Sensors for Remote Power Attacks: New Developments and Challenges

Brian Udugama, Darshana Jayasinghe, Sri Parameswaran

ASP-DAC 2024
January 22-25, 2024
Incheon Songdo Convensia, South Korea

This talk is about…

Stealthy on-chip sensors for RPA (remote power analysis) attacks

- Development of **RPA attacks.**

- **Design considerations** of on-chip sensors for RPA attacks.

- **Current challenges** in developing and countering on-chip sensors.

Remote Power Analysis Attacks & On-chip Sensors

THE UNIVERSITY OF SYDNEY

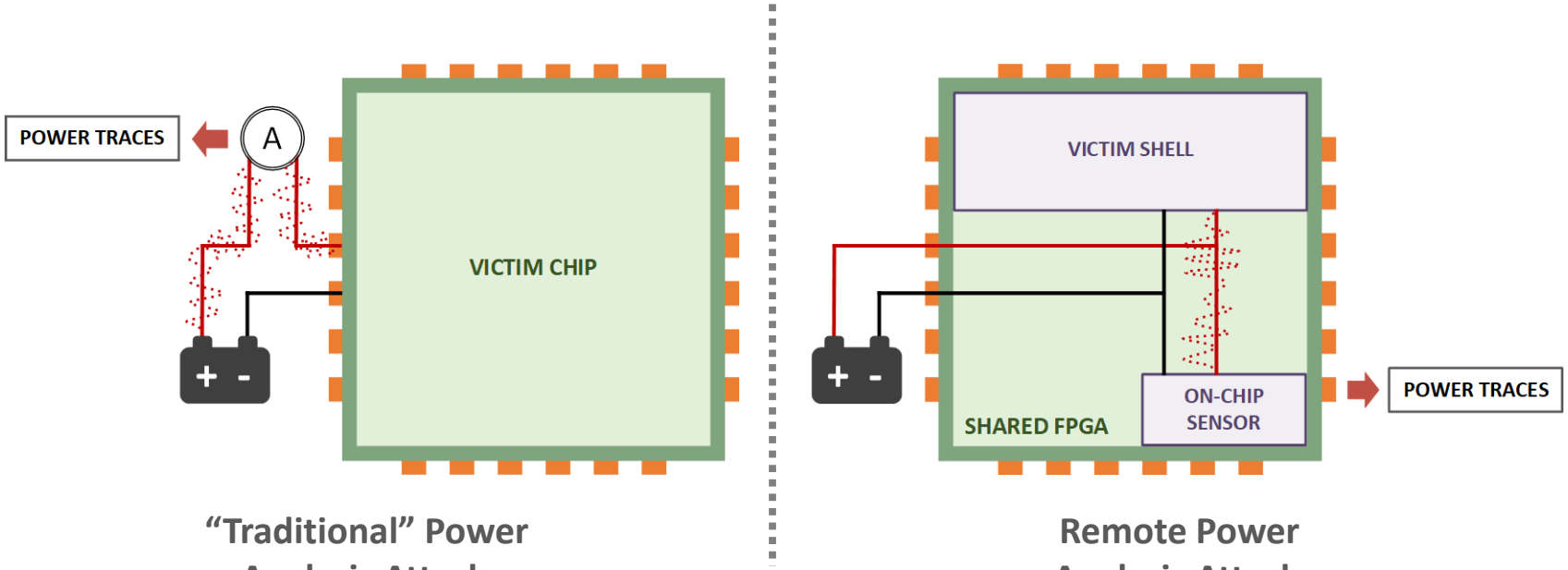
UNSW SYDNEY

Remote Power Analysis (RPA) Attacks

Extract cryptographic secrets by analyzing power consumption

Uses on-chip sensors – no oscilloscopes required

Can be **performed remotely without having physical access**



"Traditional" Power Analysis Attacks

Remote Power Analysis Attacks

THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

Remote Power Analysis (RPA) Attacks

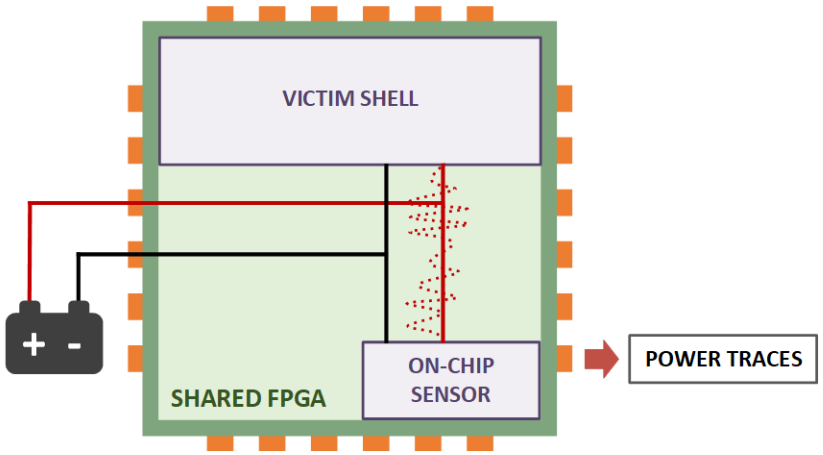
Extract cryptographic secrets by analyzing power consumption

Uses on-chip sensors – no oscilloscopes required

Can be **performed remotely without having physical access**

Typical target is an **Advanced Encryption Standard (AES)** module

Threat Model



- Two logically isolated circuits
  - Victim Shell (Victim)
  - On-chip sensor (Attacker)
- An AES module in Victim Shell
- Power traces from the on-chip sensor are analyzed to discern AES Key

On-chip Sensors for RPA Attacks

Measure variations in signal propagation delay

Propagation delay variations are related to changes in operating condition such as supply-voltage

 Power consumption leads to  supply-voltage to the chip

Therefore, **signal propagation delay can be used to measure power consumption**

Existing on-chip sensors:

- Delay line based sensors
- Ring oscillator (RO) based sensors
- Routing Delay Sensor (RDS)
- Voltage-Induced Time Interval Sensor (VITI)
- Power to Pulse Width Modulation Sensor (PPWM)

Design Considerations of On-chip Sensors

THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

On-chip Sensors - Design Considerations

1. Minimizing Hardware Resource Consumption

Hardware resource optimization is key to achieve cost-efficiency on FPGAs

Higher hardware resource consumption draws the attention of developers seeking optimization opportunities

Lower hardware resource consumption

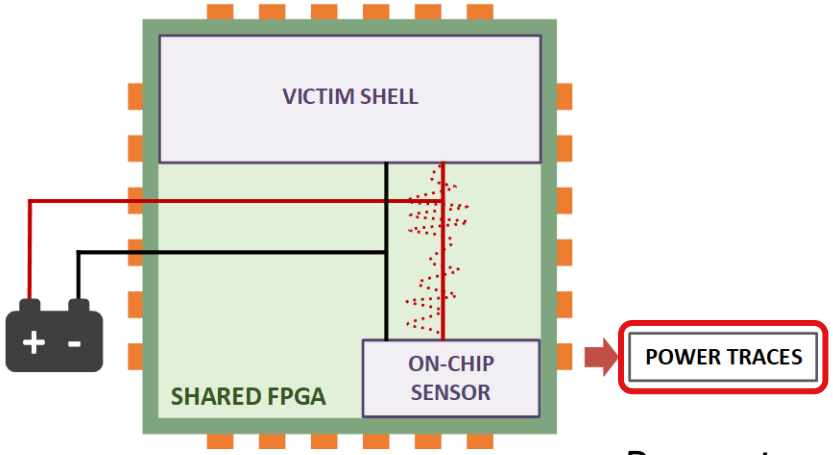
Draws lower attention and suspicion

Increased likelihood of being deployed on the intended target

On-chip Sensors - Design Considerations

2. Minimizing Bandwidth Resource Consumption

Recall Threat model



Power traces from the on-chip sensor are analyzed to discern AES Key

On-chip Sensors - Design Considerations

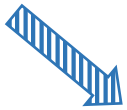
2. Minimizing Bandwidth Resource Consumption

Power traces from the on-chip sensor are often analyzed external to the FPGA

Power traces must be covertly transferred to the analysis module, without detection

Covertly transfer the power traces

Use a covert communication channel



Supports limited bandwidth

On-chip sensor must produce power traces that require minimal bandwidth

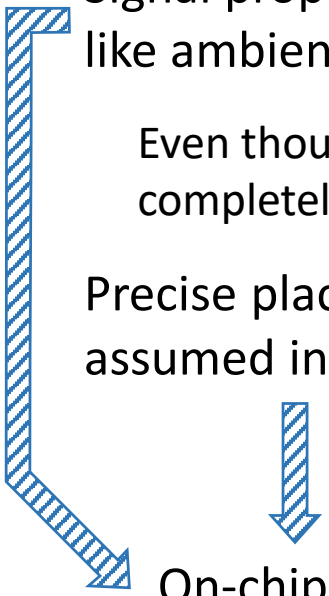
On-chip Sensors - Design Considerations

3. Fully Autonomous Self-calibration

Signal propagation delay on FPGAs are influenced by natural factors like ambient temperature and manufacturing process variation*

Even though insignificant at macro-scale, an on-chip sensor can become completely ineffective

Precise placement and routing of an on-chip sensor should not be assumed in a realistic RPA attack



On-chip sensors need to be able to autonomously calibrate

* **Jonas Krautter et al., "CPAmap: On the Complexity of Secure FPGA Virtualization, Multi-Tenancy, and Physical Design"**

On-chip Sensors - Design Considerations

4. Avoiding Characteristic Structures

Visually identifiable features on the floorplan

- ✗ Suspiciously long chains of elements 
- ✗ Combinational loops 

Features detectable using Design Rule Checks (DRC)

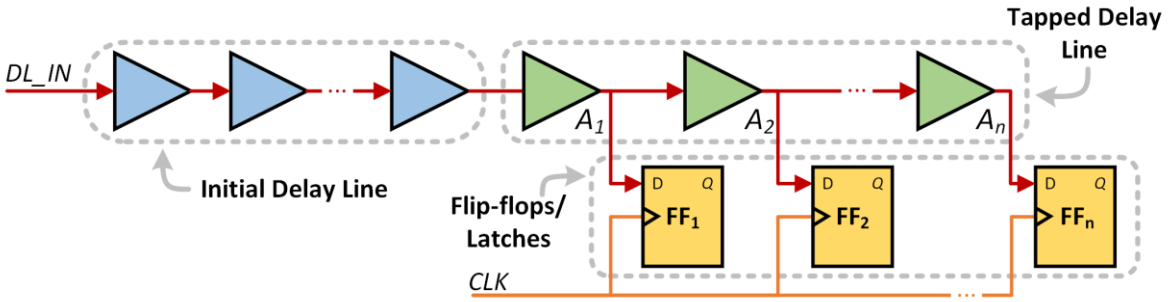
- ✗ Combinational loops
- ✗ Latches
- ✗ Other traceable patterns

On-chip Sensors in the Literature

THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

Delay Line Based Sensors



Time to digital converters (TDCs) are delay line-based sensors

The first RPA attack in the literature was carried out using a TDC*

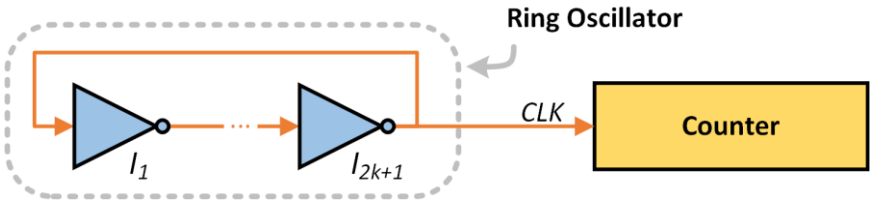
Properties with respective to design considerations:

- TDCs consume considerable (34 FPGA slices*) hardware resources ↓
- TDCs produce wide outputs requiring more bandwidth resources ↓
- TDCs can incorporate self-calibration+ (needs extra hardware resources) ↑
- Visual characteristics and latches may reveal TDCs ↓

* **F. Schellenberg et al., "An inside job: Remote power analysis attacks on FPGAs"**

\+ **Jonas Krautter et al., "CPAmap: On the Complexity of Secure FPGA Virtualization, Multi-Tenancy, and Physical Design"**

Ring oscillator (RO) based sensors



The RO sensor is made of a counter clocked using a ring oscillator

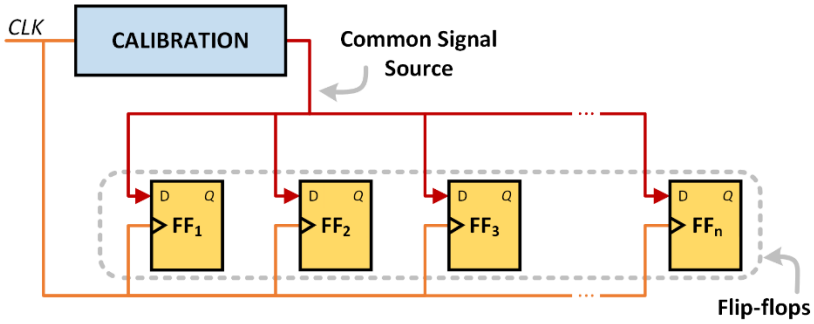
Each RO sensor is light weight; however, requires several (64) RO sensors*

Properties with respective to design considerations:

- A setup using ROs consume significant (128 FPGA slices*) hardware resources ⇩
- The cumulative bandwidth requirement is significantly higher ⇩
- Thus far, no self-calibration has been demonstrated ⇩
- Combinational loops, gated clocks and latches may reveal ROs ⇩

* **J. Gravellier et al., "High-Speed Ring Oscillator based Sensors for Remote Side-Channel Attacks on FPGAs"**

Routing Delay Sensor (RDS)



A tree of flip-flops connected to a common signal source forms RDS*

Tapped delay line variants of RDS resemble delay line-based sensors*

Properties with respective to design considerations:

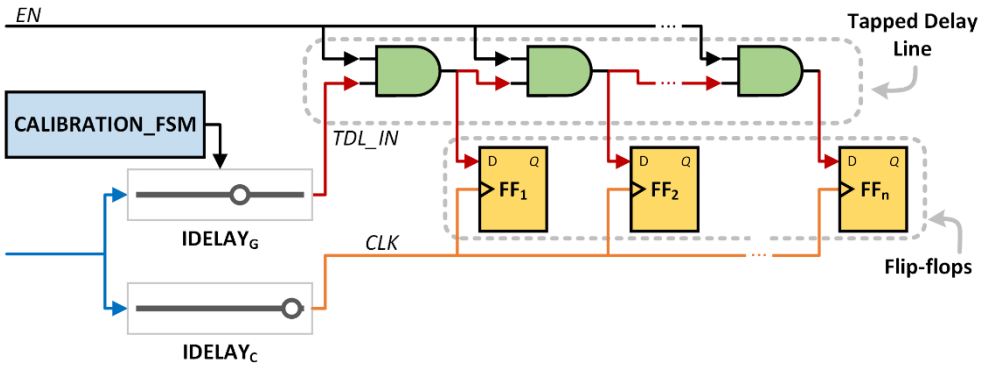
- RDS consumes considerable (40 FPGA slices*) hardware resources ↓
- RDS produces a wide output requiring more bandwidth resources ↓
- Incorporates a built-in self-calibration mechanism ↑
- Latches may reveal RDS ↓

* **D. Spielmann et al., "RDS: FPGA Routing Delay Sensors for Effective Remote Power Analysis Attacks"**

THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

Voltage-Induced Time Interval Sensor (VITI)



VITI is the first on-chip sensor designed explicitly for RPA attacks*

Made of a **short delay line implemented on LUTs**

Properties with respective to design considerations:

- VITI consumes less (8 FPGA slices + 2 IDELAY elements*) hardware resources ⇑
- VITI produces a narrow output (4-bit*) requiring less bandwidth resources ⇑
- Incorporates a built-in self-calibration mechanism ⇑
- Does not feature a traceable characteristic ⇑

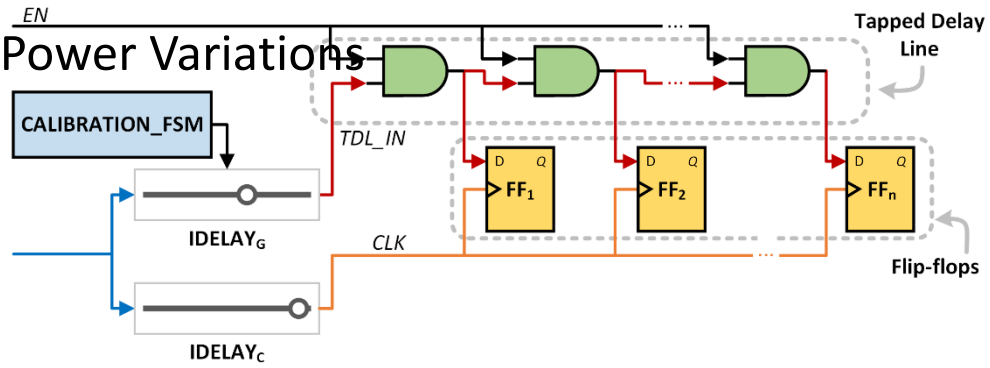
* **B. Udugama et al., "VITI: A Tiny Self-Calibrating Sensor for Power-Variation Measurement in FPGAs"**

THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

Voltage-Induced Time Interval Sensor (VITI)

Capturing Power Variations



VITI is the first on-chip sensor designed explicitly for RPA attacks*

Made of a **short delay line implemented on LUTs**

Properties with respective to design considerations:

- VITI consumes less (8 FPGA slices + 2 IDELAY elements*) hardware resources ⇑
- VITI produces a narrow output (4-bit*) requiring less bandwidth resources ⇑
- Incorporates a built-in self-calibration mechanism ⇑
- Does not feature a traceable characteristic ⇑

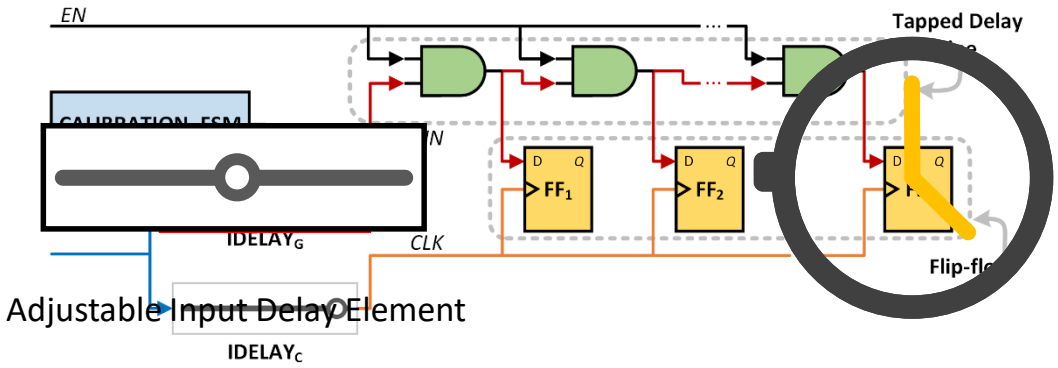
* **B. Udugama et al., "VITI: A Tiny Self-Calibrating Sensor for Power-Variation Measurement in FPGAs"**

THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

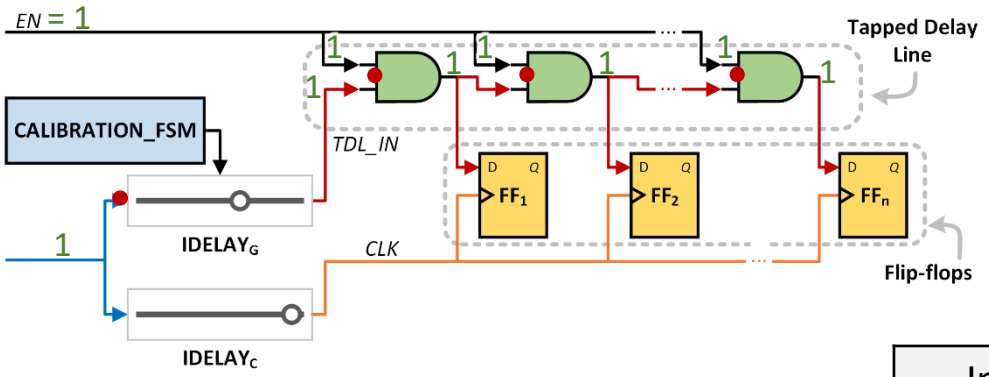
Voltage-Induced Time Interval Sensor (VITI)

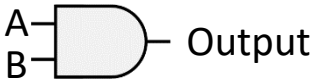
Capturing Power Variations



Voltage-Induced Time Interval Sensor (VITI)

Capturing Power Variations

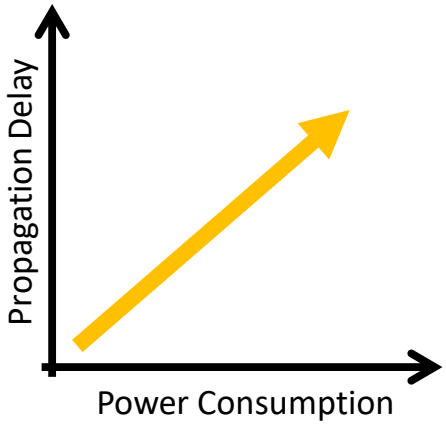




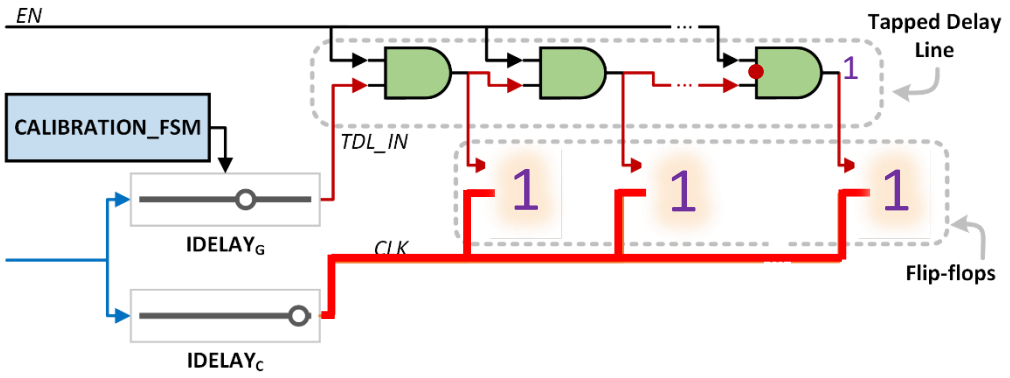
Inputs		Output
A	B	
0	0	0
0	1	0
1	0	0
1	1	1

Voltage-Induced Time Interval Sensor (VITI)

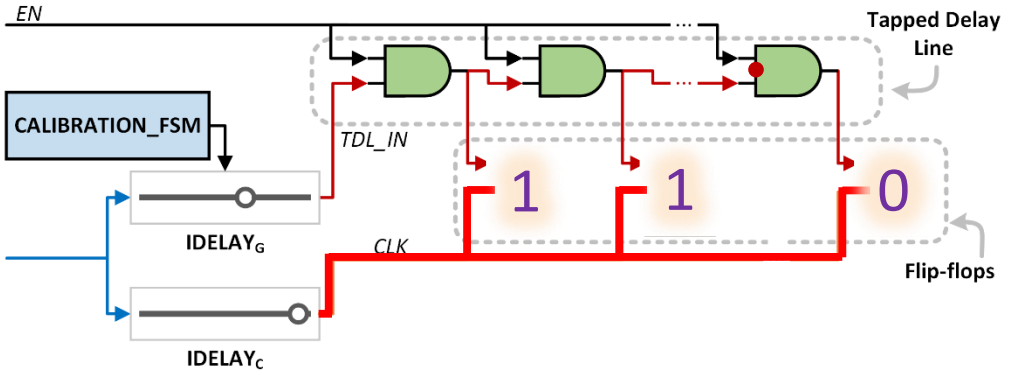
Capturing Power Variations



Low
Power
Consumption



High
Power
Consumption

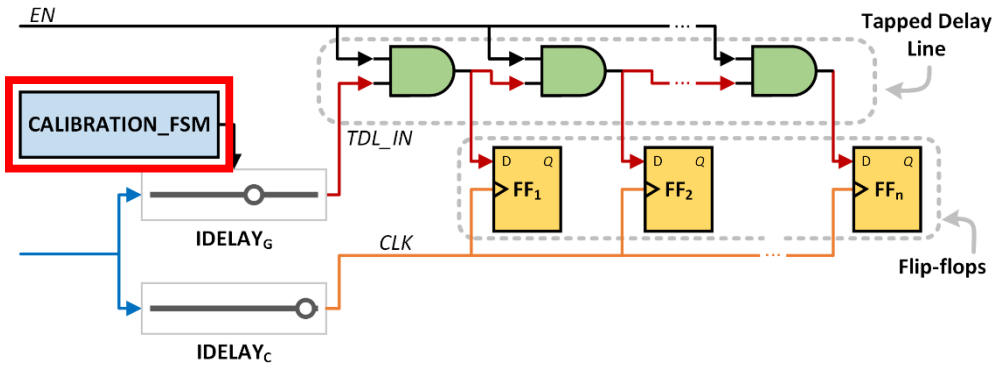


THE UNIVERSITY OF SYDNEY

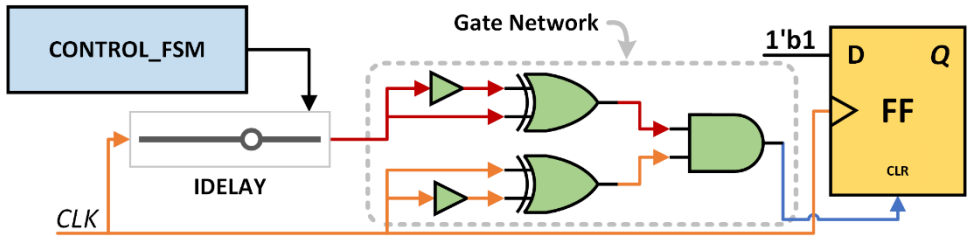
UNSW SYDNEY

Voltage-Induced Time Interval Sensor (VITI)

Capturing Power Variations



Power to Pulse Width Modulation Sensor (PPWM)



PPWM uses a gate network to **generate a pulse**, whose width is determined by the power consumption*

The pulse is used to **selectively clear a flip-flop**

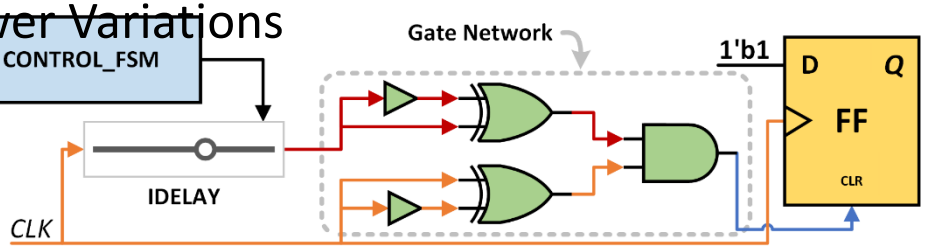
Properties with respective to design considerations:

- PPWM consumes less (13 FPGA slices + 1 IDELAY element*) hardware resources ⇑
- PPWM produces a single bit output **requiring least bandwidth resources** ⇑
- Incorporates a built-in self-calibration mechanism ⇑
- Does not feature a traceable characteristic ⇑

* **B. Udugama et al., "A Power to Pulse Width Modulation Sensor for Remote Power Analysis Attacks"**

Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations



PPWM uses a gate network to **generate a pulse**, whose width is determined by the power consumption*

The pulse is used to **selectively clear a flip-flop**

Properties with respective to design considerations:

- PPWM consumes less (13 FPGA slices + 1 IDELAY element*) hardware resources ⇑
- PPWM produces a single bit output **requiring least bandwidth resources** ⇑
- Incorporates a built-in self-calibration mechanism ⇑
- Does not feature a traceable characteristic ⇑

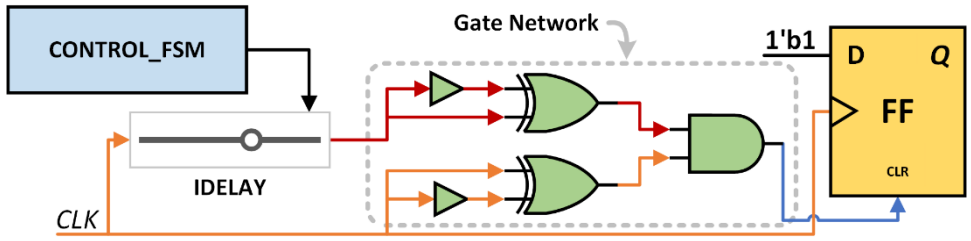
* **B. Udugama et al., "A Power to Pulse Width Modulation Sensor for Remote Power Analysis Attacks"**

THE UNIVERSITY OF SYDNEY

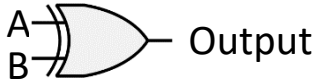
UNSW SYDNEY

Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations



Inputs		Output
A	B	
0	0	0
0	1	1
1	0	1
1	1	0



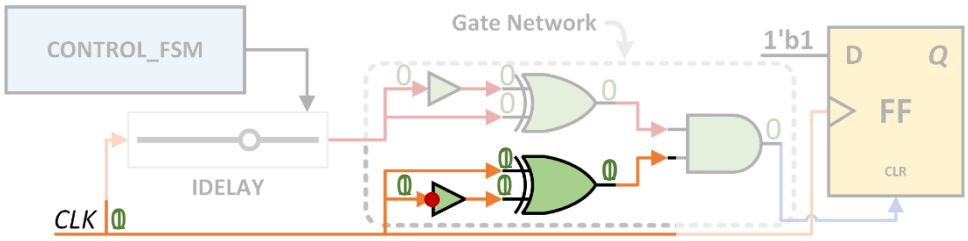
Outputs 1 if the inputs are different; 0 otherwise

THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations

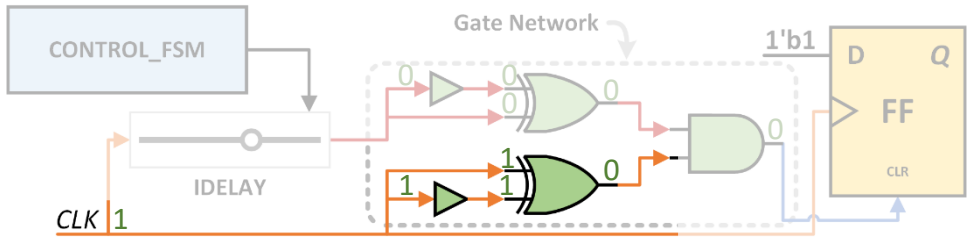


THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations

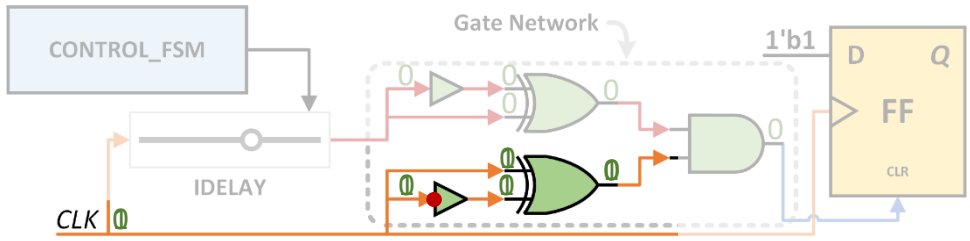


THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

Power to Pulse Width Modulation Sensor (PPWM)

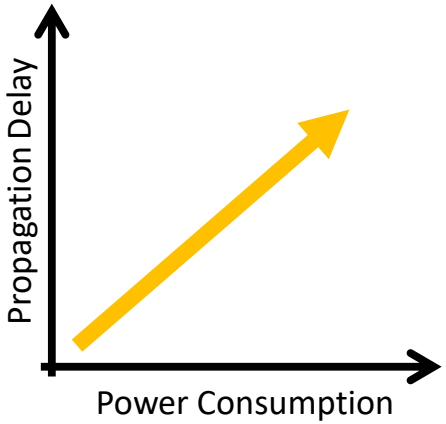
Capturing Power Variations



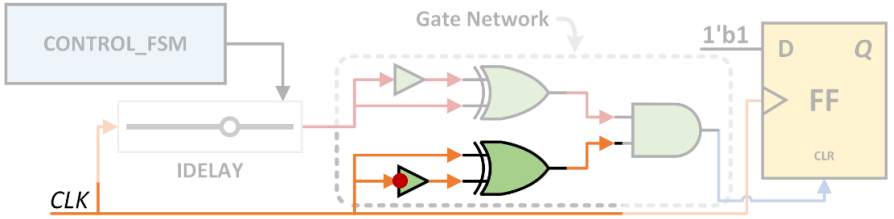
XOR Gate
Output

Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations

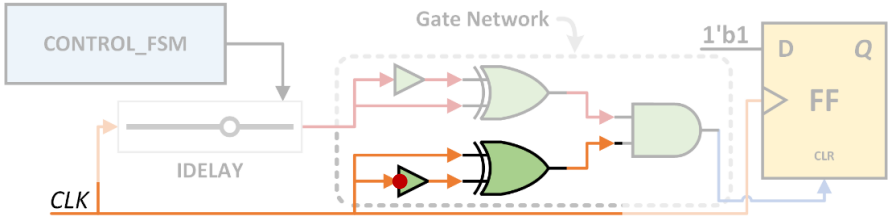


Low
Power
Consumption



Narrow
Pulse

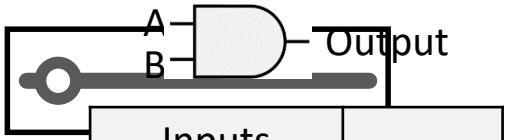
High
Power
Consumption



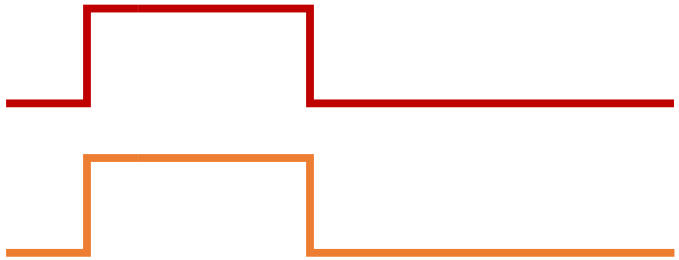
Wider
Pulse

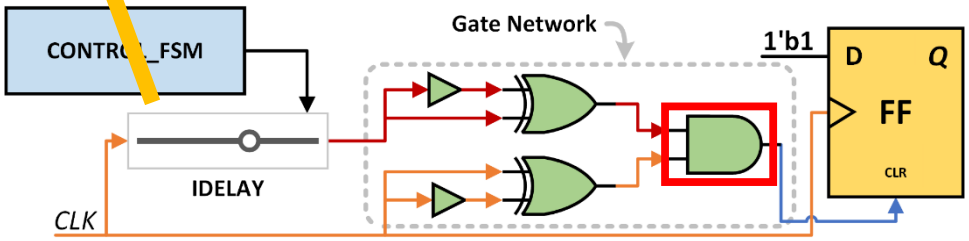
Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations



Inputs		Output
A	B	
0	0	0
0	1	0
1	0	0
1	1	1



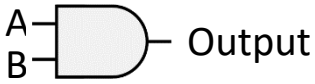


THE UNIVERSITY OF SYDNEY

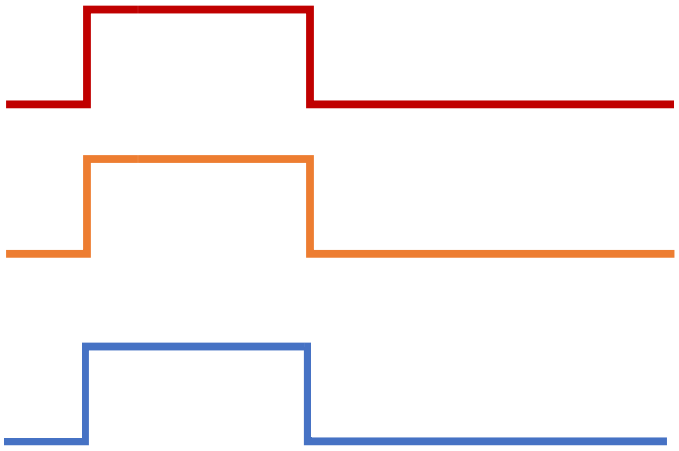
UNSW SYDNEY

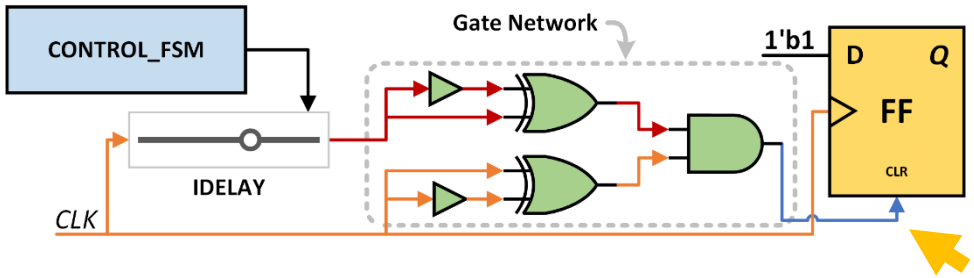
Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations



Inputs		Output
A	B	
0	0	0
0	1	0
1	0	0
1	1	1





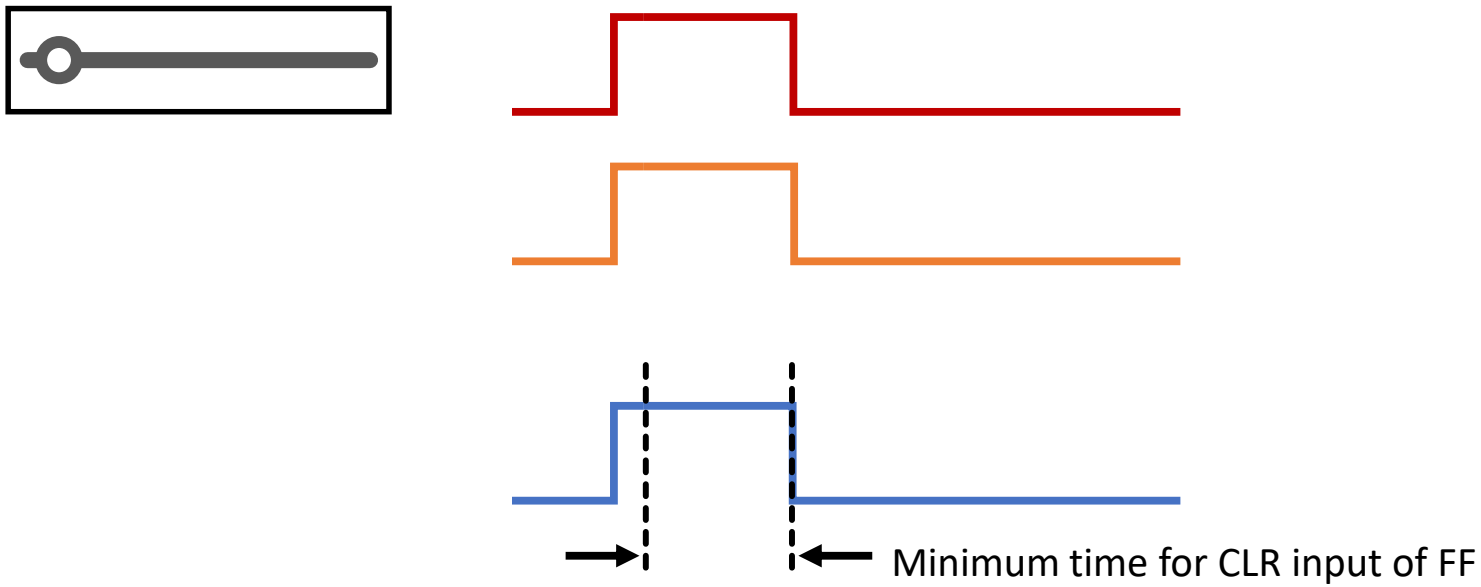
AND gate output is the CLR input of FF

THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

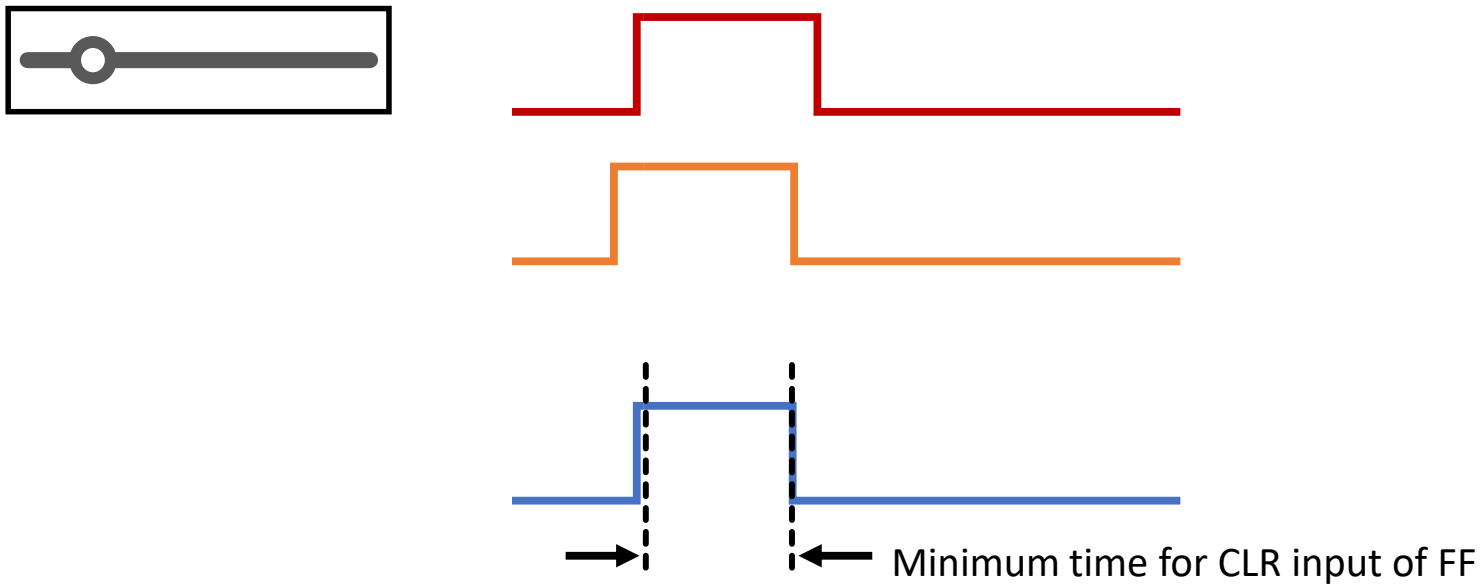
Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations



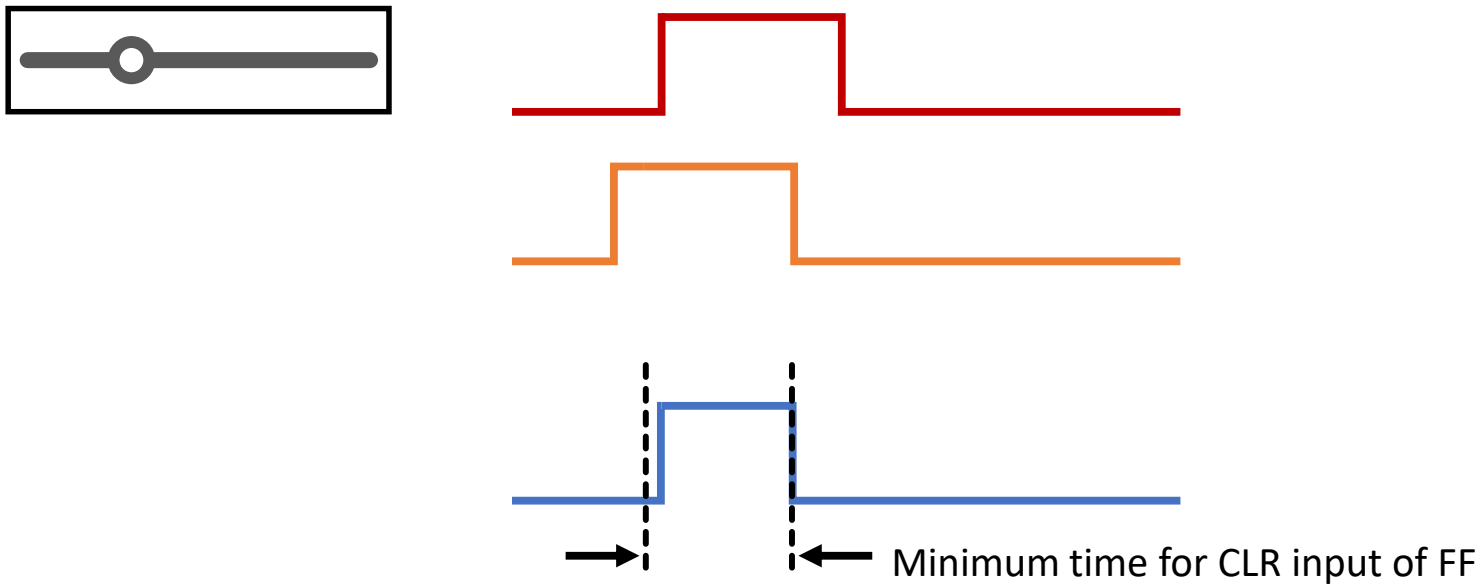
Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations



Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations

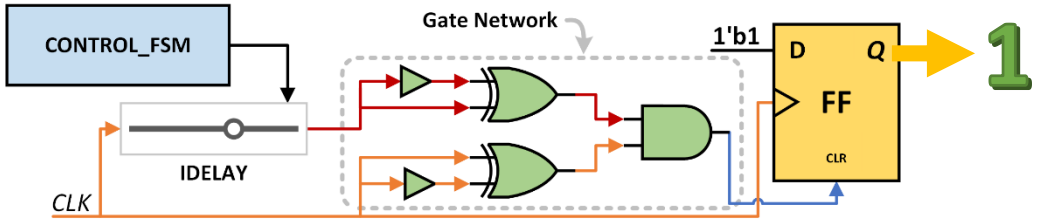


THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

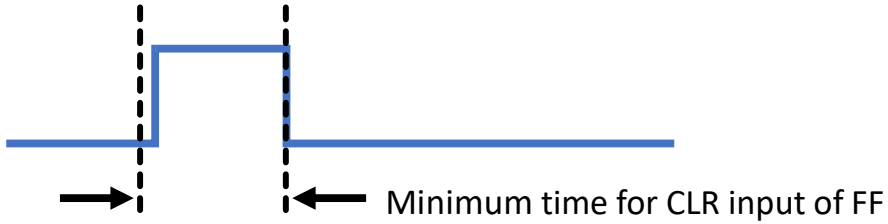
Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations



Low

Power Consumption

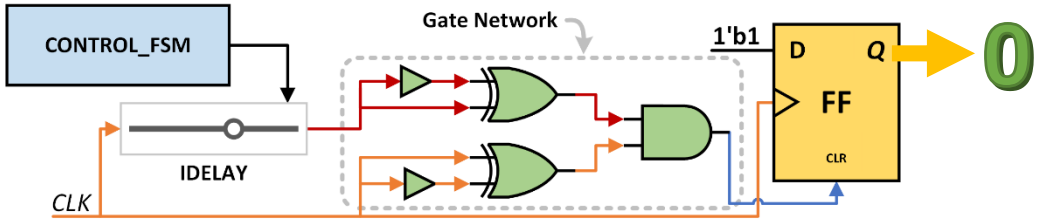


THE UNIVERSITY OF SYDNEY

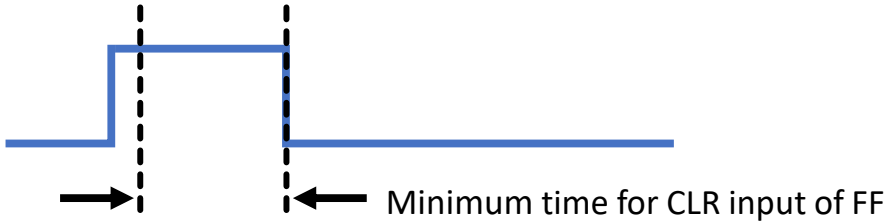
UNSW SYDNEY

Power to Pulse Width Modulation Sensor (PPWM)

Capturing Power Variations



High
Power
Consumption



THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

On-chip Sensors in the Literature - Summary

Sensor	TDC	RO	RDS	VITI	PPWM
Hardware Resources	↑	↑↑	↑	↓	↓
Bandwidth Resources	↑	↑↑	↑↑	↓	↓↓
Fully Autonomous Self-calibration	✗/✓	✗	✓	✓	✓
Free from Characteristic Features	✗	✗	✗	✓	✓

Current Challenges in On-chip Sensors

THE UNIVERSITY OF SYDNEY

UNSW SYDNEY

On-chip Sensors - Current Challenges

1. Investigating Novel On-chip Sensors

Any logic design susceptible to voltage fluctuations can be transformed to an on-chip sensor

Must pay attention to design considerations

Creating and modeling on-chip sensors need **a systematic approach**

Offers reliable means to **mathematically assess information leakage and efficacy of countermeasures**

Impact of manufacturer or FPGA architecture specific attributes on on-chip sensors are yet to be explored

Further exploration on enhancing side channel information recovery by **combining different on-chip sensors** may be beneficial

Can yield insights to improve on-chip sensors for legitimate FPGA monitoring purposes

On-chip Sensors - Current Challenges

2. On-chip Sensor Detection Framework

Identifying hidden on-chip sensors within hardware Intellectual Property (IP) is essential for countering RPA attacks

Can use **machine learning, Deep Neural Networks (DNN) and other neural network paradigms**

Functionally **similar to an antivirus software** used on a personal computer

On-chip Sensors - Current Challenges

3. Investigate RPA Attack Countermeasures

Countermeasures can be categorized into three groups

Device-specific: leverages unique hardware components to enhance resistance

Design-specific: protects specific algorithms or hardware designs

Generic: safeguards the entire FPGA, as a whole

On-chip Sensors - Current Challenges

3. Investigate RPA Attack Countermeasures

Can examine **design-specific "traditional" power analysis attacks countermeasures** such as MUTE-AES* and NORA+

Generic random clock execution techniques such as RFTC# and SCRIP‡ could be tested for efficacy against RPA attacks

These techniques may be less effective as on-chip sensor is within the FPGA as opposed to an oscilloscope which is external

More countermeasures tailored for RPA attacks needed to be devised to protect FPGA designs

* **J. Ambrose et al., "MUTE-AES: A multiprocessor architecture to prevent power analysis based side channel attack of the AES algorithm"**
+ **D. Jayasinghe et al., "NORA: Algorithmic Balancing without Pre-charge to Thwart Power Analysis Attacks"**
# **D. Jayasinghe et al., "RFTC: Runtime Frequency Tuning Countermeasure Using FPGA Dynamic Reconfiguration to Mitigate Power Analysis Attacks"**
‡ **D. Jayasinghe et al., "SCRIP: Secure Random Clock Execution on Soft Processor Systems to Mitigate Power-based Side Channel Attacks"**

On-chip Sensors - Current Challenges

4. Applicability of Novel On-chip Sensors in ASICs

TDCs*and ROs[+] are used in ASICs for power measurement

Deployment of newer on-chip sensor such as RDS, VITI and PPWM on ASICs is yet to be explored

Identifying the ability to deploy more compact on-chip sensors on ASICs is useful

Security evaluation of ASICs

Saving silicon real estate required for legitimate monitoring purposes

* **W. Roberts et al., "A Brief Introduction to Time-to-Digital and Digital-to-Time Converters"**

+ **A. Ferraiuolo et al., "Experimental Analysis of a Ring Oscillator Network for Hardware Trojan Detection in a 90nm ASIC"**

In this talk…

Remote power analysis (RPA) attacks

Design considerations of RPA attack specific on-chip sensors

On-chip sensors in the literature

Current challenges pertaining to on-chip sensors

It is time for your questions!

Thank you!