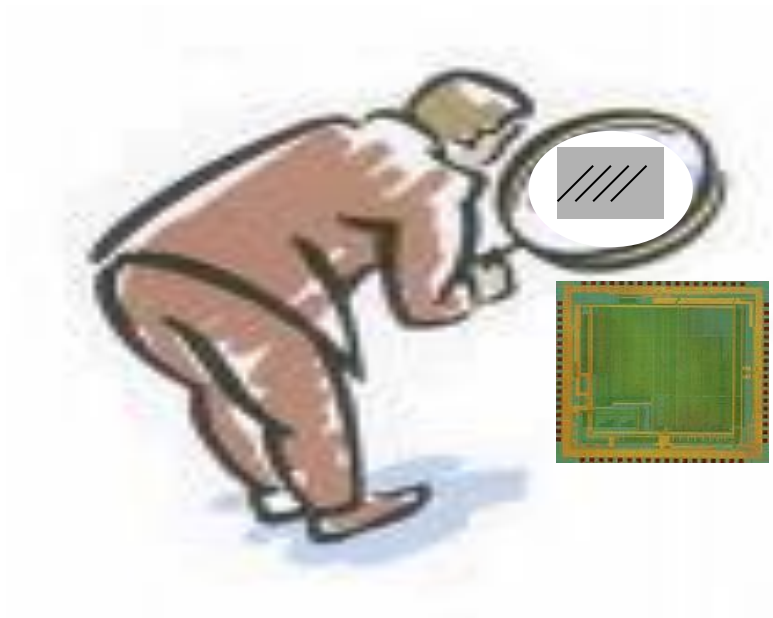
Hardware Trojan Detection

IC Authentication: Trojan Detection and Isolation

- **The objective is to ensure that the designed chip/system will carry out only our desired function and nothing more**

It requires a good understanding of:

- **Pattern generation**
- **chip/system design process**
- **physical layout**
- **side-channel analysis**
- **hardware security**
- **Verification**
- **Etc.**



ATPGs Deficiency

Automatic Test Pattern Generator (ATPG)

- **Functional patterns could potentially detect a "functional" Trojan**
  - **Exhaustive test would be effective**
  - **Not applicable for large circuits**
  - **64 input adder → 2^{65} input combination (including carry in)**
    - **$2^{65} > 10^{18}$ – This is impractical**
    - **Over 100 years at 10GHz**
  - **Only a few and more effective patterns are used → Trojans can escape.**
  - **The fault coverage is low for manufacturing test**

- **In practice, structural tests are used.**

ATPGs Deficiency

Automatic Test Pattern Generator (ATPG)

- **Structural tests cannot verify functionality of a circuit**
  - **Trojan is not a defect until is being activated.**
- **Fault Models:**
  - **Stuck-at Fault**
  - **Bridging Fault**
  - **Timing Delay Fault (TDF)**
- **Cannot provide 100% fault coverage**
- **A Trojan can have impact on circuit delay → Gross or small delay**
  - ATPGs are not capable of addressing it well enough

ATPGs Deficiency

- **ATPGs provide a list of:**
  - ***hard-to-detect*** **fault sites**
  - ***hard-to-activate*** **paths**
  - ***Untestable faults***
- **An adversary can take advantage of such locations in the circuit to ensure that Trojans won't be detected during manufacturing tests**

- **According the taxonomy, there are many types of Trojans that are not functional and cannot be activated using test patterns.**

Key Definitions

- Full Activation: The process in which a triggered Trojan launches its malicious function.

- Partial Activation: The process in which some gates, often at the earlier stages, switch.
  - "activity" will refer to partial activation in this class.

Detection Schemes

- Activation Techniques
  - Attempt to fully activate Trojans
  - Improve the likelihood of partial activity
    - Use in conjunction with side-channel techniques
- Side Channel Techniques
  - Monitor a circuit's side-channel parameters to determine abnormalities
- Design for Trust
  - Modify design process to make Trojan-insertion difficult
- Reverse Engineering (Non-destructive)
  - Thoroughly examine the physical manifestation of the circuit

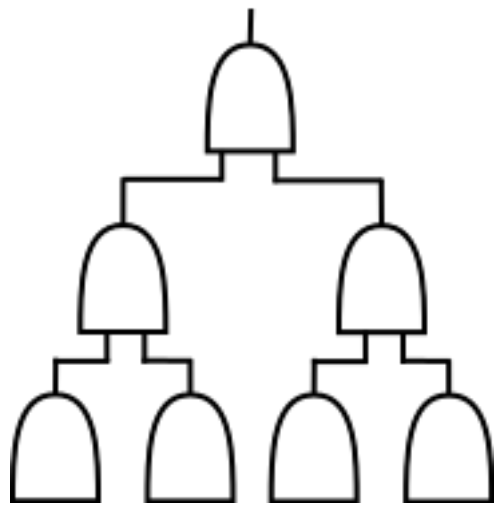
Trojan Detection

- **Side Channel Signal Analysis**
  - **Transient Power (Current) Analysis**
    - **Full activation is not necessary**
    - **Switching at the inputs of a Trojan and inside the Trojan can increase transient power**
  - **Circuit Delay Analysis**
    - **Trojan does not need to be targeted**
    - **Trojan will impact circuit path delay**
    - **Target paths rather than Trojans**

- **Full Activation of Trojans**
  - **Not applicable to all Trojans (Combinational and Sequential Trojans only)**
  - **Requires increased controllability and observability**

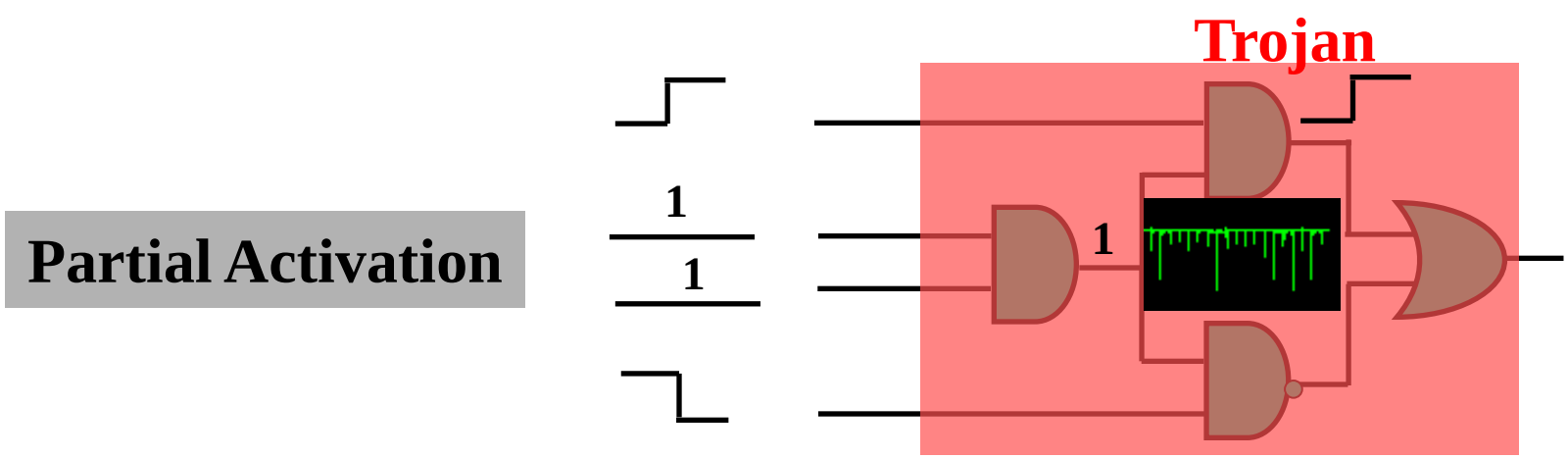
Side Channel Detection Techniques

- Full activation is extremely difficult
- Path delays are changed without partial or full
- Partial activation is more common and causes
  - power consumption
- Simplified Example:
  - FA: 1/256
  - PA: 3/8
  - Partial is 96 times more likely



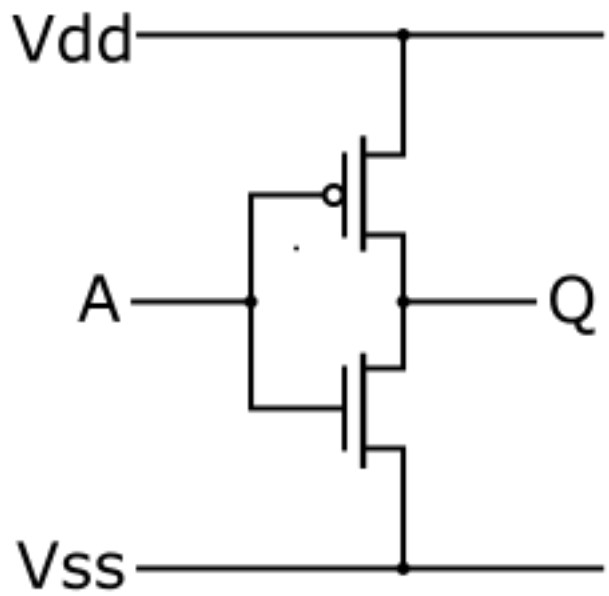
Side Channel Signal Analysis -- Power

- Hardware Trojans inserted in chip can change the power consumption characteristics
- Tight or loose distribution of Trojans can significantly impact detection through power analysis and isolation
- Partial activation of Trojan can be extremely valuable for power analysis
- The current drawn is dependent on the number of gates which are partially activated



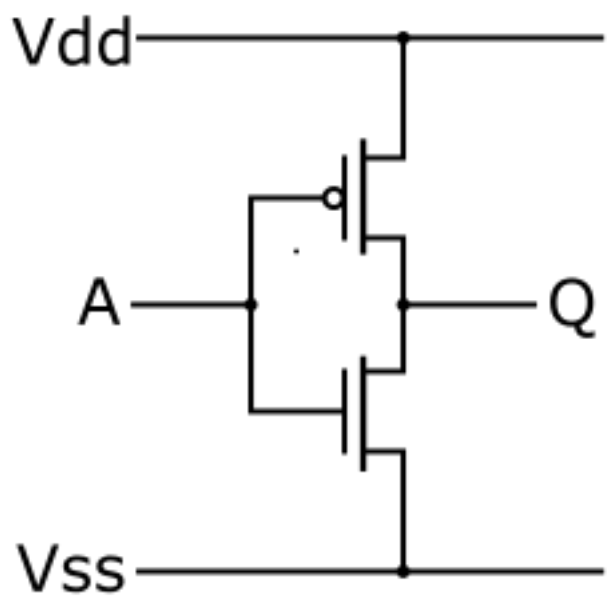
Side Channel Detection: Power

- Trojan gates will consume power.
  - CMOS static power is negligible
    - Leakage increased for lower technology nodes
    - Trojan area small compared to circuit
  - $P_{switch}=\alpha f C_L V_{DD}^2$
- Activity, α, is the chance of partial activation



Side Channel Detection: Power

- Heavily dependent on partial activation
- Activation probability is inversely related to path length
  - Short path -> more power
- Power techniques:
  - Good for Trojans on short paths
  - Misses Trojans on longer paths



Power Analysis -- Challenges

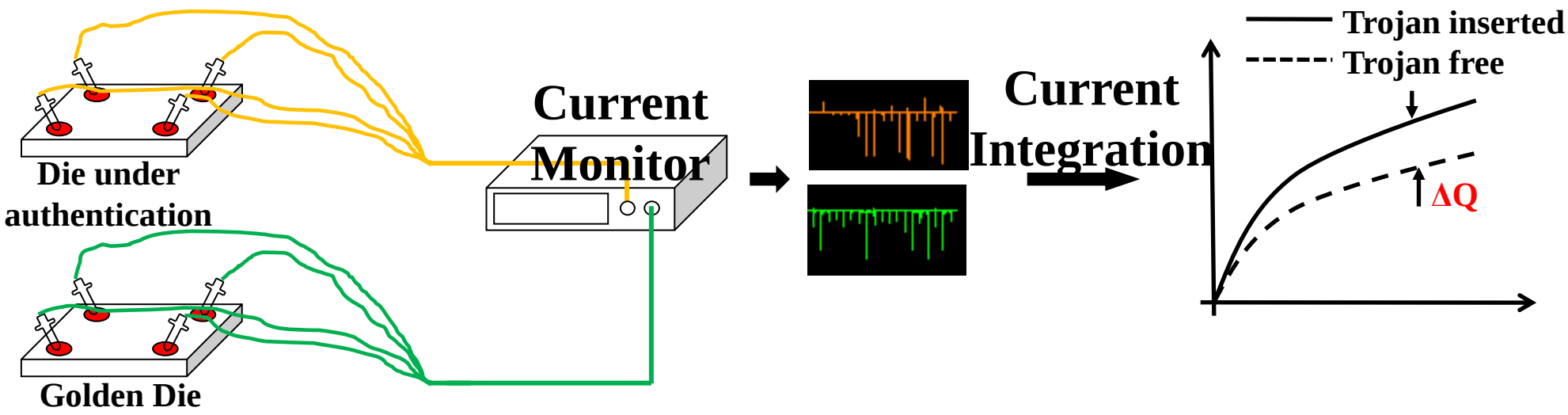
- **Pattern Generation**
  - How to increase switching activity in Trojans?
  - How to reduce background noise?
  - Switching locality
  - Random Patterns
    - No observation is necessary , Similar to test-per-clock
- **Measurement Device Accuracy**
  - Measurement noise
- **Process Variations**
  -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

Current Integration Method

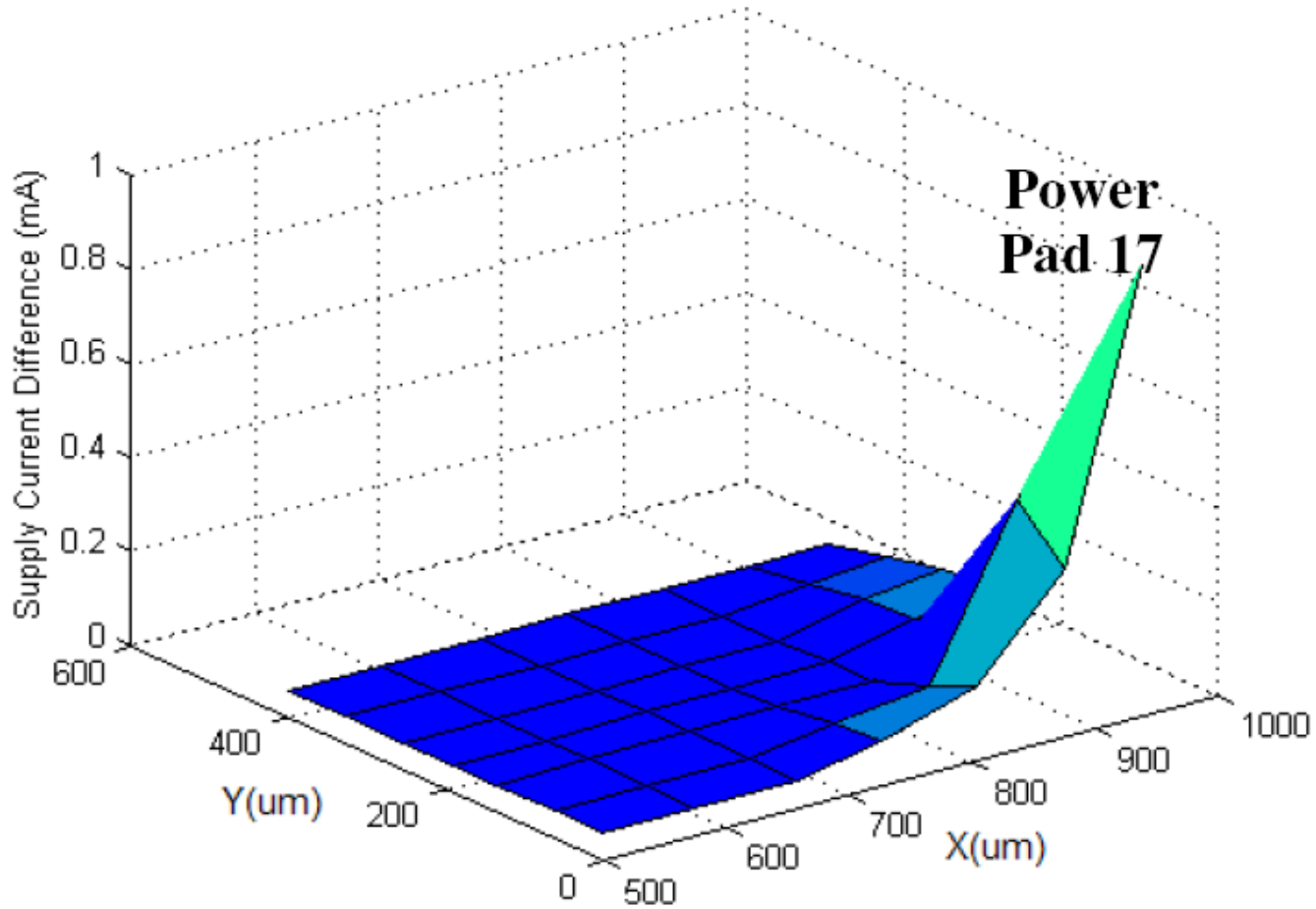
- **Current consumption of Trojan-free and Trojan-inserted circuits**

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

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



Power Analysis -- 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.

Process Variations

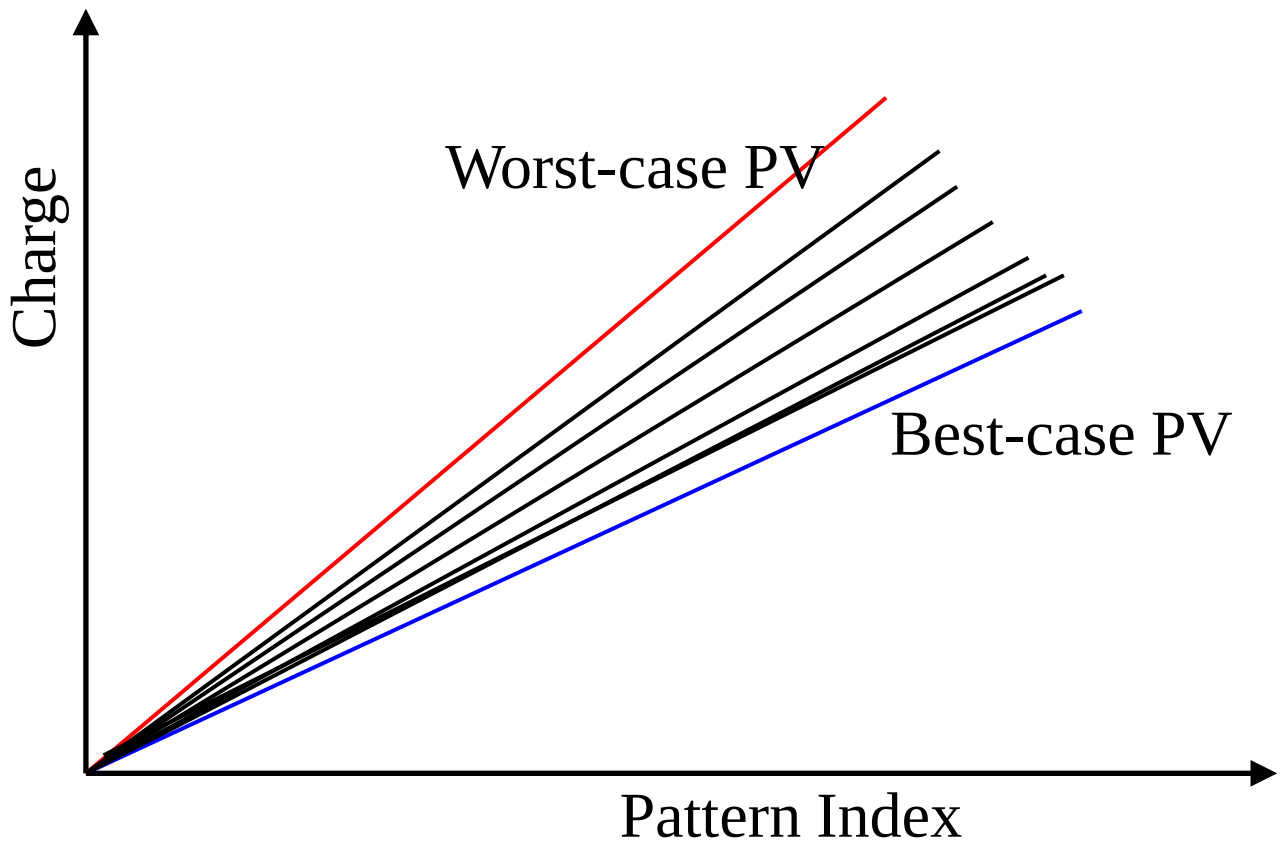
- **Worst & Best Cases:**
  - **Define lower and upper bounds on current consumption**
  - **Determine confidence level on Trojan detection**

PV:

L: Channel Length)

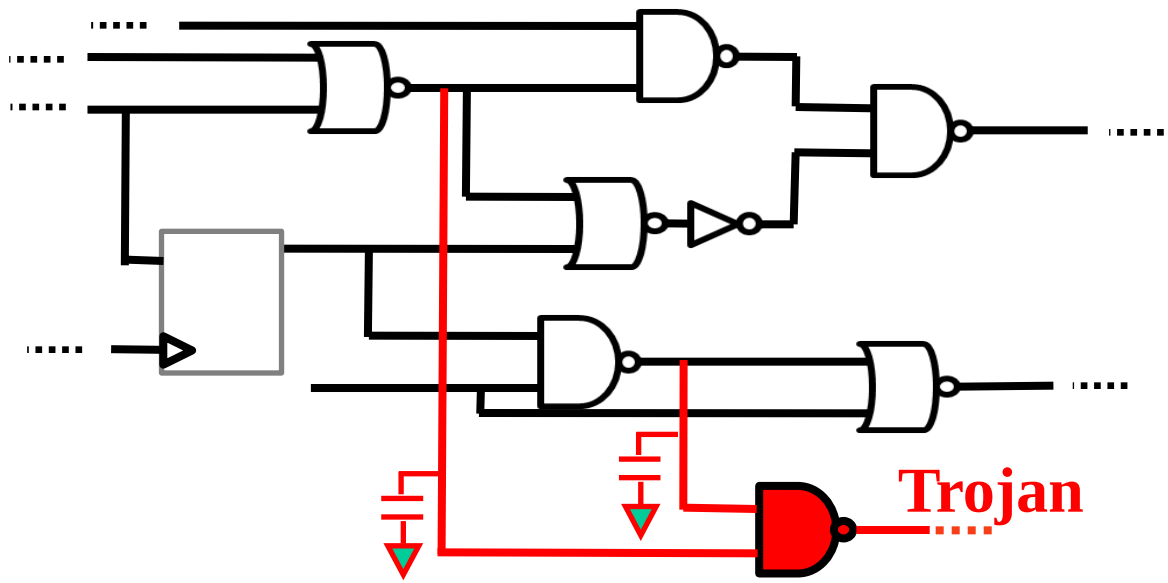
Vth: Threshold voltage

Tox: Oxide Thickness



Side Channel Analysis -- Delay

- Hardware Trojans can also change the circuit delay characteristics
- Some Trojans cannot be detected using power analysis methods
- A change in physical dimension of the wires and transistors can also inject delay to the paths in the circuit



Side Channel Detection: Delay

- Path Slack: difference between operating period and the period where a particular path is likely to fail and cause a timing error.
- Critical Path: The longest path in the circuit. The critical path is used to determine the operating frequency.
- Path slack decreases with path length.
  - A Trojan is more likely to cause a timing error on a longer path
  - A Trojan will consume more power on a shorter path.
  - Adversaries must find a balance while also achieving the desired malicious effect.

Delay Analysis -- Challenges

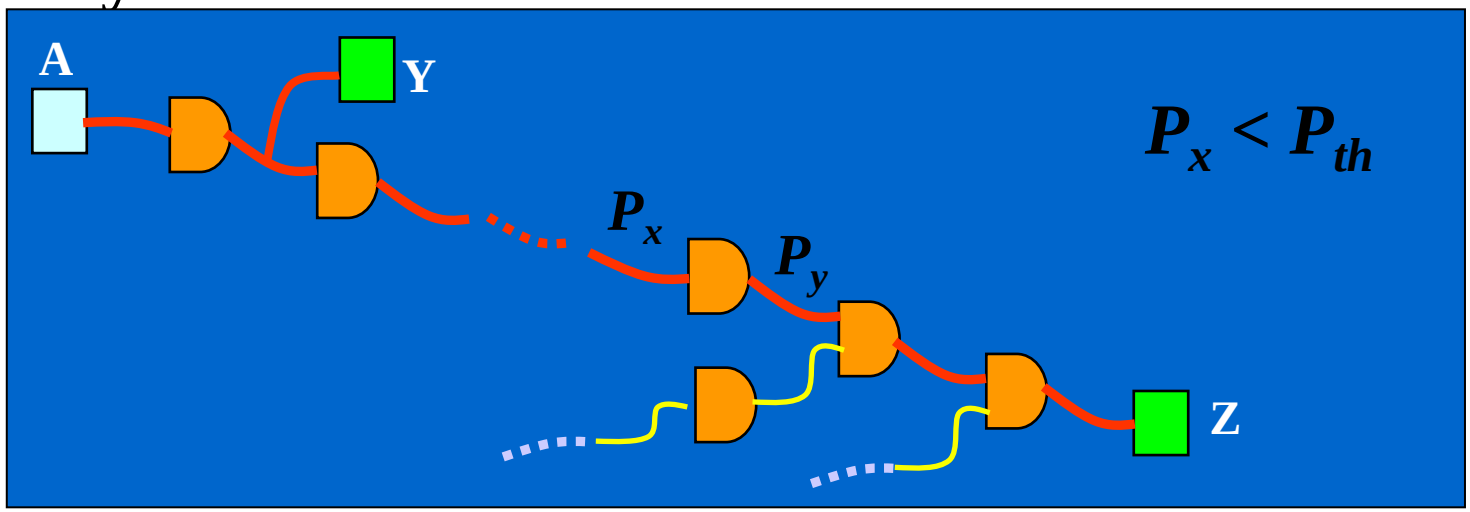
- **Major advantage over power analysis: No activation is required.**
- **Detection and Isolation**
  - How significant is the delay inserted by the Trojan?
  - It depends on Trojan size and type
  - Location: on short paths vs long paths
- **Pattern Generation**
  - Delay test patterns
  - Differentiate small delay caused by manufacturing defects
  - Timing-aware ATPGs
- **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 impacts several paths**

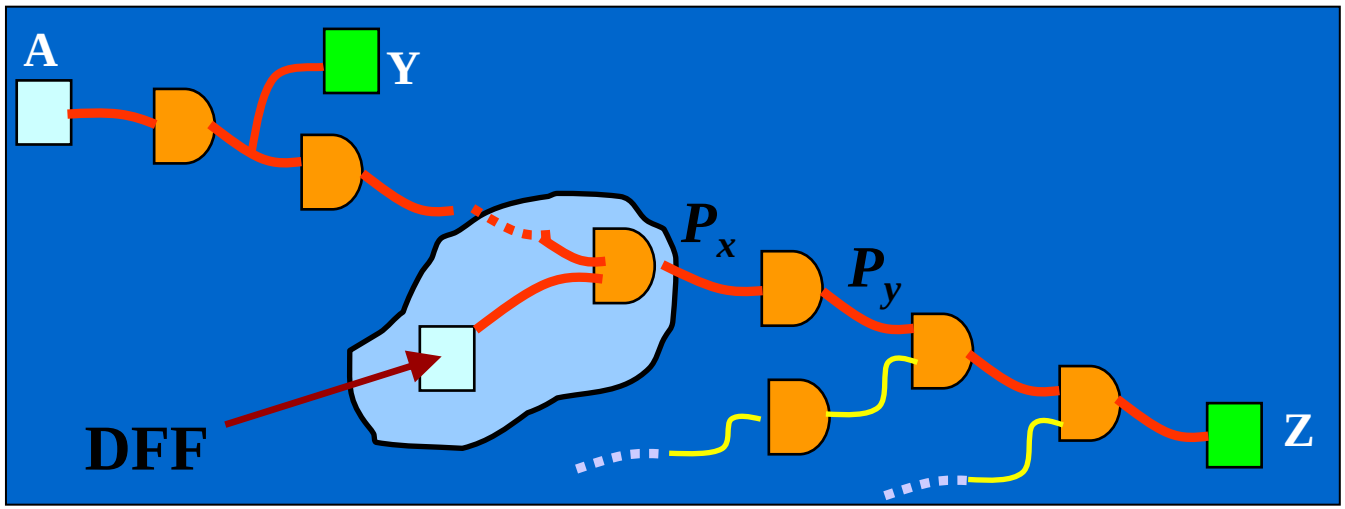
Increasing Probability of Partial/Full Activation

- **Challenge:**
  - **How to generate transitions in the Trojans?**
  - **There is no knowledge on the type, size, and location of Trojans**
  - **You may argue that Trojans are inserted in rare triggering areas of the circuit**
    - **Difficult to generate switching in these areas**

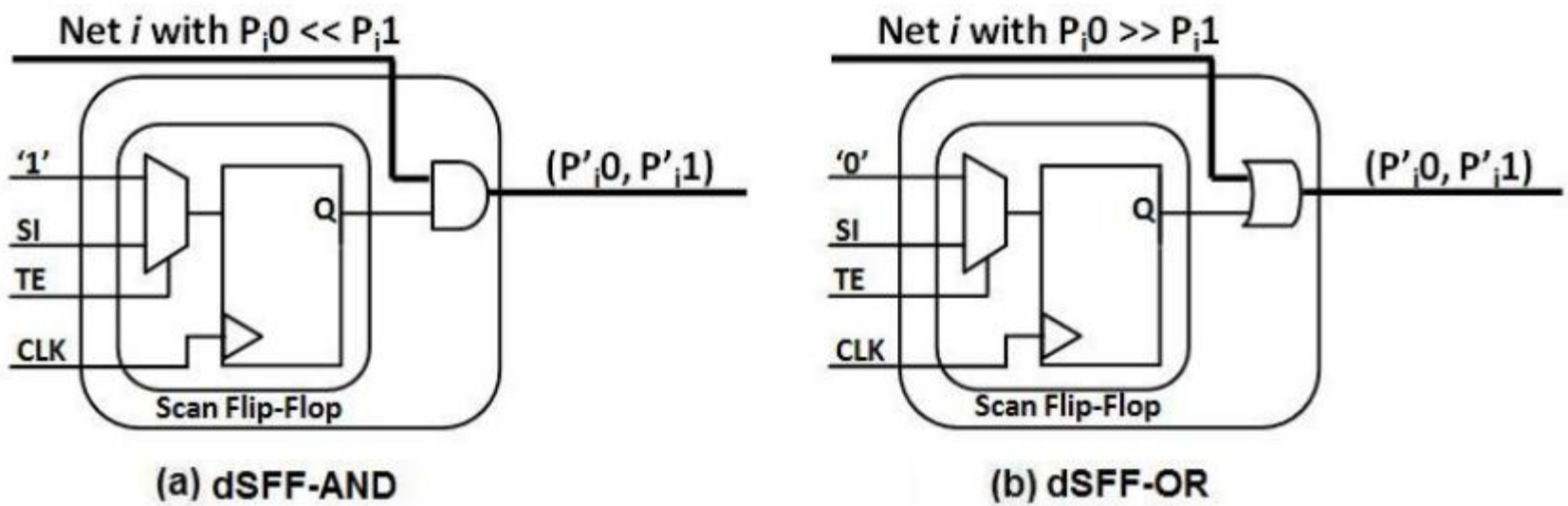
Increasing Probability of Partial/Full Activation

- **Inserting dummy FFS on path with very low activation probability**





Increasing Probability of Partial/Full Activation



Golden Models

- Golden Model: data set collected from verified Trojan-free ICs.
- Generalized Steps:
  1. Collect data from random ICs
  2. Destructively reverse engineer ICs
  3. Keep the data if the destroyed ICs were Trojan-free
- A golden model is used to compare all other ICs in most side-channel based techniques.

Golden Models

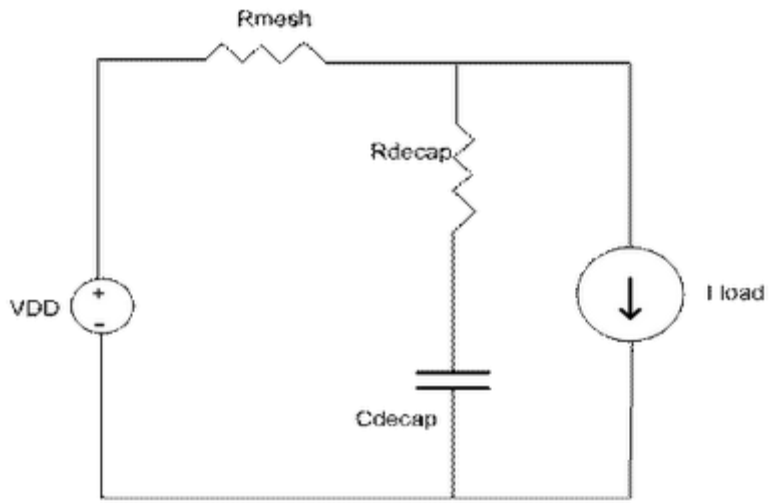
- Problems with Golden Models
  - GDSII masks are expensive
    - Adversaries likely to insert Trojans in all chips
  - Obtaining Golden Models is expensive
    - A large number of samples is required
    - Determining the number of samples needed can be problematic

Design for Trust

- Any technique that alters the design process to make Trojan-insertion more difficult.
  - Does not aim to detect Trojans that have already been inserted.
- An adversary must avoid changing the layout
  - Fill unused standard cells.
- Can a tamper-resistant structure be produced to fill unused standard cells?

Design for Trust

- Unused spaces are often filled with DeCaps (decoupling capacitors)
  - Reduce noise
  - Consume power
- Some may be removed without any noticeable change to the circuit.



Reverse Engineering

- Destructive reverse-engineering is used to build golden models
- Alone, destructively testing a subset of all ICs cannot guarantee that the rest of the ICs are actually Trojan Free.
  - What if a second mask was used to produce a small number of Trojan-inserted ICs.
- What about non-destructive tests?

Reverse Engineering

- MARVEL: Malicious Alteration Recognition and Verification by Emission of Light
- Active devices emit infrared light when turned on
- High sensitivity photon sensors capture the weak emission while the circuit is supplied with test patterns.
- How is data interpreted?