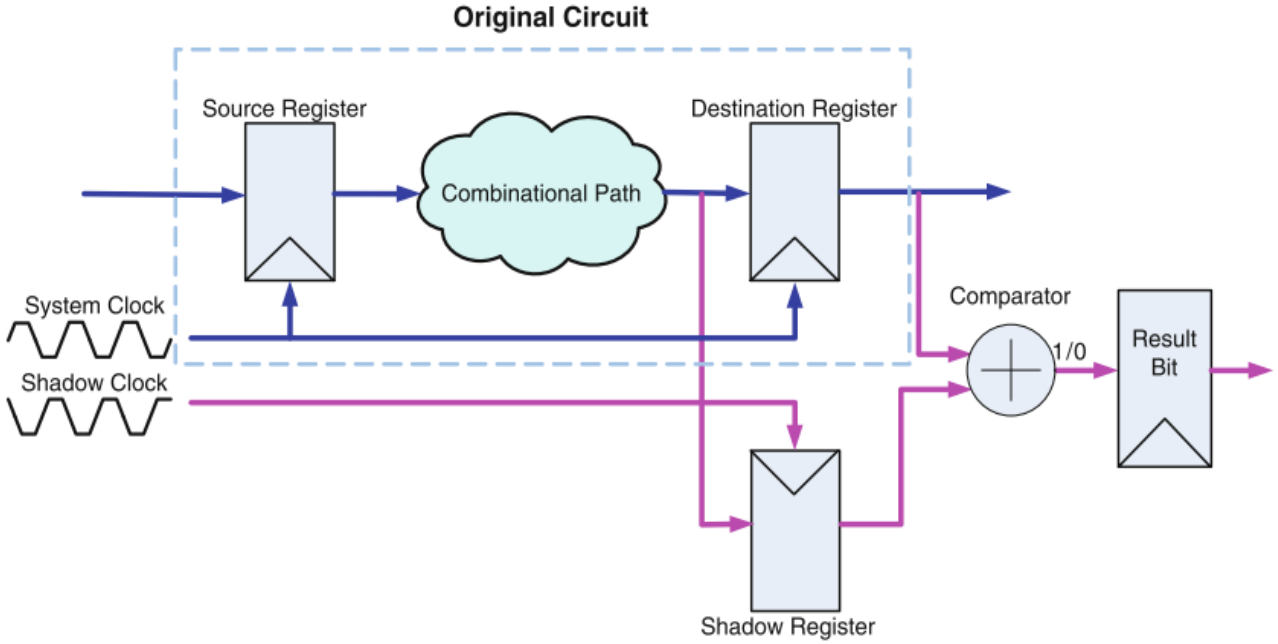
Side Channel Analysis -- Delay

- Hard to detect using power analysis are:
  - Distributed Trojans
  - Hard-to-activate Trojans
- **Path delay**: A change in physical dimension of the wires and transistors can also change path delay.
- Some methods can detect additional delays on each path of the circuit.



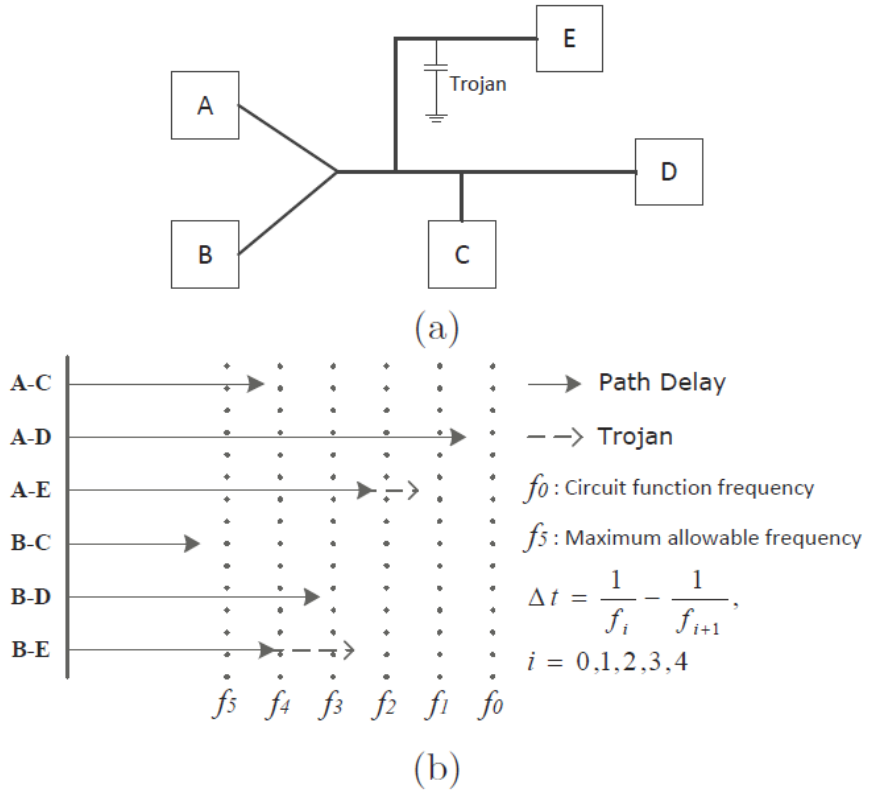
Delay-based Methods

- 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.
- Shadow registers are used here to measure internal delays
- **Limitations**:
  - Process Variation
  - 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)**

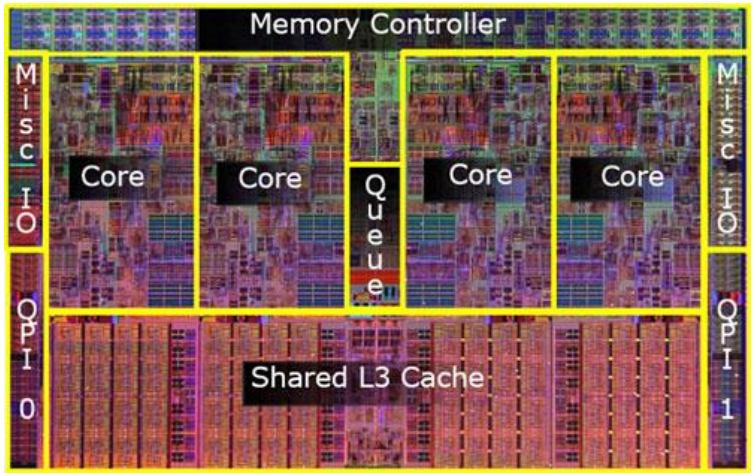
Trojan Detection

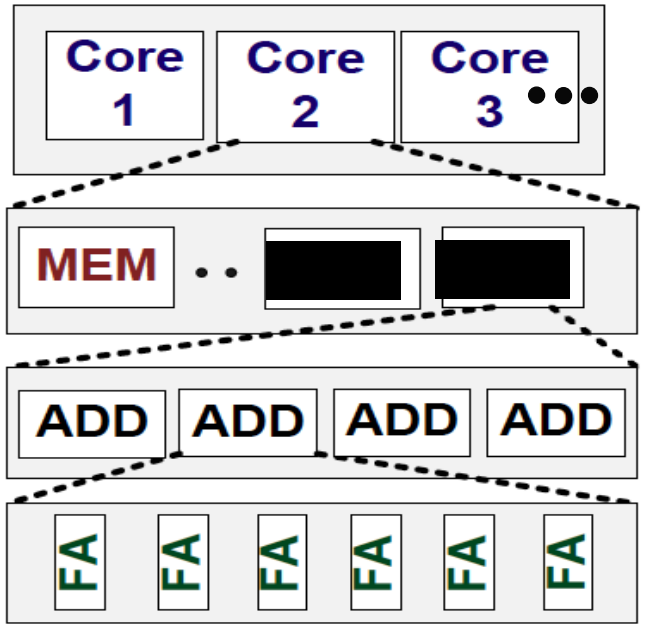
Trojan				Power Analysis	Delay Analysis	Fully Activation
Trojan Classification	**Physical Characteristics**	Type	Functional	D	P	P
			Parametric	P	D	P
		Size	Small		D	P
			Large	D	P	P
		Distribution	Tight	D	D	P
			Loose	P	D	P
		Structure	Modify Layout	P	D	
	Activation Characteristics	Always-on			D	
		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

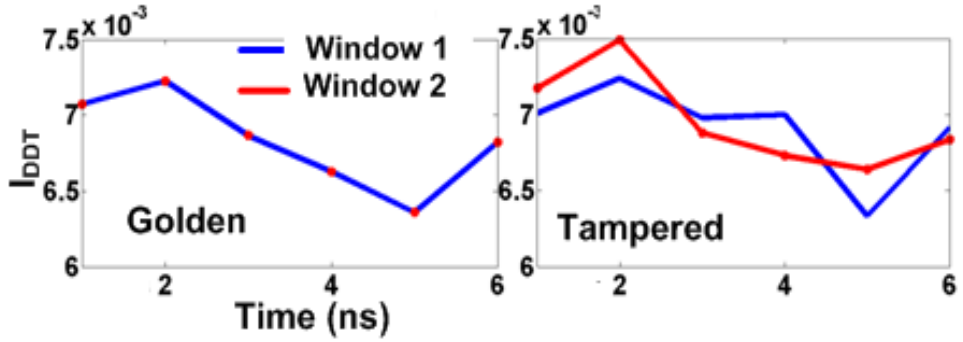
P: Detection is possible **D: High level of confidence**

Self-similarity in Space & Time – for Trust Verification

Image courtesy: Intel







Uncorrelated switching in time due to a seq. Trojan!

Simultaneously detects Trojan & aged/recycled ICs!

No golden chip required!!!