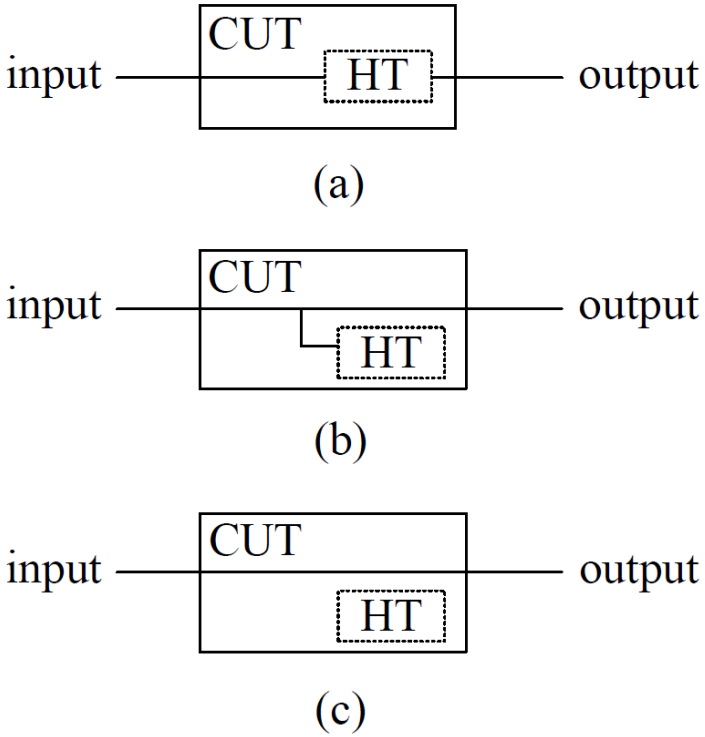
HT Detection Challenge

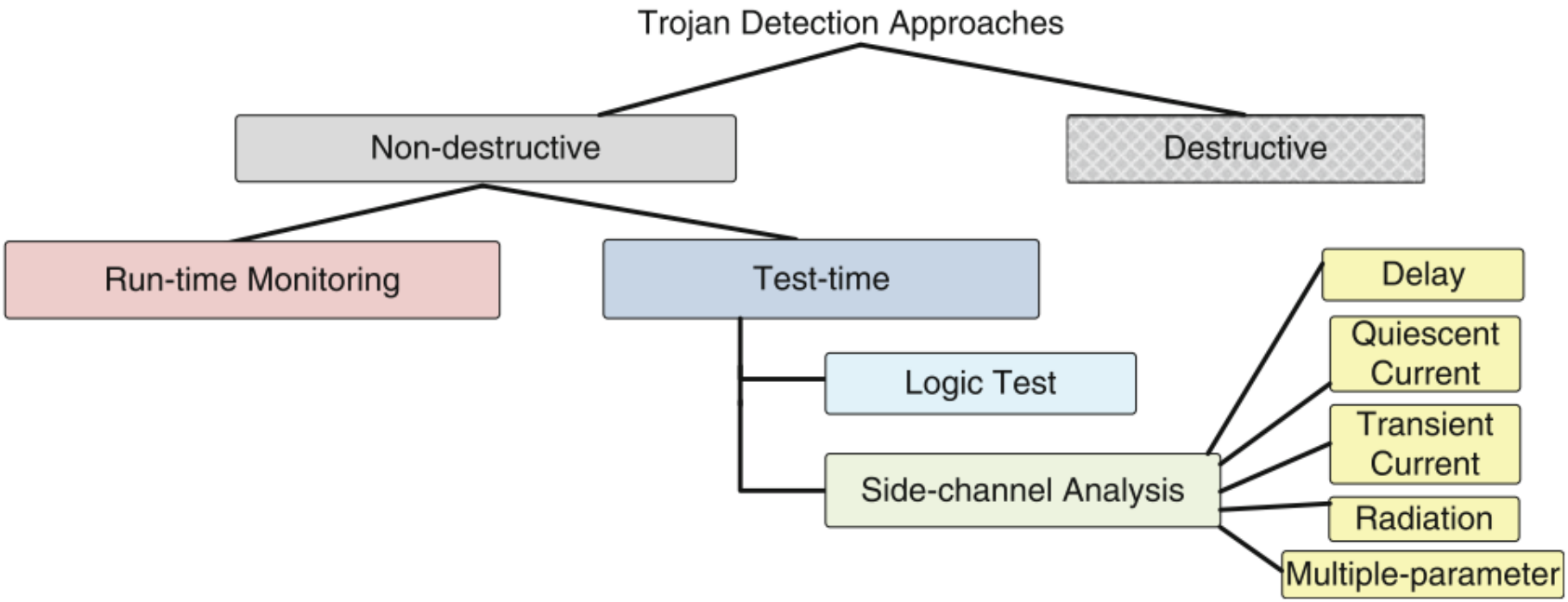
- HT size is tiny compared to host-circuit. The parametric effect caused by HT can be easily covered by noise and operating variations.
- HT is designed to be dormant at most of the time to evade detection.

HT Location



HT Location in CUT, (a) In-Path, (b) By-Path, (c) Off-Path

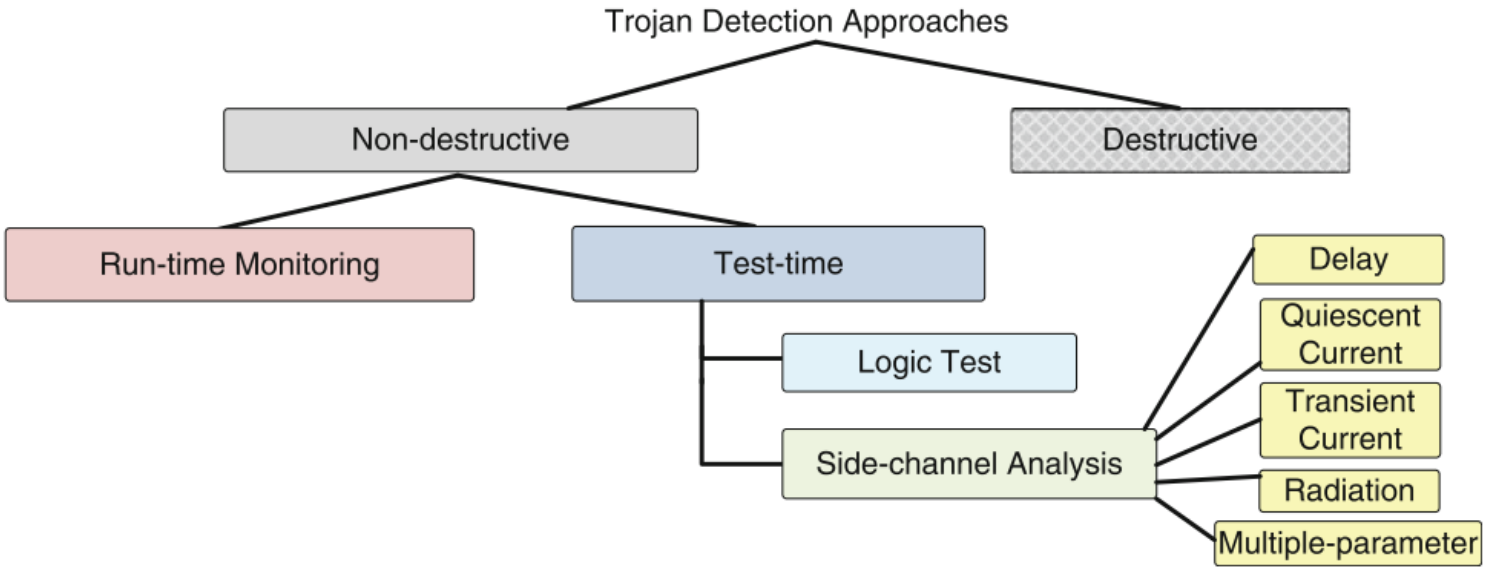
Classification of Trojan Detection Approaches



- **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 not transmitting information by antenna.

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.

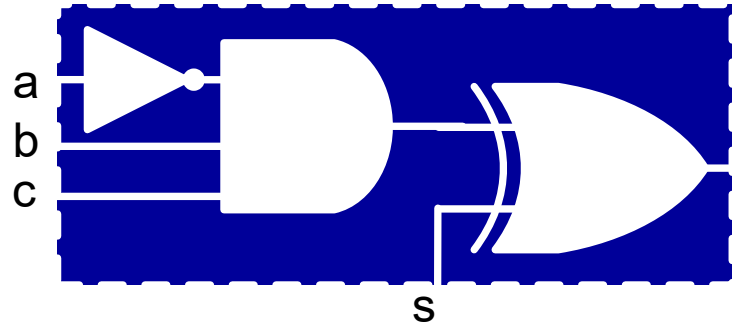
Functional Testing

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

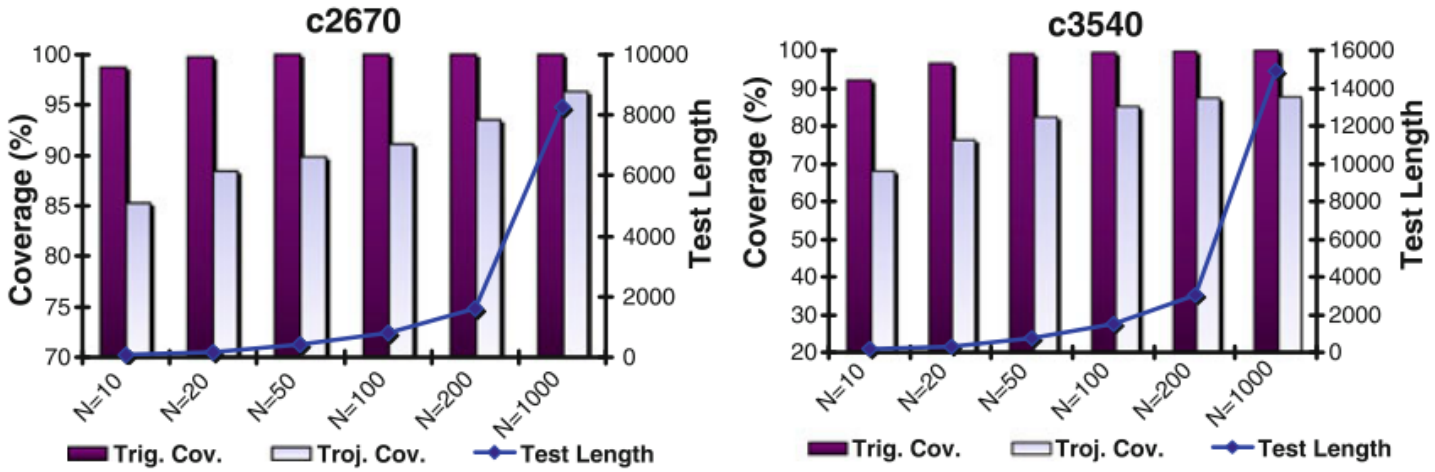


Fig. 15.6 Trigger coverage and Trojan coverage and test length for two ISCAS-85 benchmark circuits for different values of "N," using the MERO approach [8]

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

Side-channel Signals

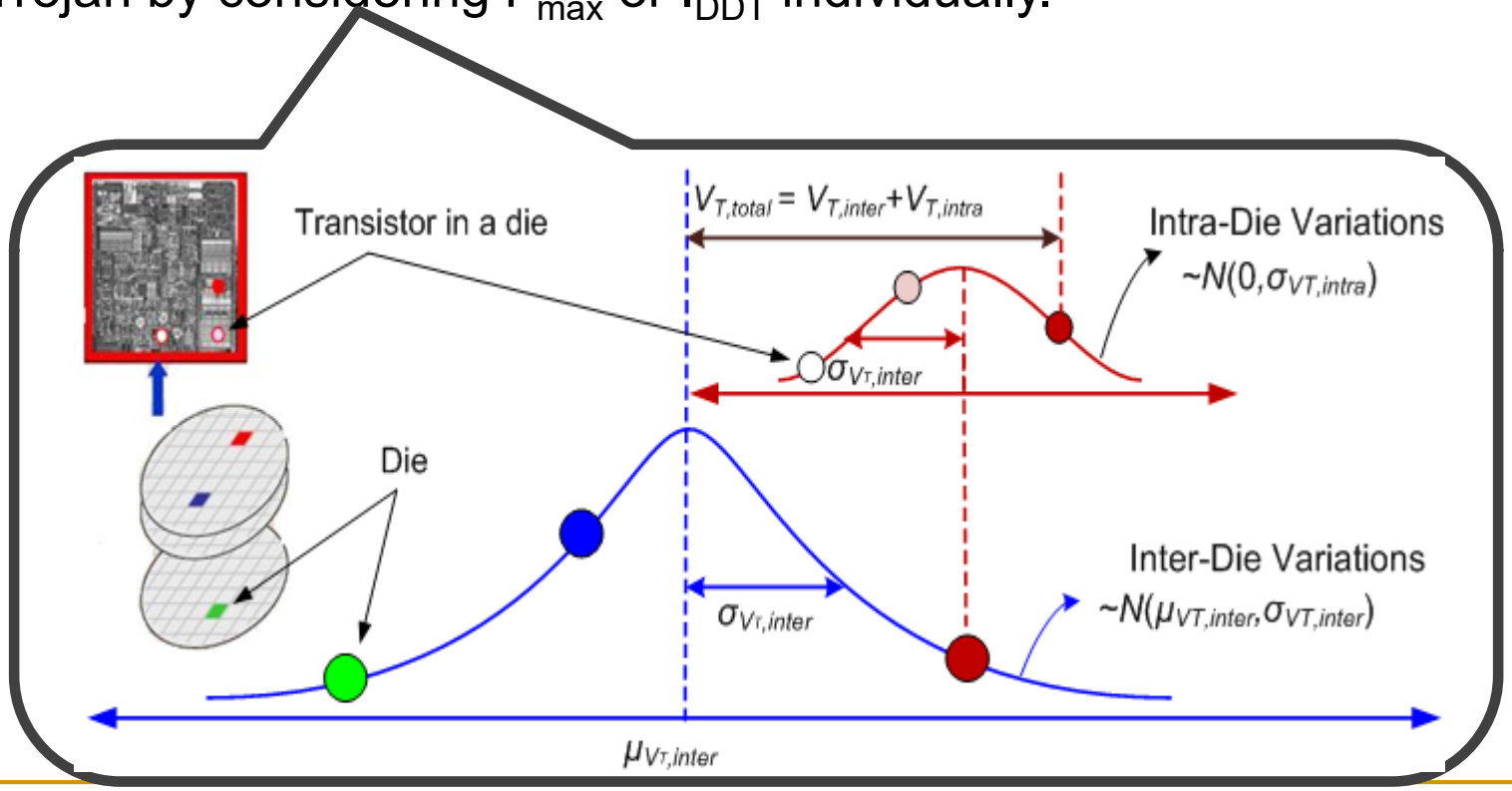
- All the side-channel analyses are based on observing the effect of an inserted Trojan on a physical parameter such as
  - **IDDQ**: Extra gates will consume leakage power.
  - **IDDT**: Extra switching activities will consume more dynamic power.
  - **Path Delay**: Additional gates and capacitance 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!

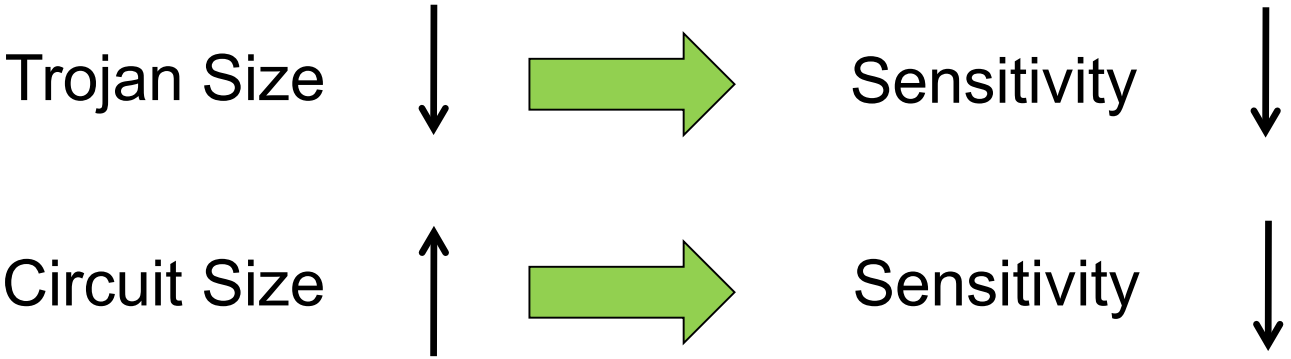
Side-Channel Trojan Detection Challenge

- **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} individually.



Sensitivity Metric

- **Improving Detection Sensitivity**

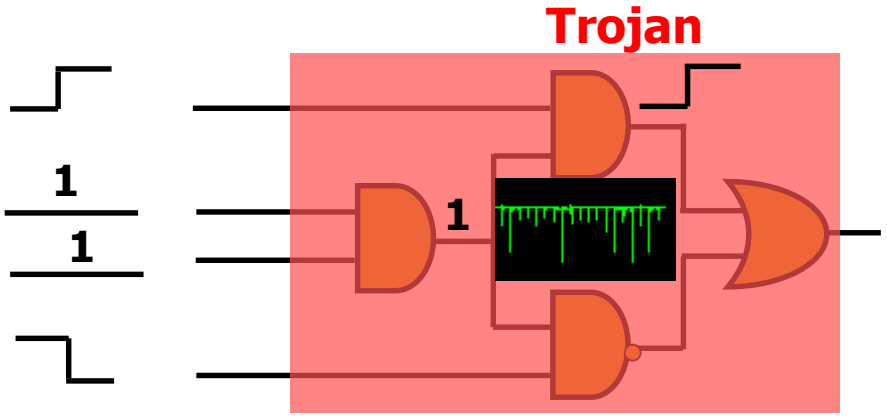


$$Sensitivity = \frac{I_{tampered} - I_{original}}{I_{original}} \times 100\%$$

Side Channel Signal Analysis --Dynamic 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.

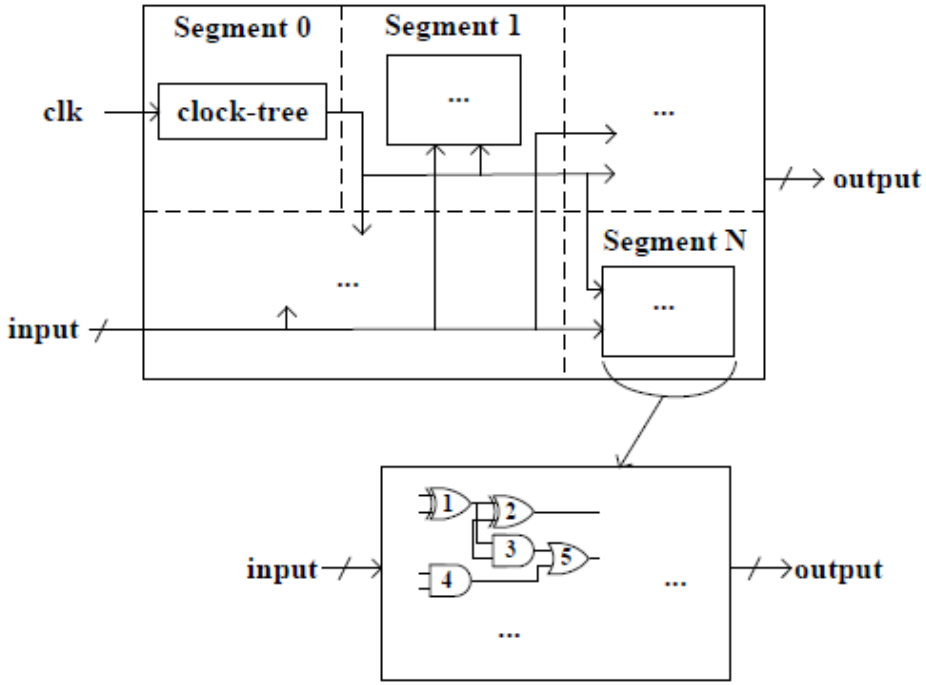
Partial Activation



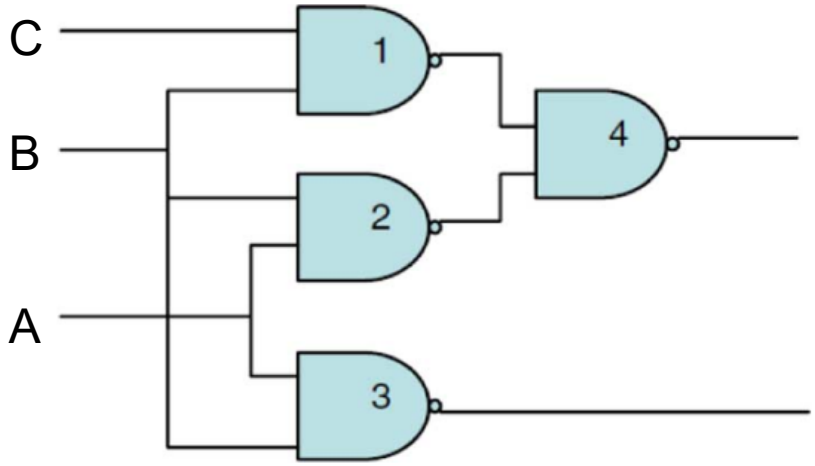
Golden chip required!

Self-reference-based HT Detection—Static Power

- A CUT is partitioned into N segments
- All partitioned segments in the CUT must be controllable by primary inputs.
- Each segment uses a separate power rail.
- To measure one segment static power, the voltage supply is applied to this segment along with the clock-tree rail, while leaving the other power rails float.



Static Power Matric for Gates



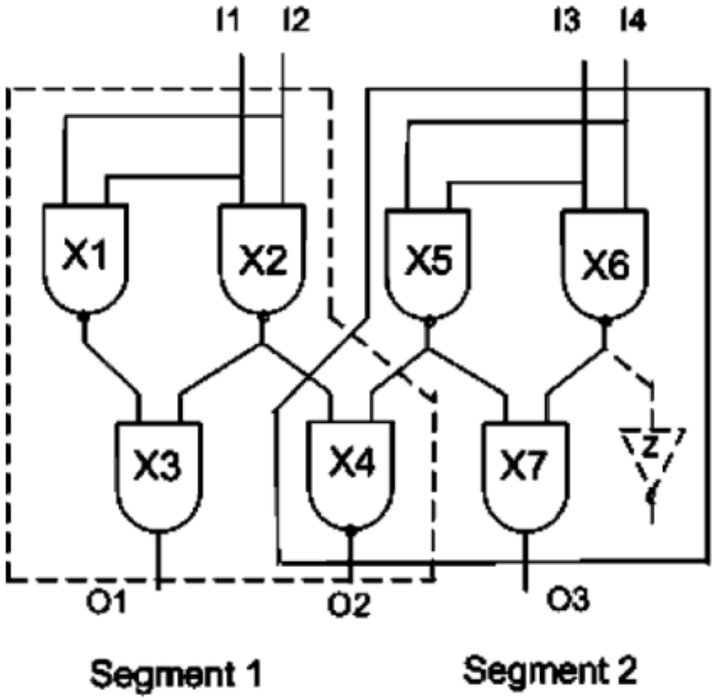
ABC

Input Vector	Gate 1	Gate 2	Gate 3	Gate 4
000	37.84	37.84	37.84	454.5
001	100.3	37.84	37.84	454.5
010	95.17	100.3	100.3	454.5
011	454.5	100.3	100.3	95.17
100	37.84	95.17	95.17	454.5
101	100.3	95.17	95.17	454.5
110	95.17	454.5	454.5	100.3
111	454.5	454.5	454.5	37.84

$$P_{static} = \sum_{i=1}^{4} \lambda_i p_i$$

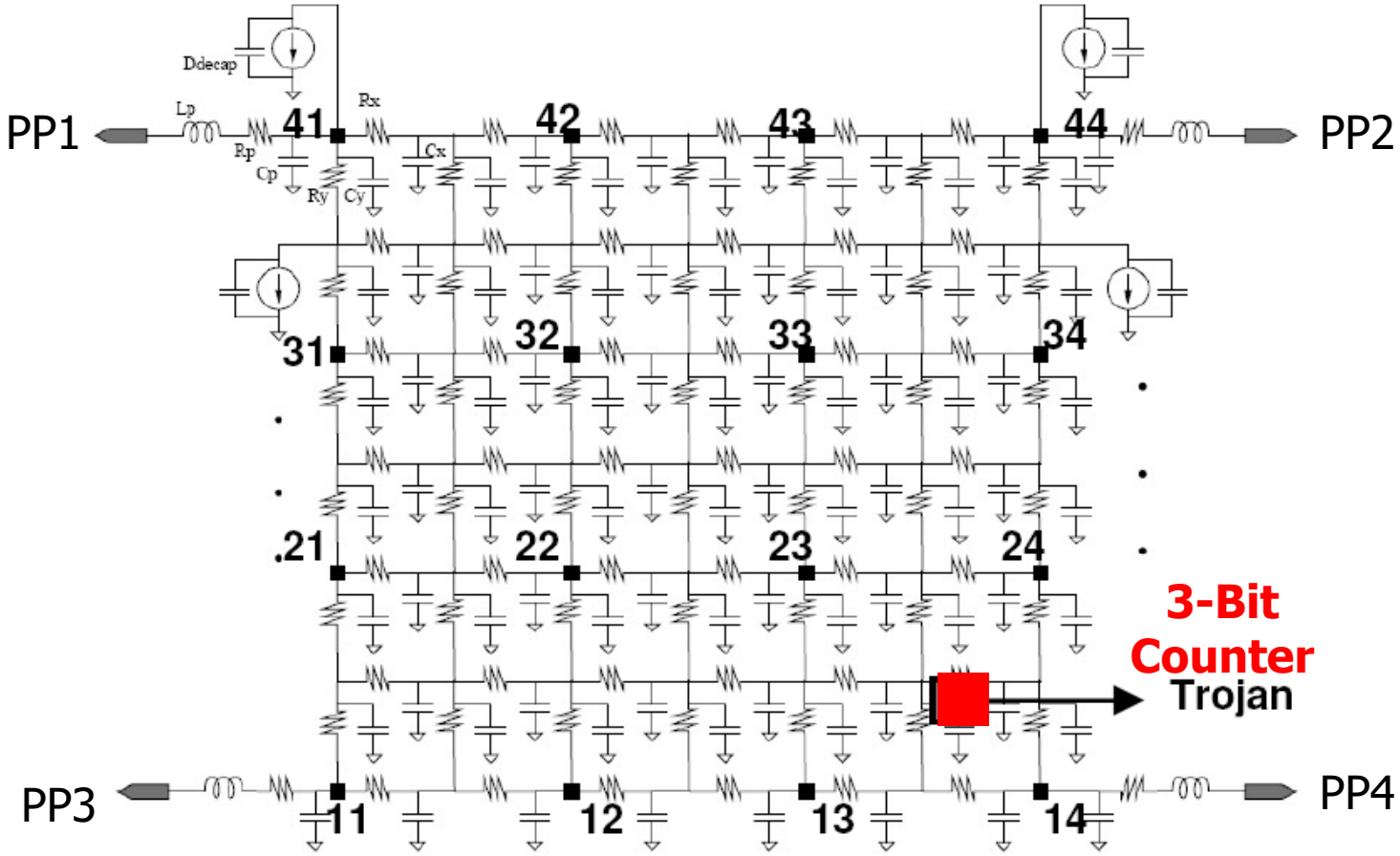
λ, PVT variation scaling factor

Example



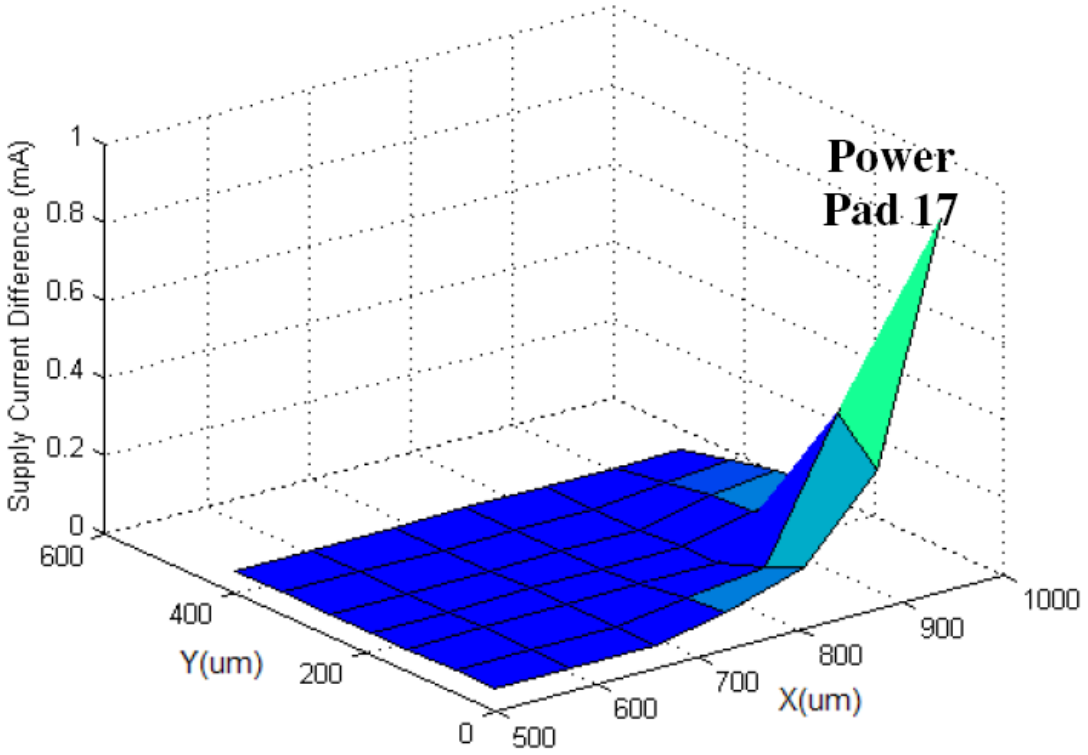
- Use $P_{static} = \sum_{i=1}^{4} \lambda_i p_i$ to find λ_{x4} in segment 1 & 2.
- HT increases λ of components in the same segment.

Trojan Inserted into s38417 Benchmark



PP: Power Pad

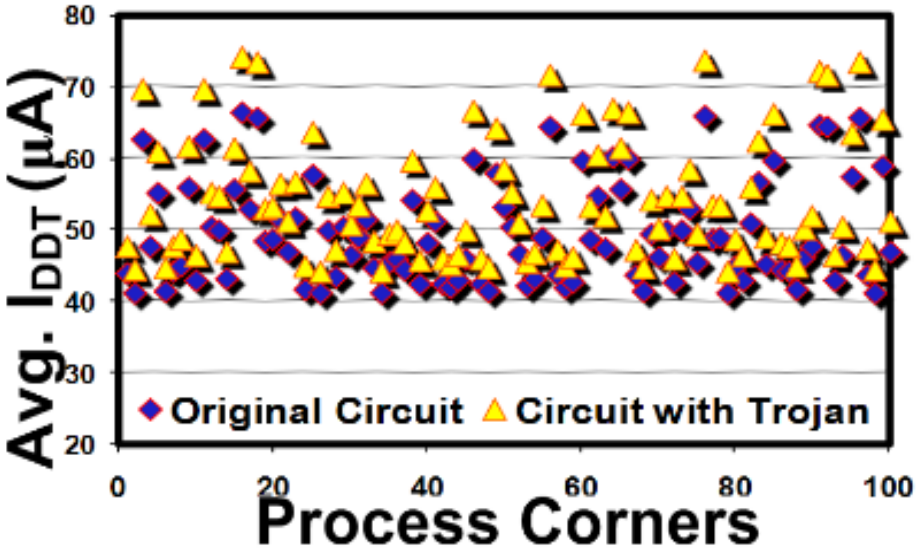
Power Analysis -- Locality

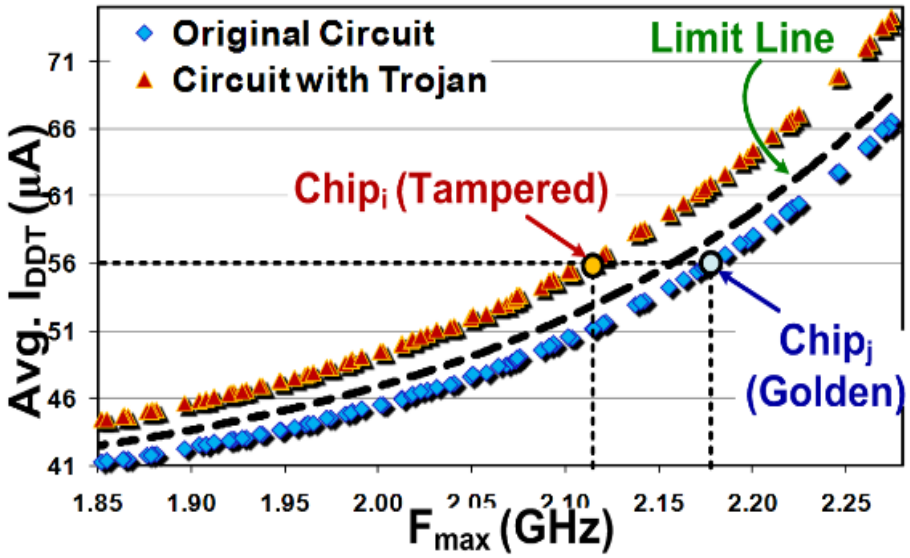


- **Current difference measured from power pad 17 (Trojan-free vs Trojan-inserted)**
- **There is no change in layout of the circuit. Trojan was inserted in an unused space in the circuit layout.**

Side-channel Approach

- *Multiple-parameter Trojan Detection*
  - Due to process variations, Trojan detection by F_{max} or I_{DDT} alone is challenging!





- Consider the intrinsic relationship between I_{DDT} and F_{max}

Golden chip required!

Power Analysis -- Challenges

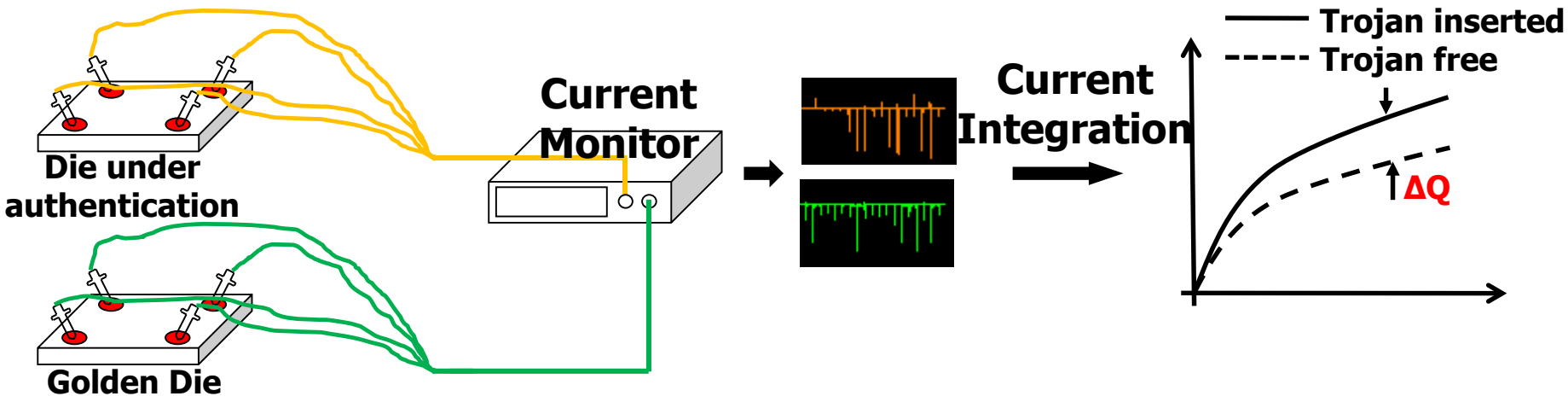
- **Pattern Generation**
  - How to increase switching activity in Trojans?
  - How to reduce background noise?
  - Switching locality
  - Random Patterns
    - No observation is necessary , Similar to test-per-clock
- **Measurement Device Accuracy**
  - Measurement noise
- **Process Variations**
  -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

Current (Charge) Integration Method

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

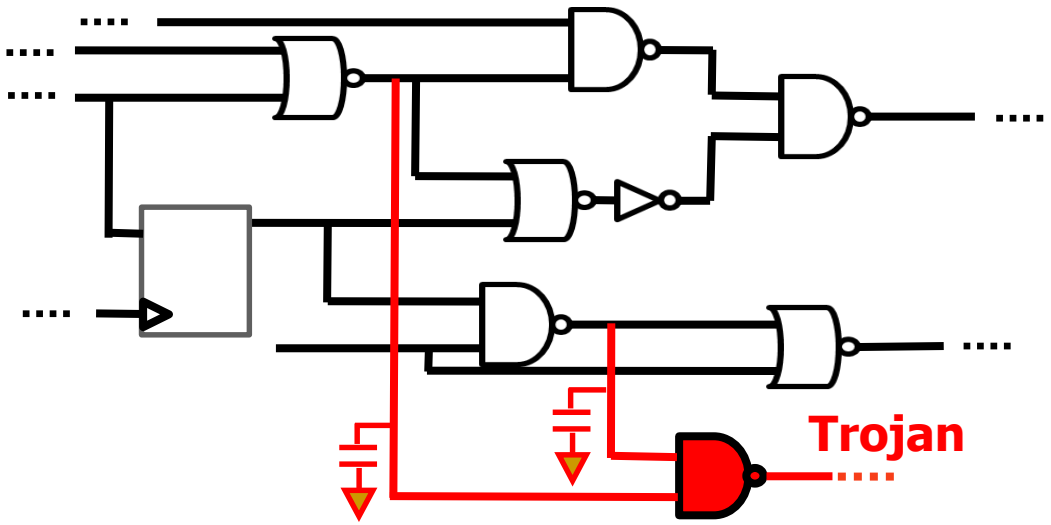
$$Q_{trojan\text{-}free}(t) = \int I_{trojan\_free}(t) \; . \; dt$$

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



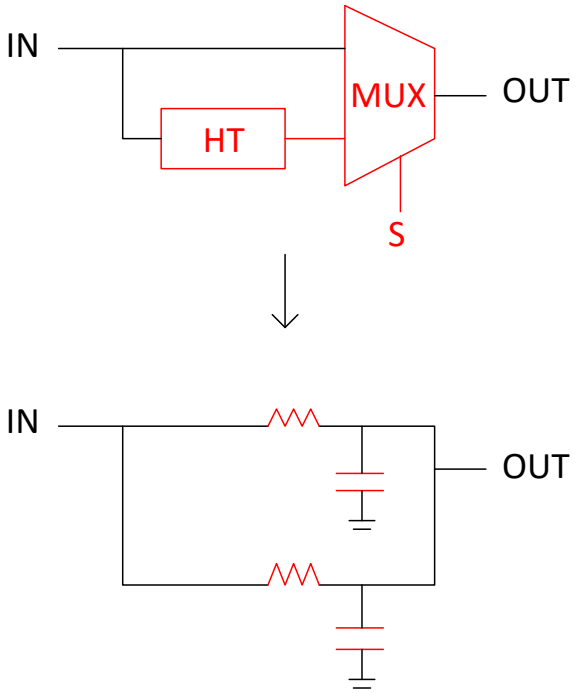
Side Channel Analysis -- Delay

- 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.
- Developing new methods that can detect additional delays on each path of the circuit.



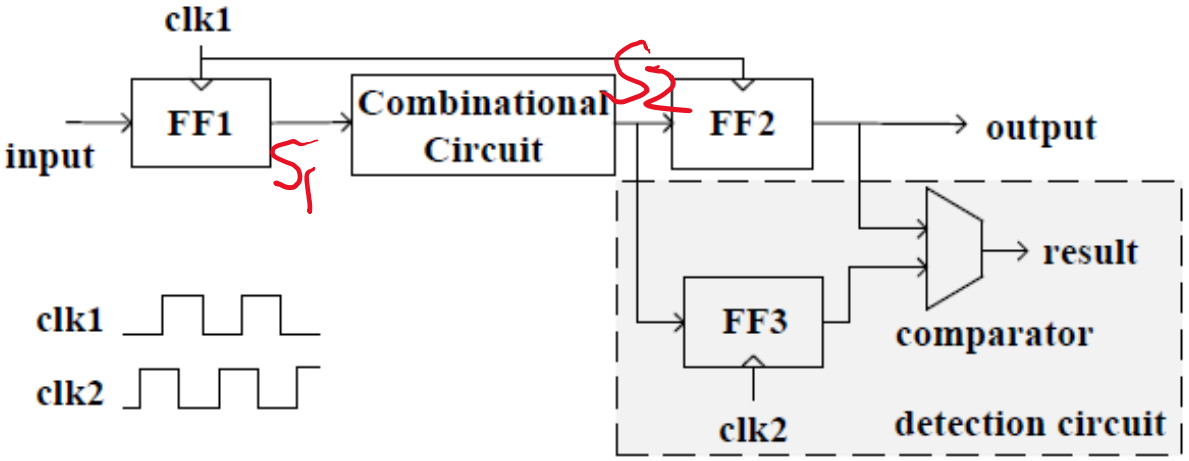
Timing analysis-based HT detection

- Embedded HT will add extra capacitance, resulting in more charging and discharging delays to HT affected paths. HT can be revealed by measuring the differential timing characteristics of the attacked circuit.



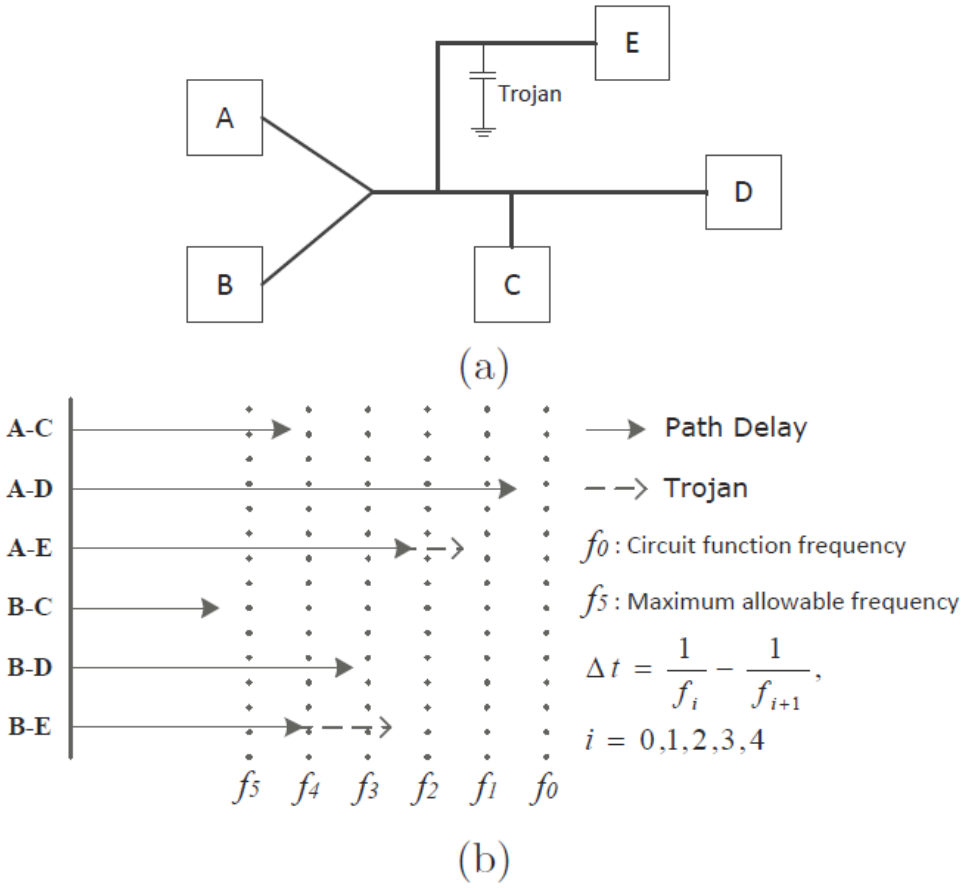
Delay-based Methods—Shadow Register (FFT3)

- Detect HT in register-to-register paths
- The registers (*FF1*, *FF2*) in *main circuit* are triggered by the main system clock (*clk1*)
- *FF3* is triggered by a shadow clock (*clk2*), which has the same frequency with *clk1* and a controlled negative phase shift
- The negative shift of shadow clock makes *FF3* to be triggered earlier than *FF2*, thereby output of *combinational circuit* arrives *comparator* through *FF3* ahead of it through *FF2*
- Then the shadow clock negative shift is increased until the register outputs are unequal. That clock shift time is claimed to be the *combinational circuit* delay. The *combinational circuit* is suspicious of being HT-attacked if the measured delay is substantially different from the pre-determined designed timing.
- **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



References

- [8] Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou and Swarup Bhunia, “MERO: A Statistical Approach for Hardware Trojan Detection”. 57470397.pdf (iacr.org)