On Borrowed Time – Preventing Static Side-Channel Analysis

Robert Dumitru[*†], Thorben Moos[‡], Andrew Wabnitz[§], and Yuval Yarom[†]

[*] THE UNIVERSITY of ADELAIDE

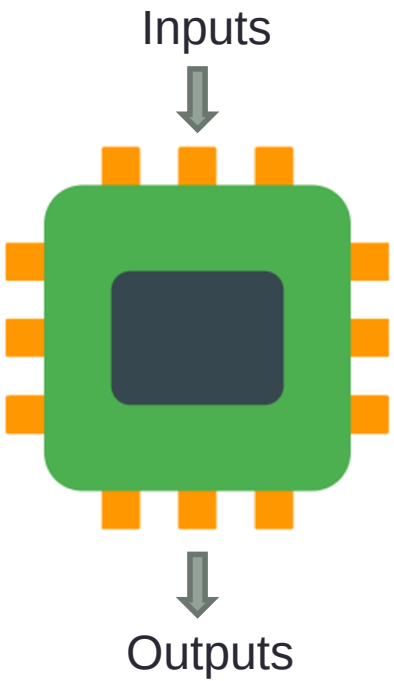
[†] RUB

[‡] UCLouvain

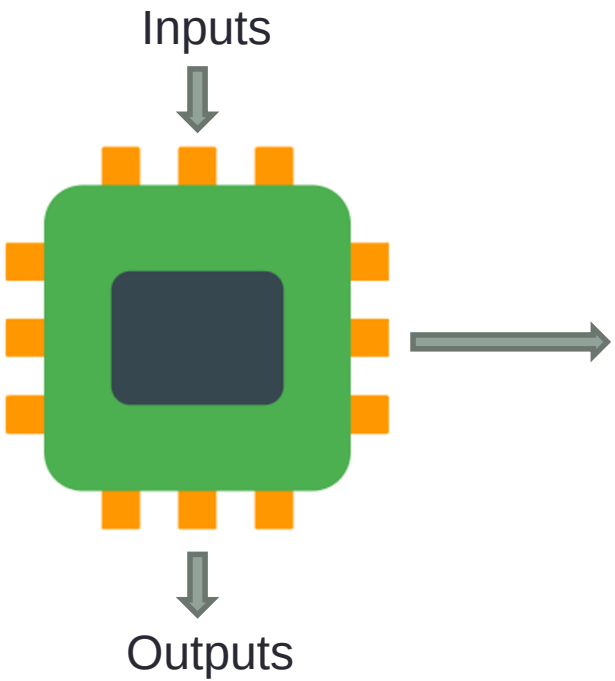
[§] Australian Government, Department of Defence, Science and Technology

Also supported by CASA Cyber Security in the Age of Large-Scale Adversaries, Internet Society

Information leakage through physical side-channels



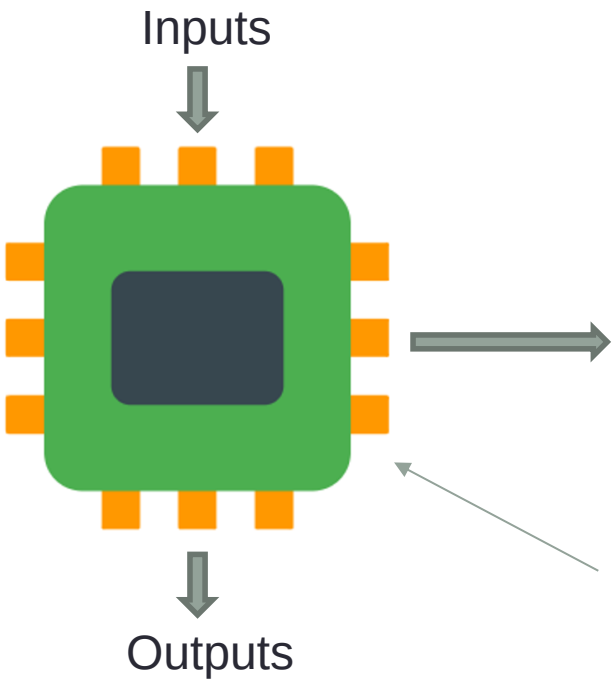
Information leakage through physical side-channels



Environmental effects:

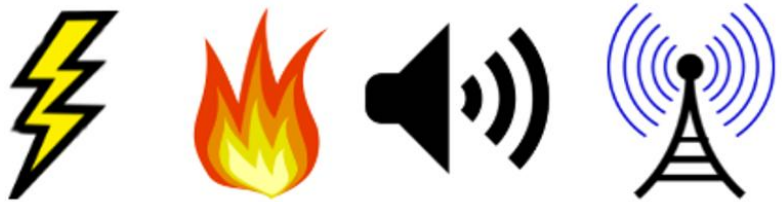
Power, Temperature, Acoustic, Electromagnetic

Information leakage through physical side-channels



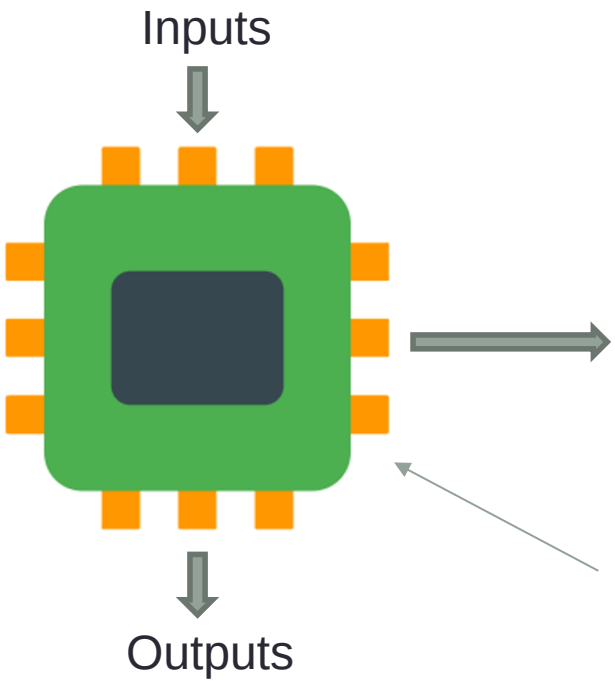
Environmental effects:

Power, Temperature, Acoustic, Electromagnetic



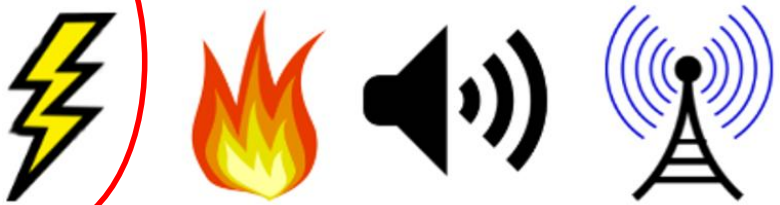
Black box model does not hold

Information leakage through physical side-channels



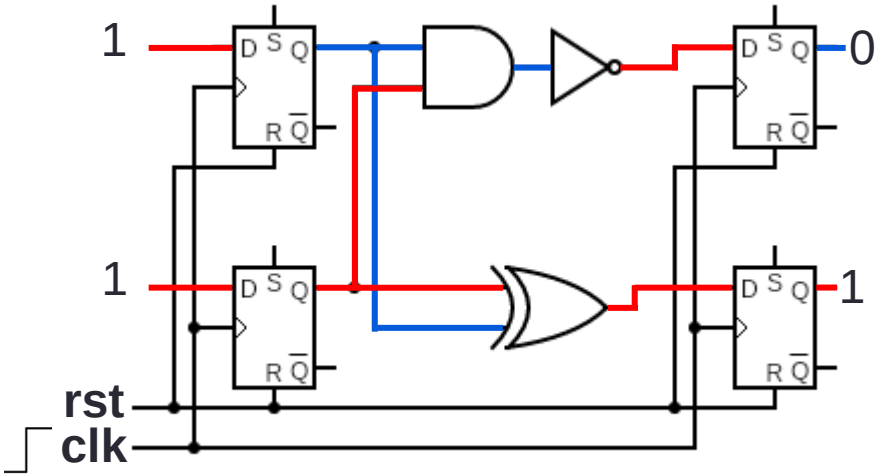
Environmental effects:

Power, Temperature, Acoustic, Electromagnetic

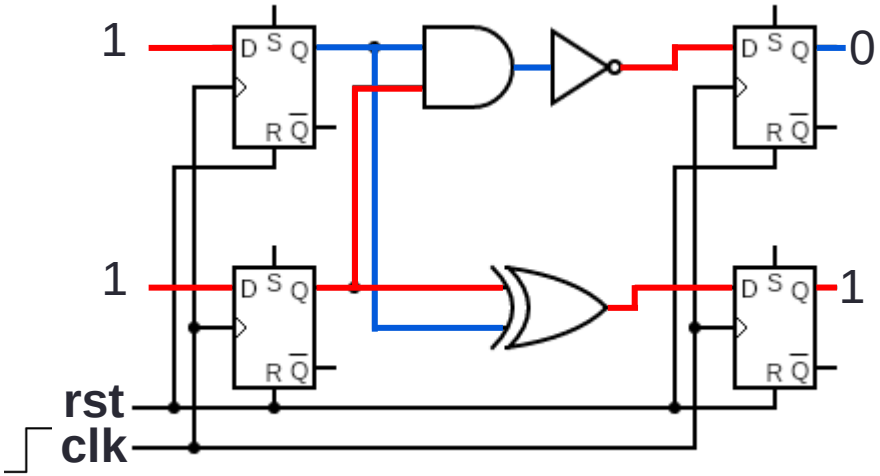


Black box model does not hold

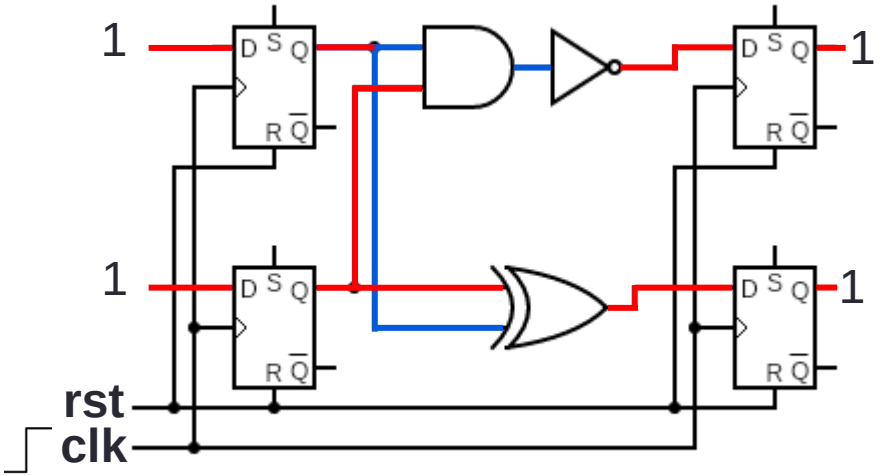
Power Analysis:
Static vs Dynamic Leakage Model



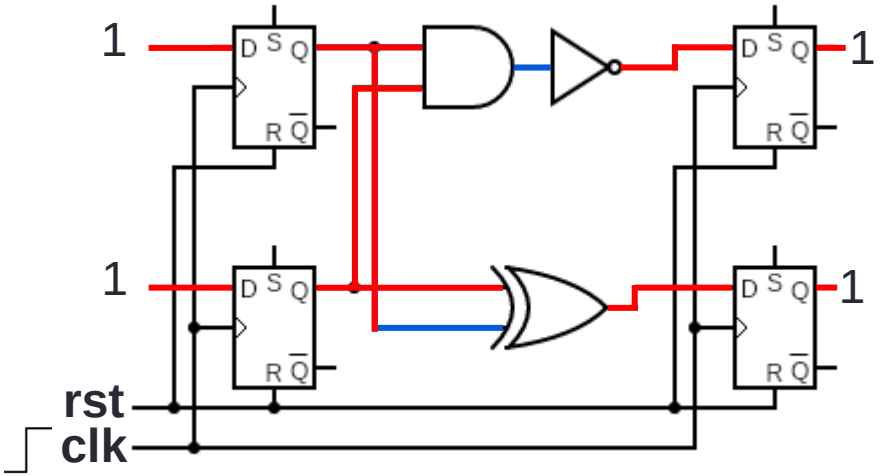
Power Analysis:
Static vs Dynamic Leakage Model



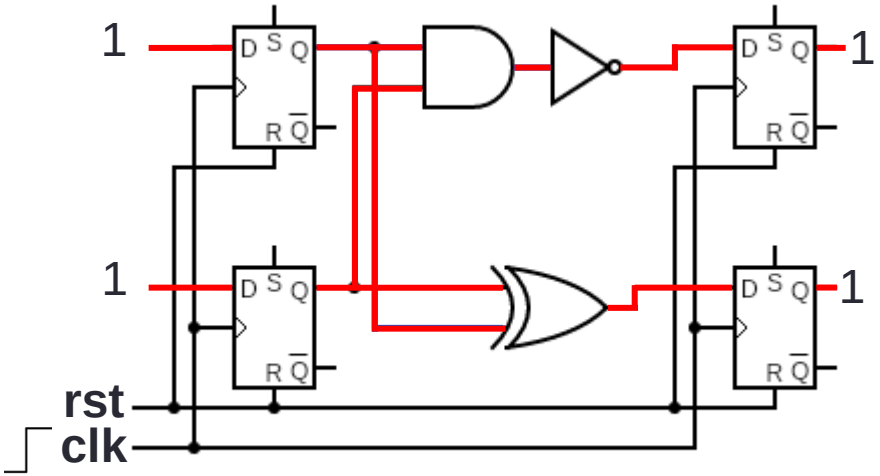
Power Analysis:
Static vs Dynamic Leakage Model



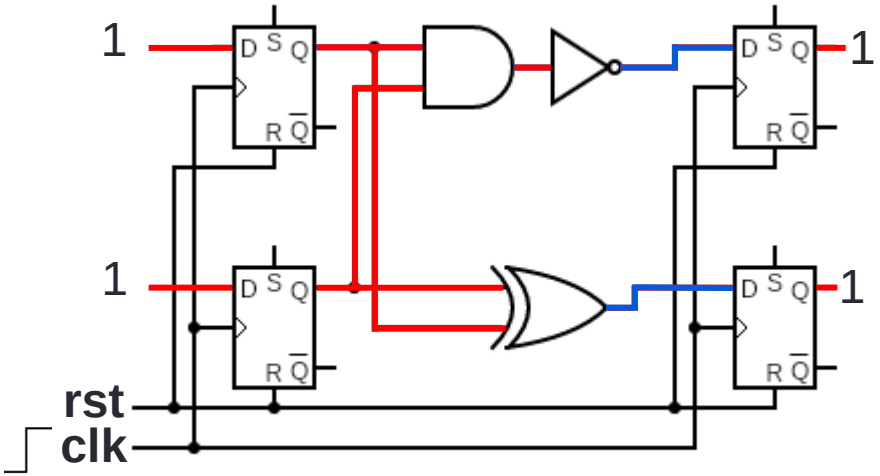
Power Analysis:
Static vs Dynamic Leakage Model



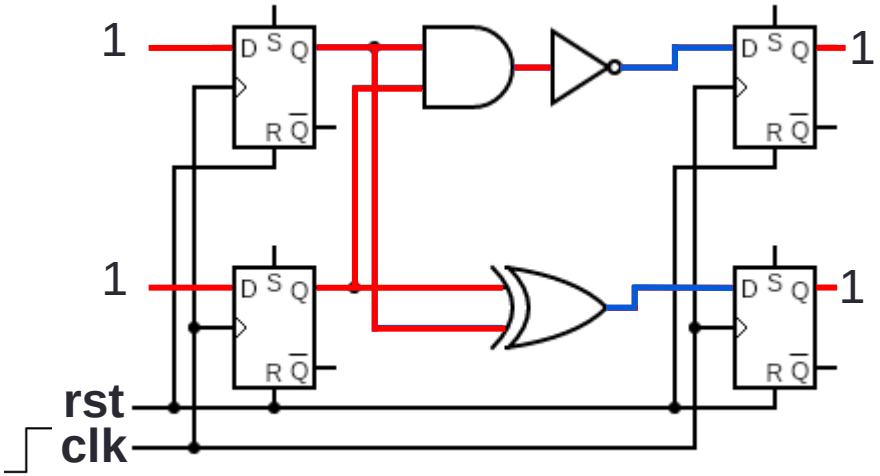
Power Analysis:
Static vs Dynamic Leakage Model

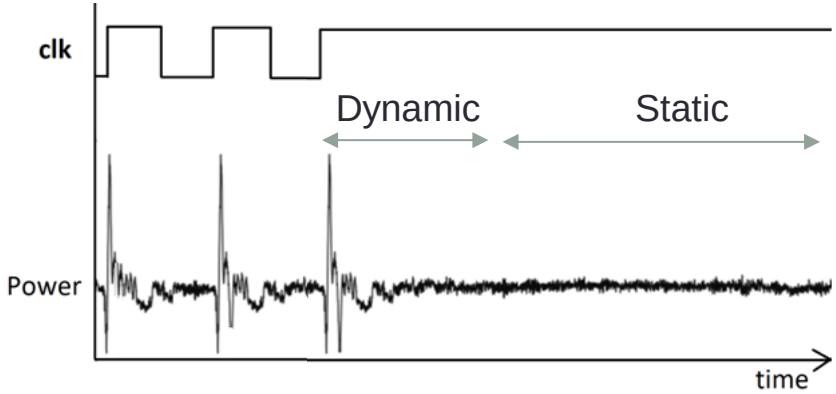


Power Analysis:
Static vs Dynamic Leakage Model



Power Analysis: Static vs Dynamic Leakage Model

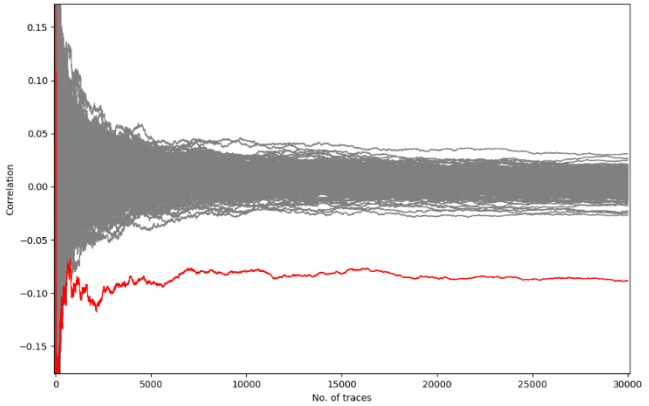


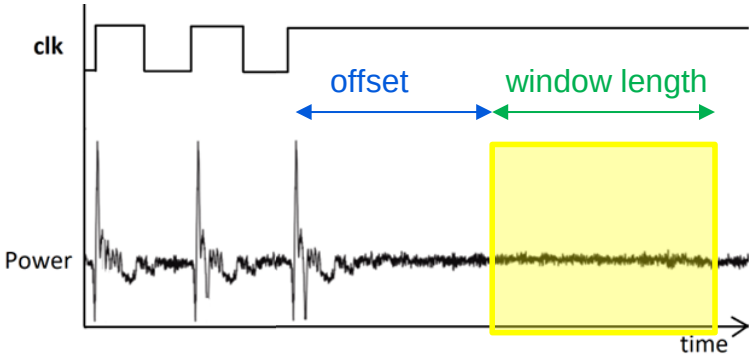


- Dynamic leakage comes from switching at clock transitions
- Static ‘steady-state’ leakage comes from values held in stateful elements

Determining the attack parameters

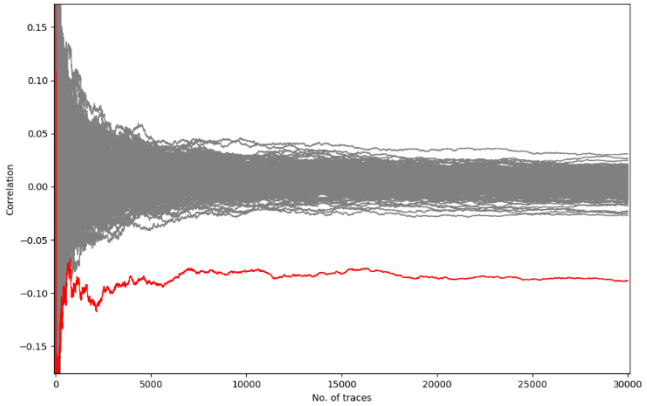
- We perform Correlation Power Analysis (CPA) on an AES FPGA implementation
- With a 20ms wait time (offset) and window length, we can recover the full key with 1,500 MTD

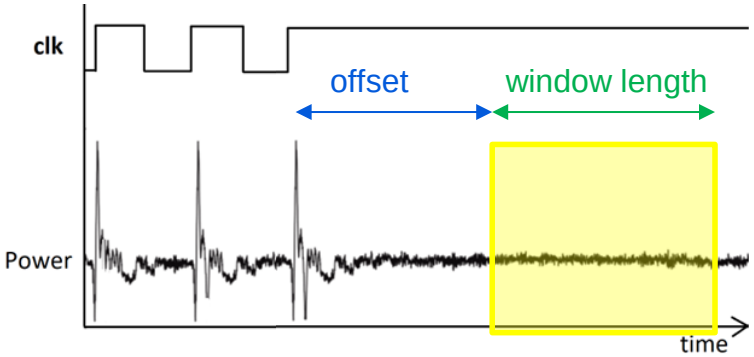




Determining the attack parameters

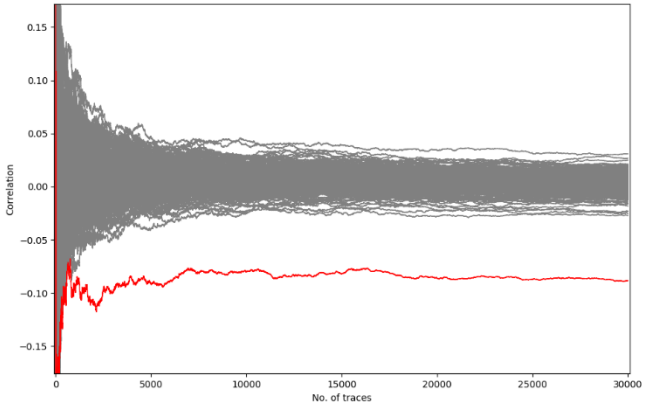
- We perform Correlation Power Analysis (CPA) on an AES FPGA implementation
- With a 20ms wait time (offset) and window length, we can recover the full key with 1,500 MTD
- We reduce the offset and window length

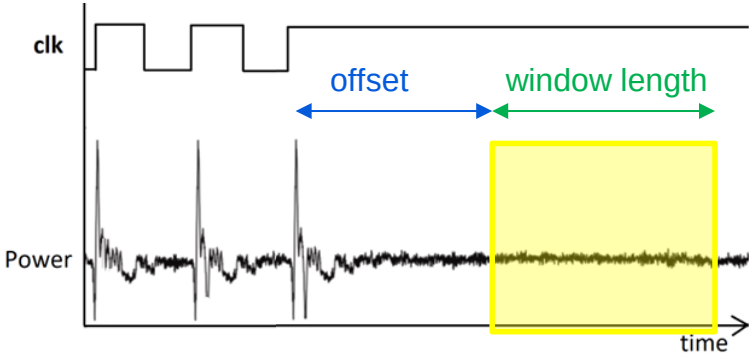


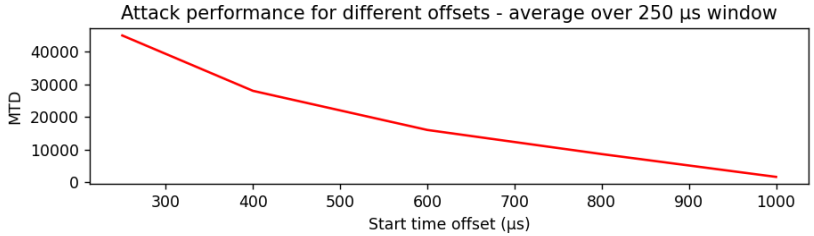


Determining the attack parameters

- We perform Correlation Power Analysis (CPA) on an AES FPGA implementation
- With a 20ms wait time (offset) and window length, we can recover the full key with 1,500 MTD
- We reduce the offset and window length
- No leakage for over 1 million traces at **200µs offset**



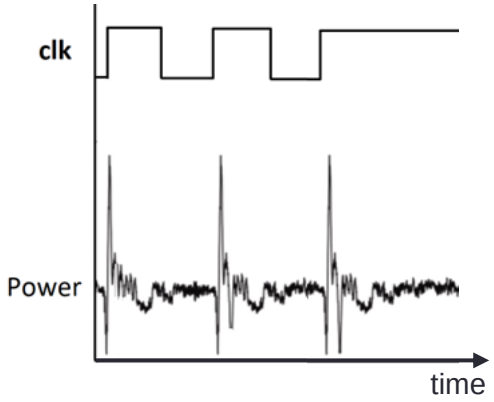




Borrowed Time countermeasure

Two conditions must hold within a target for static attack:

- The clock must be stopped
- Sensitive content must be retained in registers

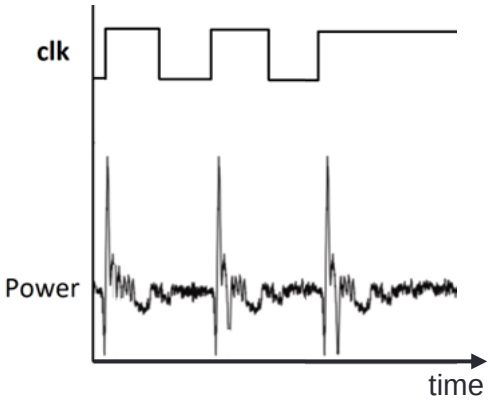


Borrowed Time countermeasure

Two conditions must hold within a target for static attack:

- The clock must be stopped
- Sensitive content must be retained in registers

Protection: prevent these simultaneous conditions



Borrowed Time countermeasure

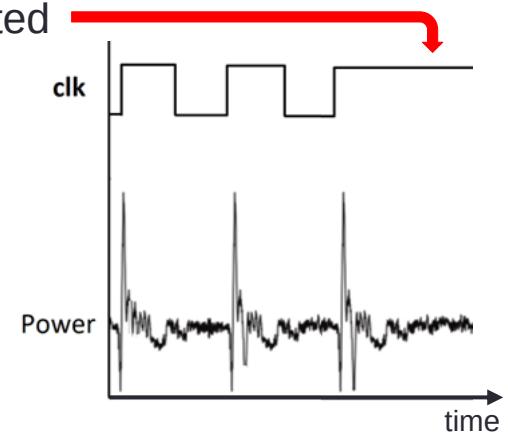
Two conditions must hold within a target for static attack:

- The clock must be stopped
- Sensitive content must be retained in registers

Protection: prevent these simultaneous conditions

Stopped clock detected

1

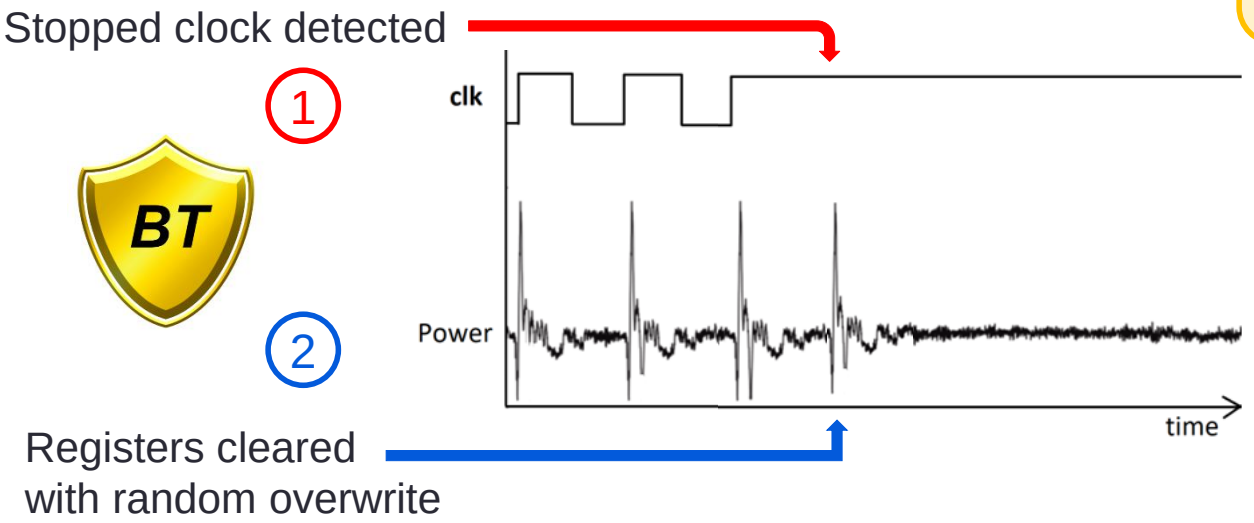


Borrowed Time countermeasure

Two conditions must hold within a target for static attack:

- The clock must be stopped
- Sensitive content must be retained in registers

Protection: prevent these simultaneous conditions



Borrowed Time variants

Two clock sensor primitives:

PLL-based

- Maintain internal oscillator and use this to check external clock source

Delay-chain-based

- Use asynchronous circuitry to check external clock source

Borrowed Time variants

Two clock sensor primitives:

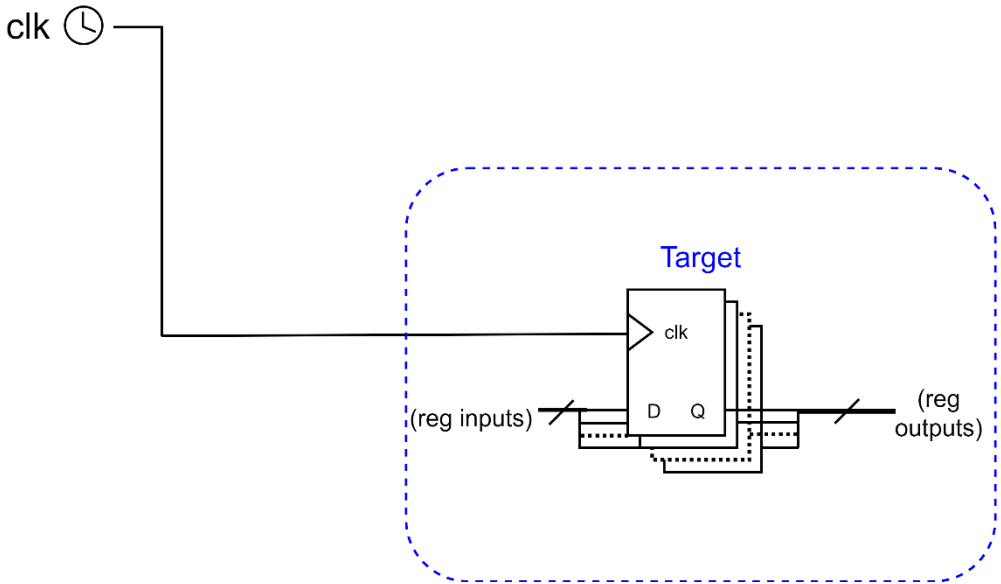
PLL-based

- Maintain internal oscillator and use this to check external clock source

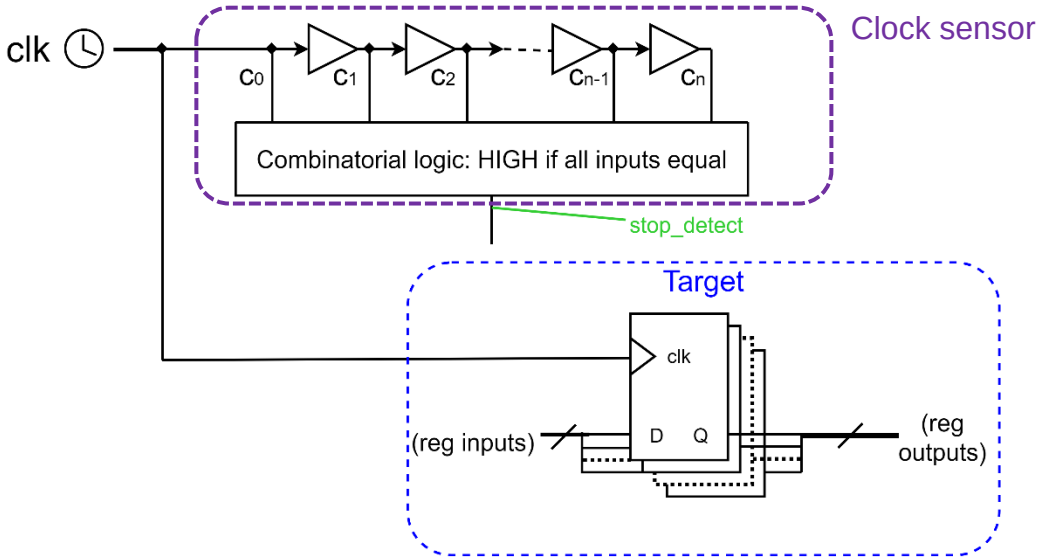
Delay-chain-based

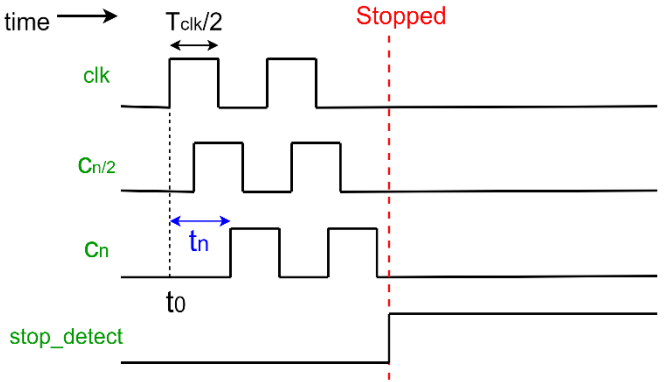
- Use asynchronous circuitry to check external clock source

Borrowed Time design

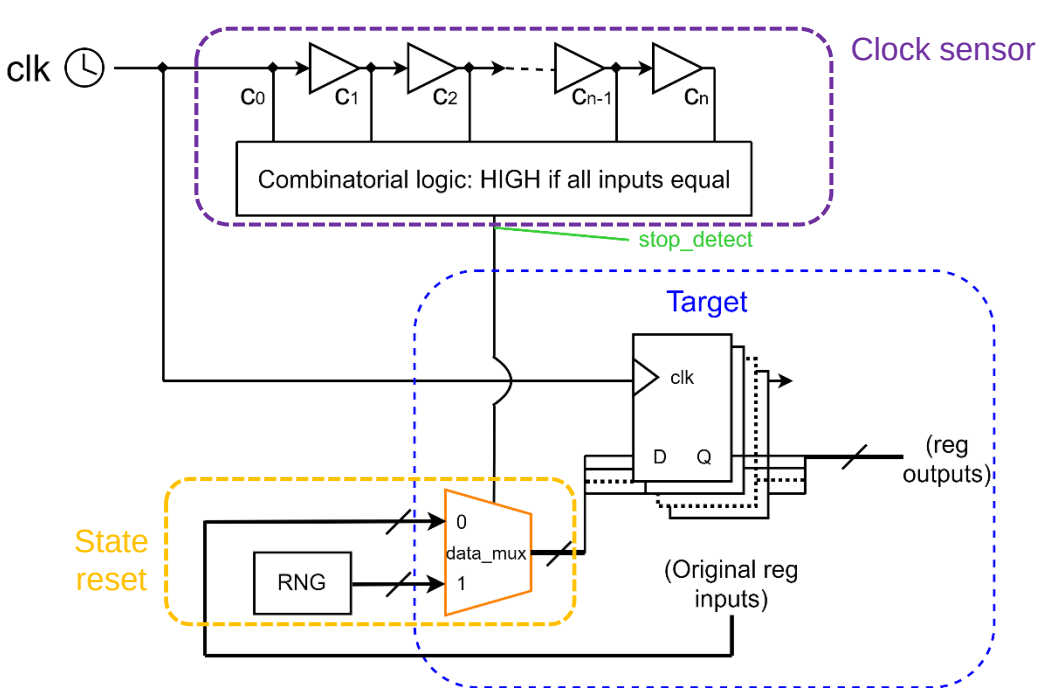


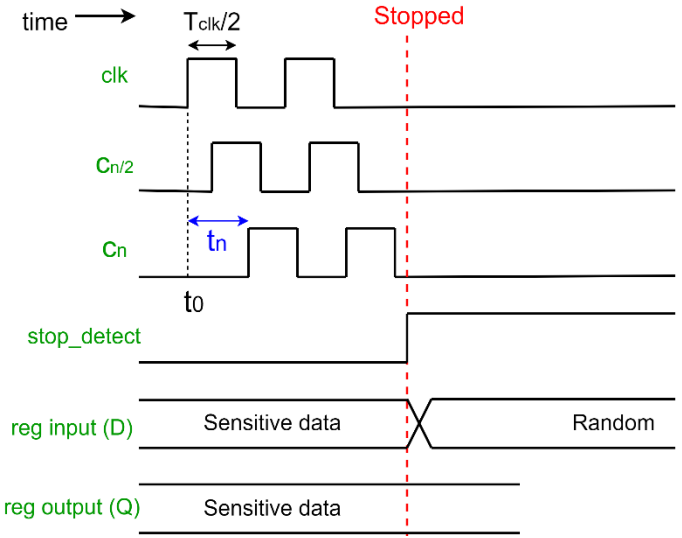
Borrowed Time design



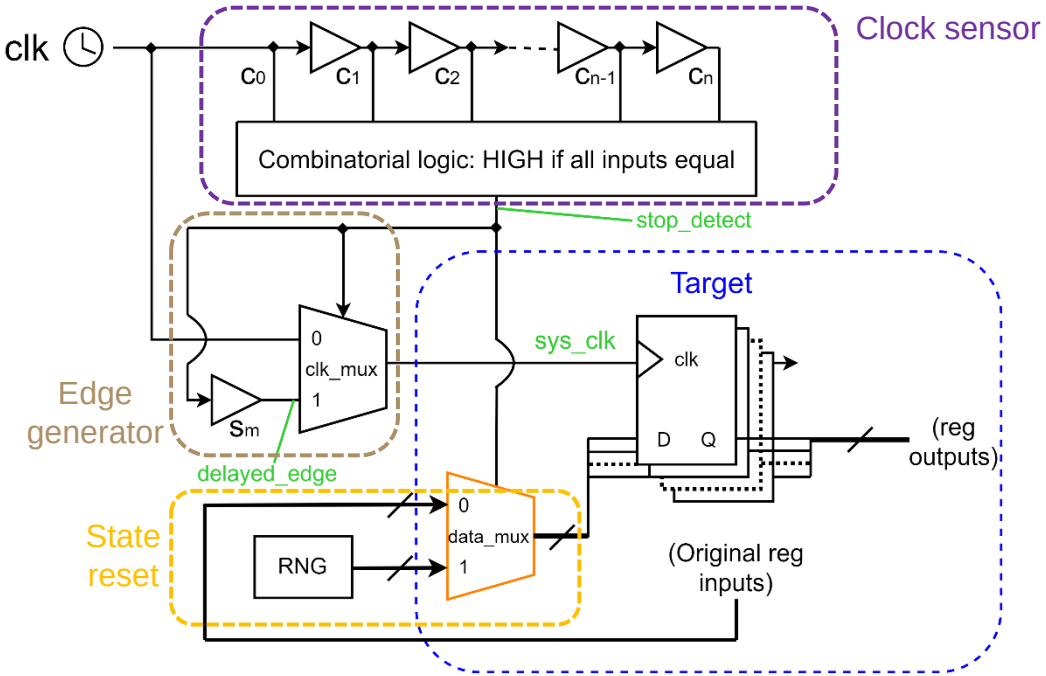


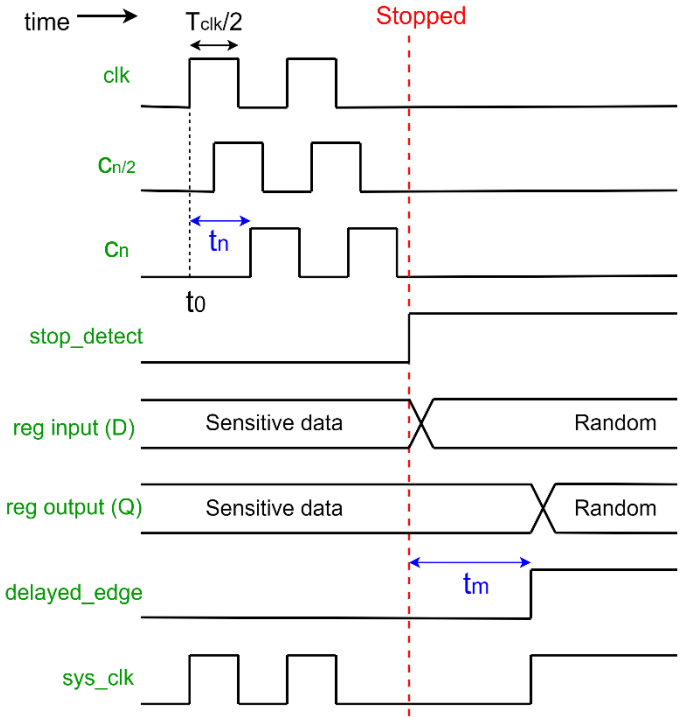
Borrowed Time design



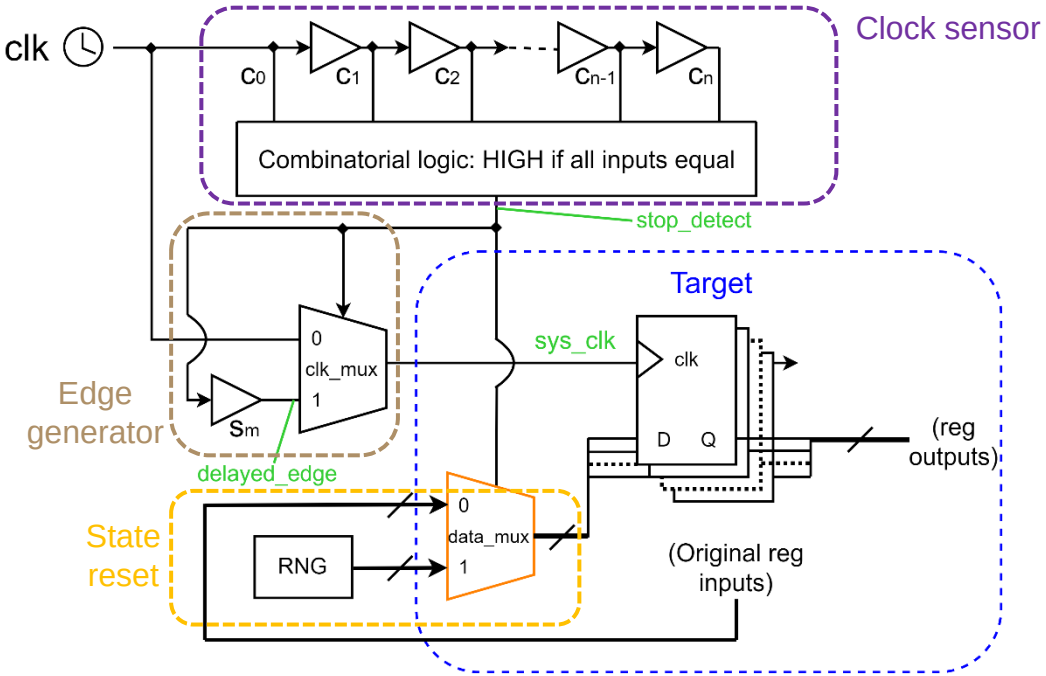


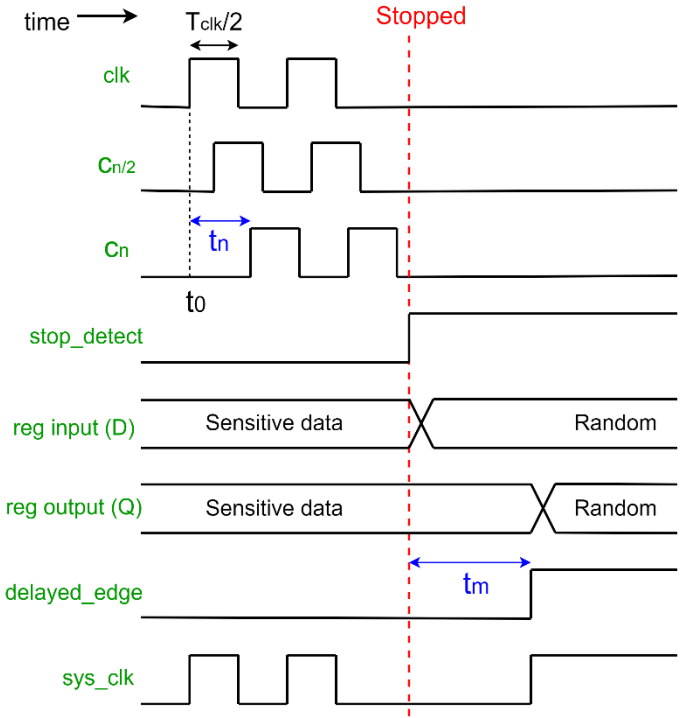
Borrowed Time design





Borrowed Time design

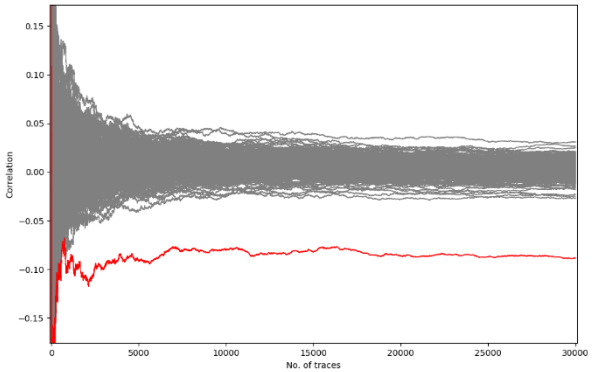




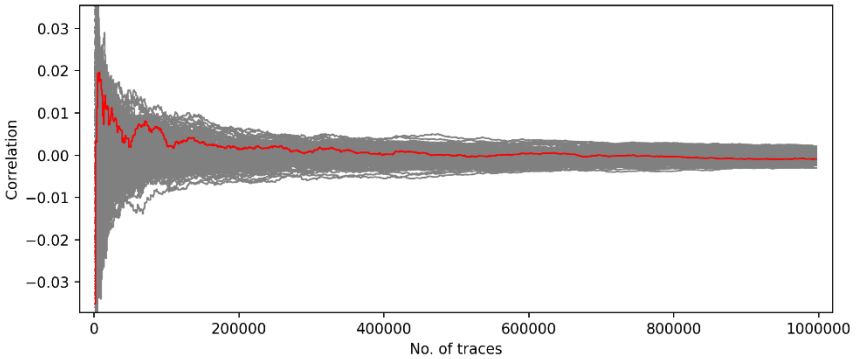
Assuming target operates in MHz range, BT can clear registers within **1µs** (<< 200µs)

Borrowed Time evaluation

Without countermeasure



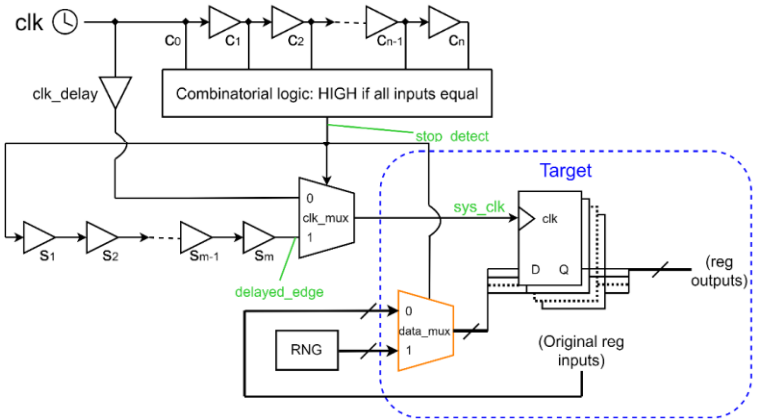
With Borrowed Time



Borrowed Time

- Flexible in-chip design to protect against static SCA
- Can allow for operation over a given frequency range
- Clock glitching resilient
- Enables safe operation inside clock-gated system
- Modest relative overhead

Paper



Code