Characterizing Power Distribution Attacks in Multi-User FPGA Environments

George Provelengios, Daniel Holcomb, and Russell Tessier

Department of Electrical and Computer Engineering
University of Massachusetts Amherst

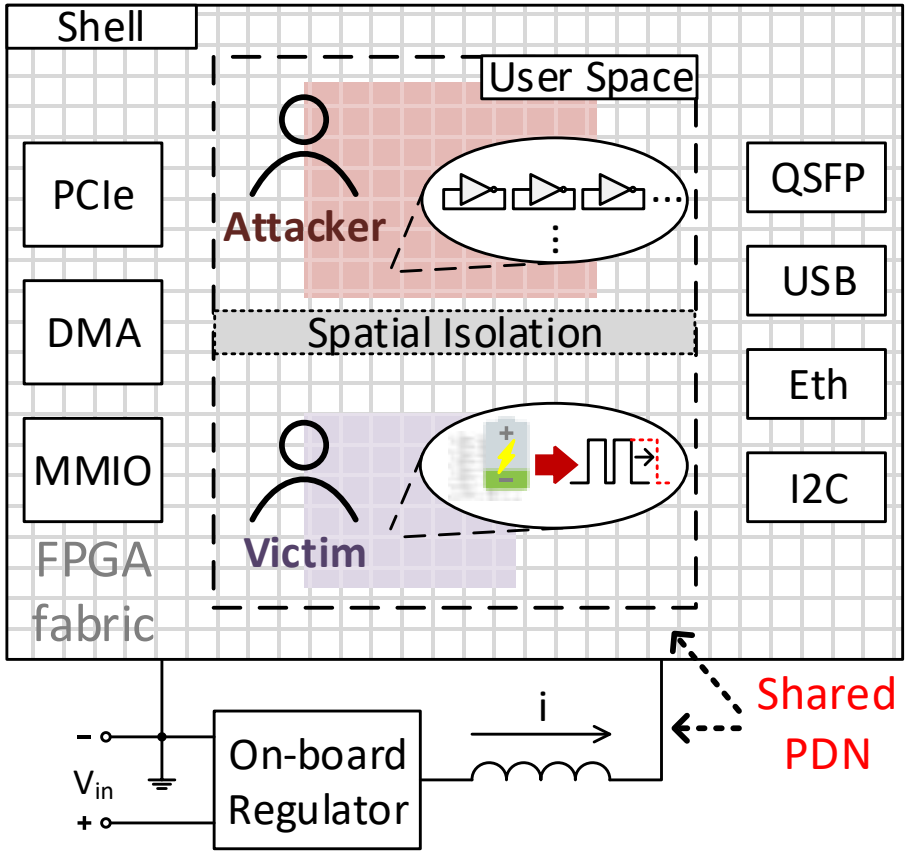
(Funded by a grand from Intel's Corporate Research Council)

Overview

- Two tenants are using simultaneously the device
- Tenant A (attacker) consumes power aggressively in an attempt to induce timing faults in tenant B (victim)

Threat model:

- ✓ Tenants are spatially isolated but share the FPGA power distribution network (PDN)
- ✓ Tenants do not have physical access to the board
- ✓ The tools used for interacting with the FPGA are secure

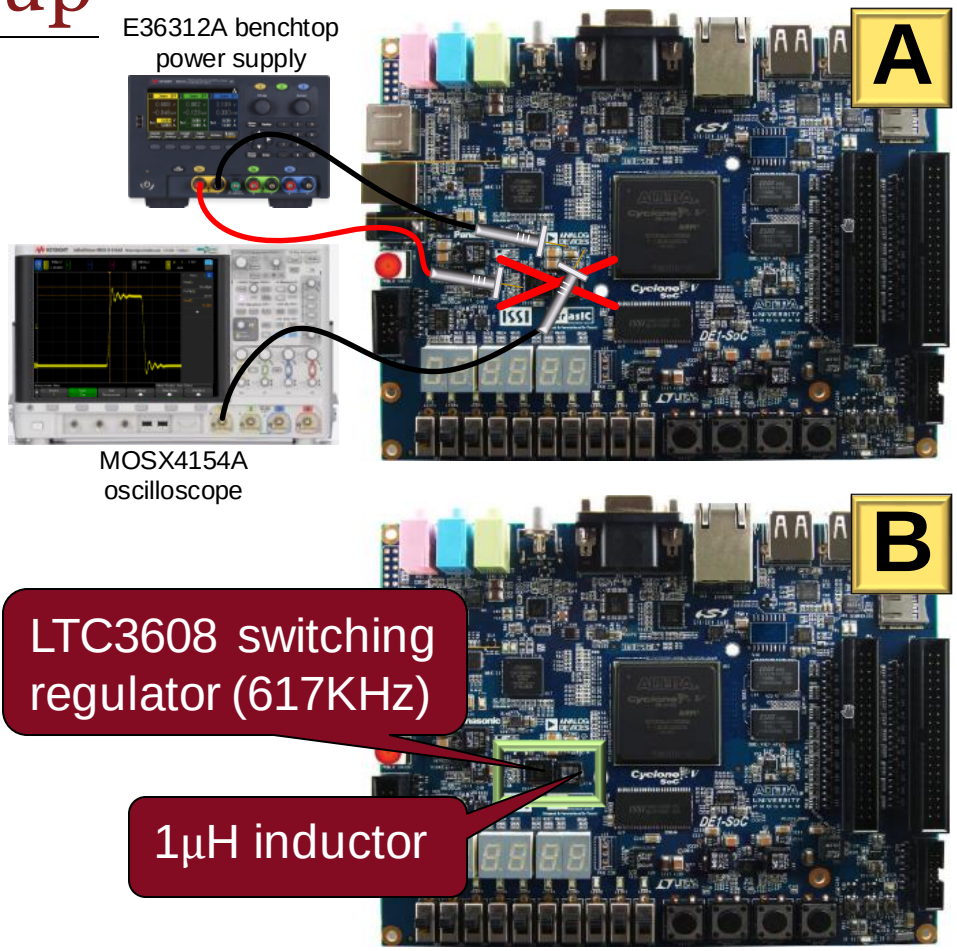


Contribution

- We investigate on-chip voltage attacks and specifically how their impact depends on:
  - Duration of voltage disruption
  - Consumed power by attacker
  - Distance between attacker & victim
- We evaluate the ability of power wasting circuits to induce timing faults to victim
- We examine the use of small on-chip voltage sensors to quickly identify the location of the attacker

Characterization platform and experimentation setup

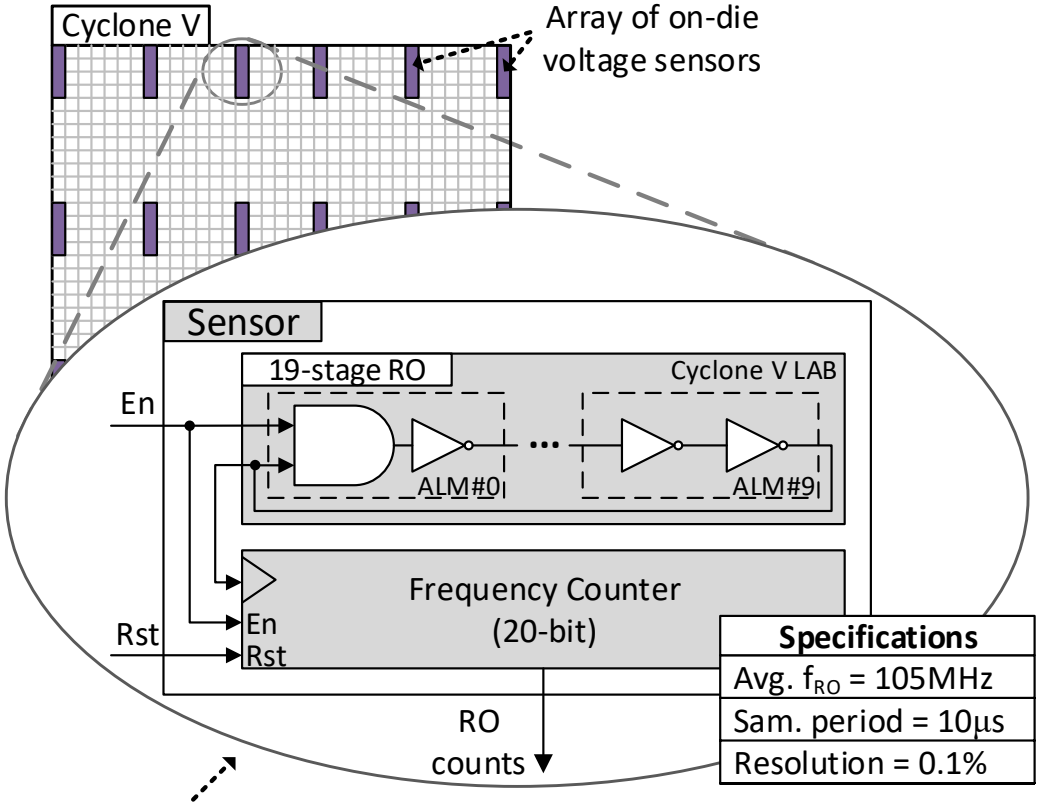
- Two DE1-SoC boards (Cyclone V FPGA)
  - A: for calibrating the sensors
  - B: for characterizing on-chip voltage attacks
- A benchtop power supply for controlling the input voltage
- An oscilloscope for measuring the on-board voltage (testpad VCC1P1)



Terasic DE1-SoC board - Cyclone V FPGA (28nm)

Voltage sensor architecture

- A regular rectangular grid of 46 sensors
- 19 inverting stages:
  - ✓ Meet timing constraints
  - ✓ Minimize local effects[1]
  - ✓ Fit in a single CV LAB
- Resolution: 1 part in 1000

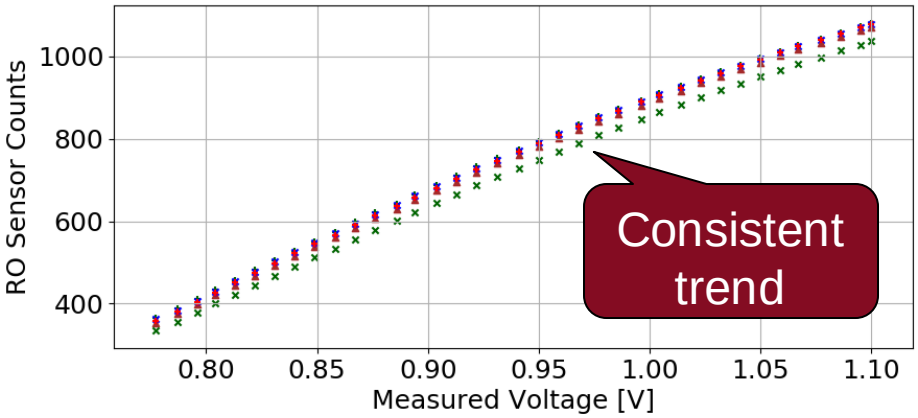


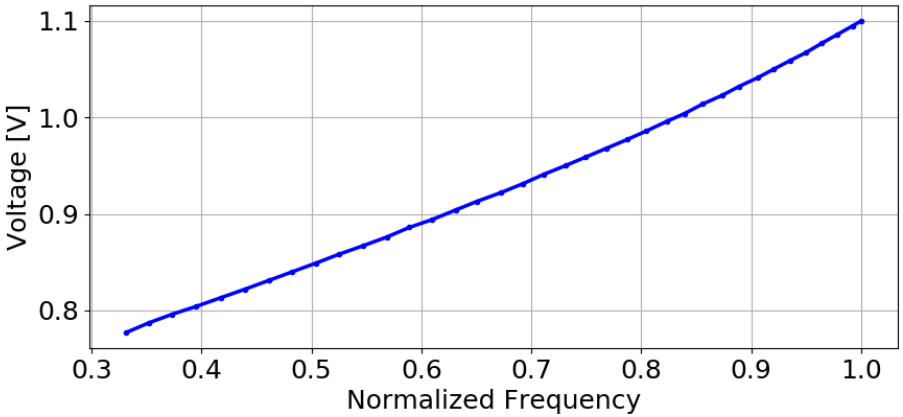
Controller reads and resets all the sensors simultaneously in every sampling period

[1] M. Barbareschi, G. Di Natale, and L. Torres, "Implementation and analysis of ring oscillator circuits on Xilinx FPGAs," in *Hardware Security and Trust.* N. Sklavos, R. Chaves, G. Di Natale, and F. Regazzoni, Eds. Springer, 2017, ch. 12, pp. 237-251

Sensor calibration

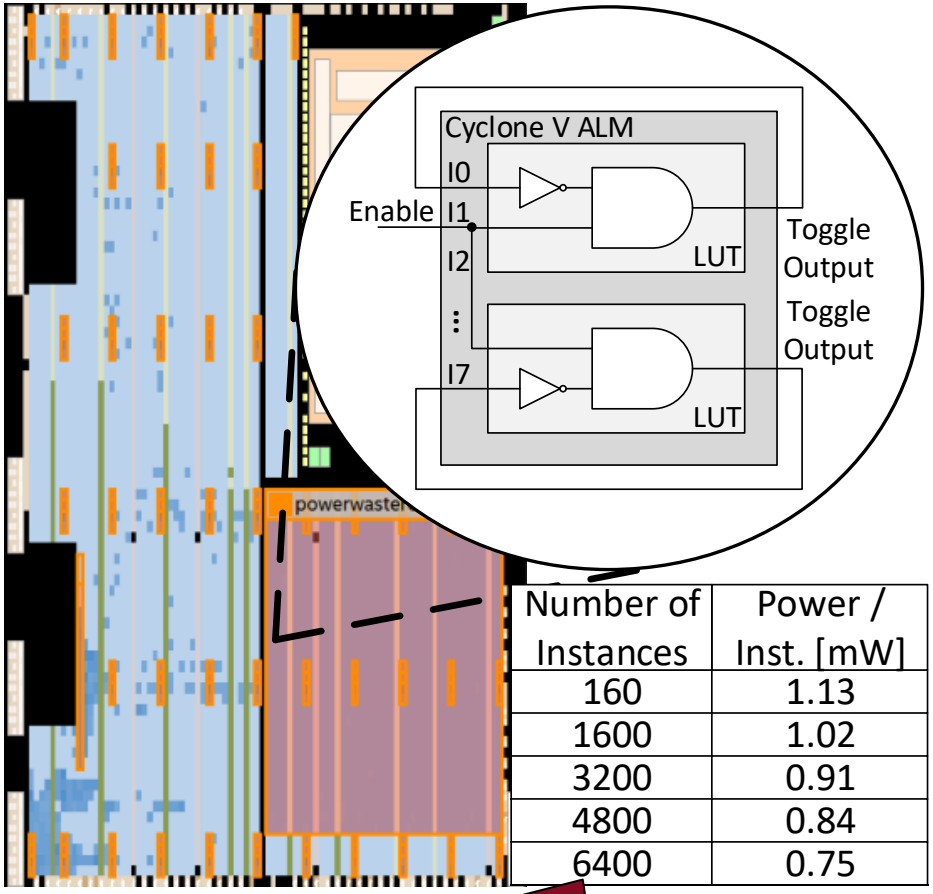
- To use ROs as on-chip voltage sensors:
  - Sweep the input voltage (780mV – 1.1V) and record:
    - ✓ Voltage at FPGA power pin
    - ✓ RO counts from on-chip sensors
- Minimize the power drawn by the FPGA during measurements





Attacker circuitry

- $P_{dyn} = C \times V_{DD}^2 \times f_{SW}$
- 1-stage ROs as power wasters
- In an area of 1,408 LABs (44x32) fit up to 12K PWs
- Placed uniformly at random locations in the attack area
- Power/instance is diminished as the number of PWs increases

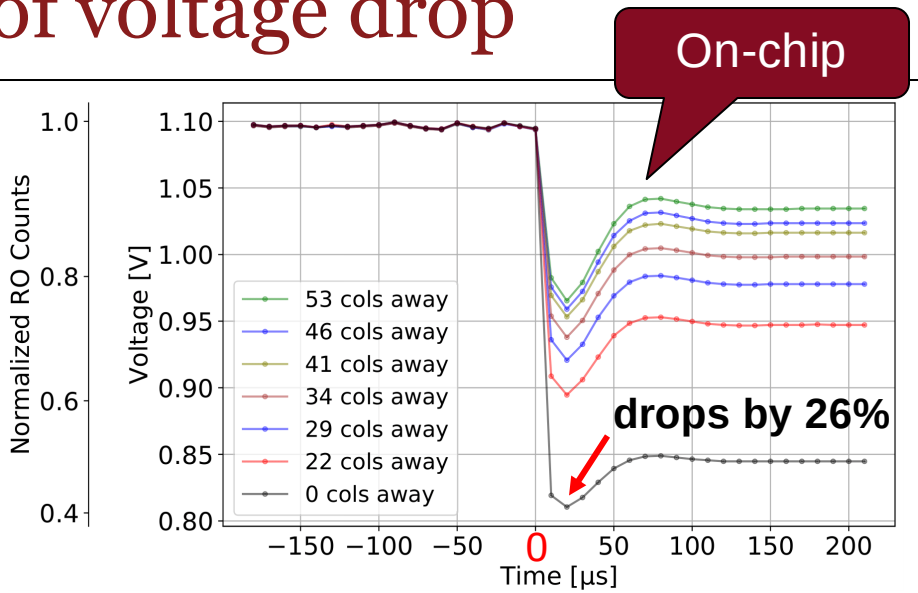


Number of Instances	Power / Inst. [mW]
160	1.13
1600	1.02
3200	0.91
4800	0.84
6400	0.75

Hit the 5A current limit of the E36312A benchtop supply

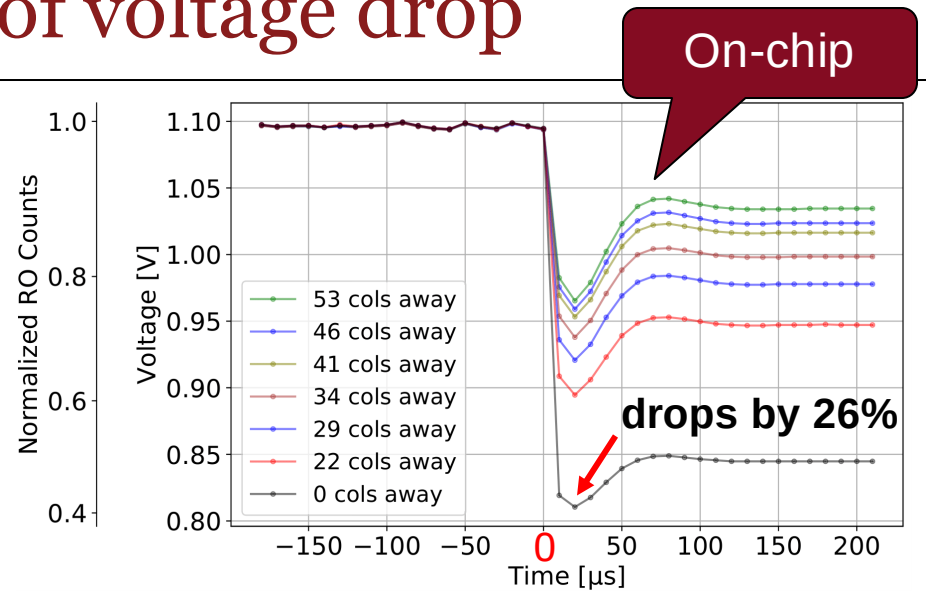
Physical characterization of voltage drop

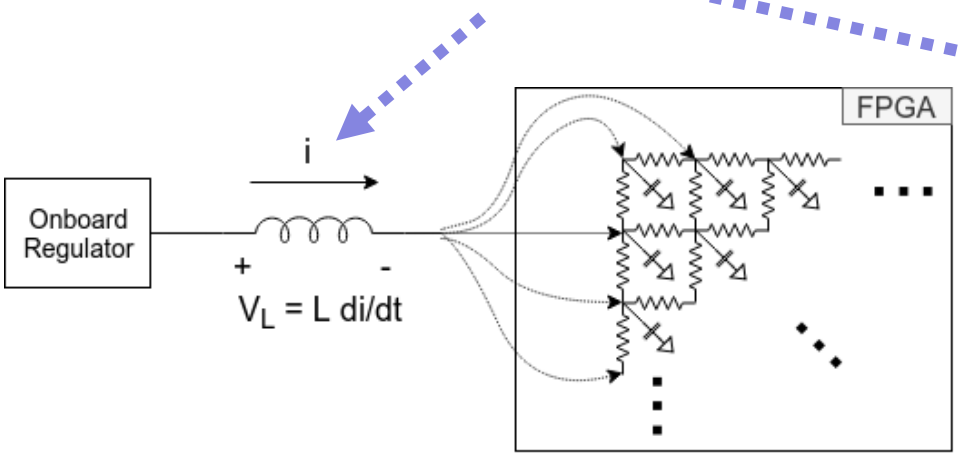
- Characterize disturbance as a function of:
  - disruption time
  - distance to center of PW (7 locations examined)

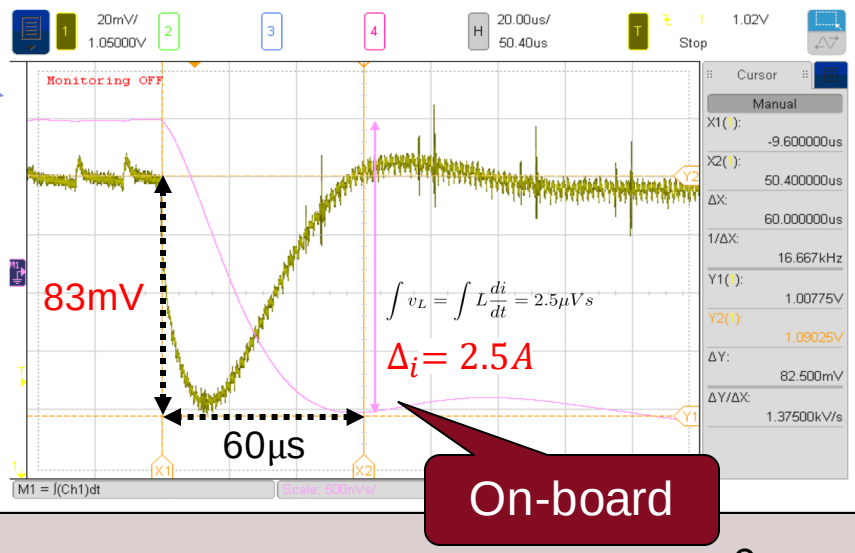


Physical characterization of voltage drop

- Characterize disturbance as a function of:
  - disruption time
  - distance to center of PW (7 locations examined)
- Voltage drop across the on-board inline inductor

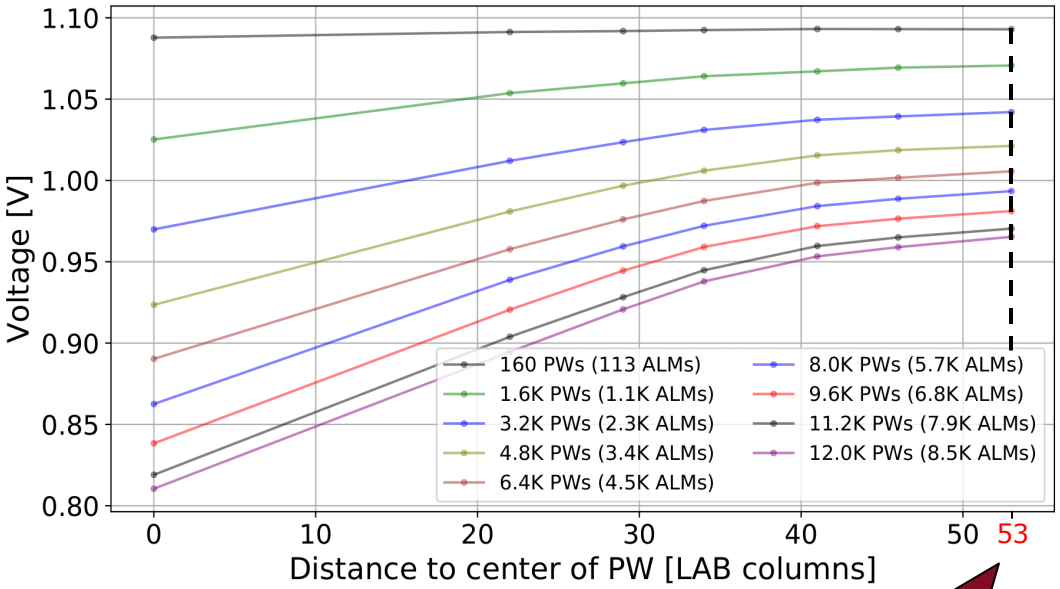






Intensity and distance

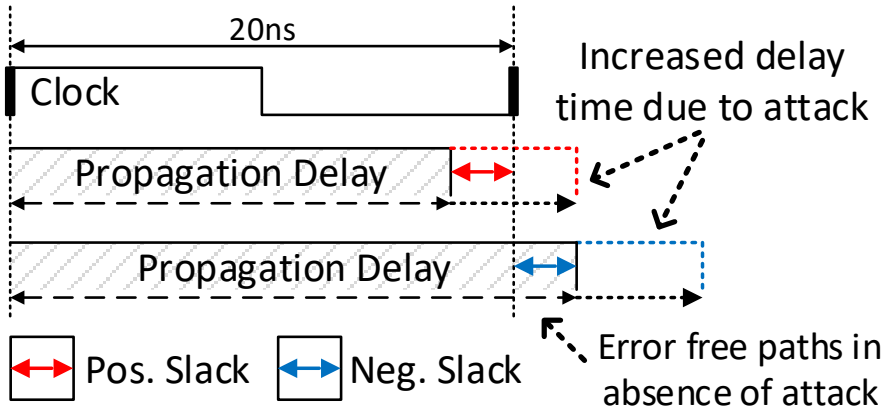
- Power consumed by attacker (160PWs -> 12K PWs)
- The 83mV voltage drop across the inductor impacts every part of the chip
- The victim will notice the drop regardless of its location on the chip

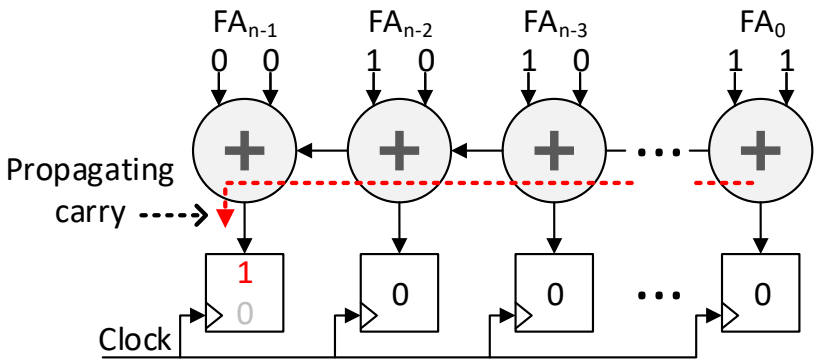


53 columns away the voltage drops to 967mV in the strongest attack

Characterizing timing faults

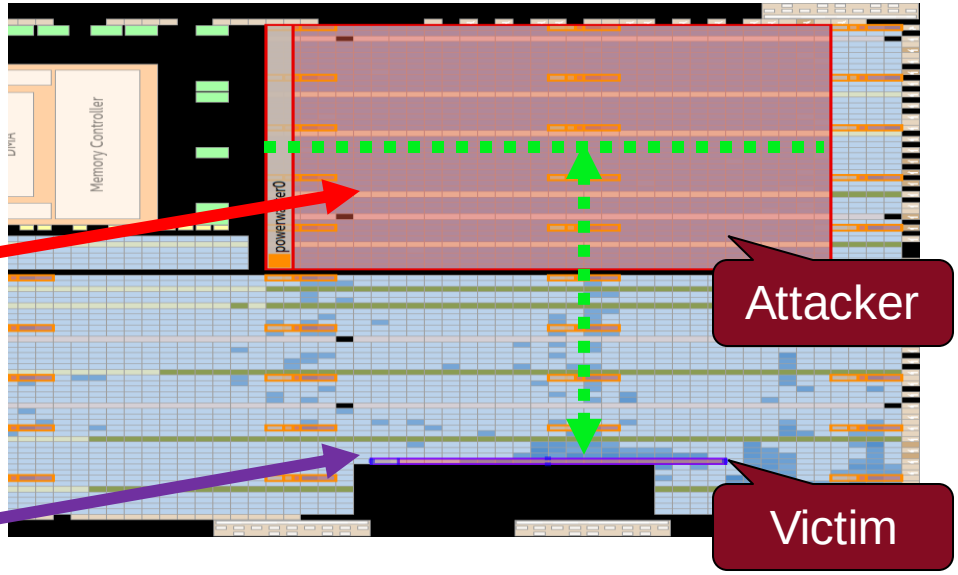
- Voltage drop causes delay of combinational logic to increase
- Wrong values captured if paths do not complete before capturing clock edge arrives
- Must overcome conservative timing models
- Use ripple carry adder as a representative test circuit can sensitize any desired path length

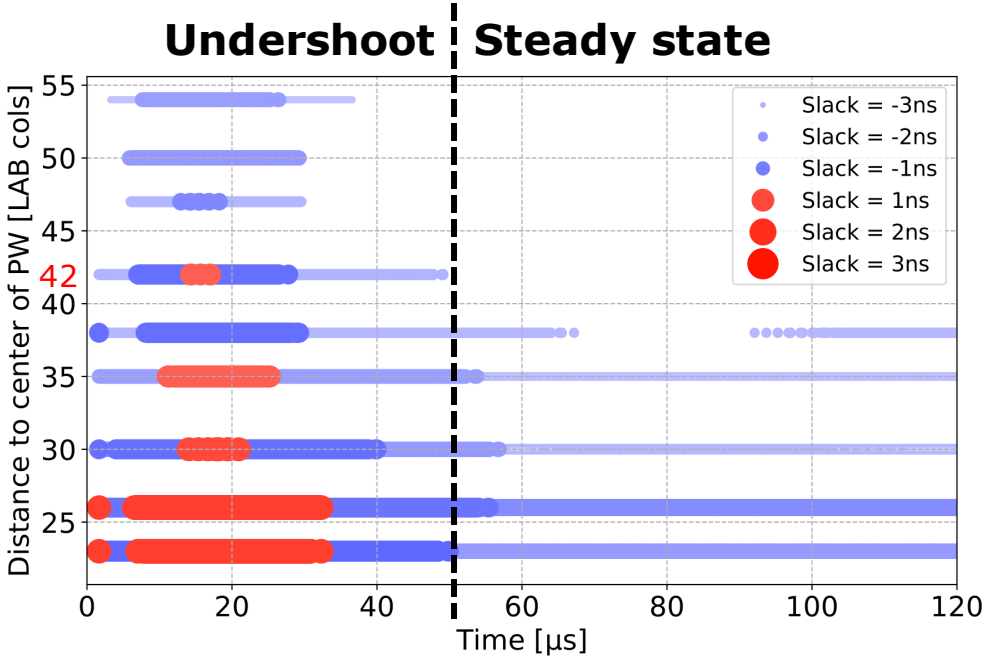




Inducing timing faults

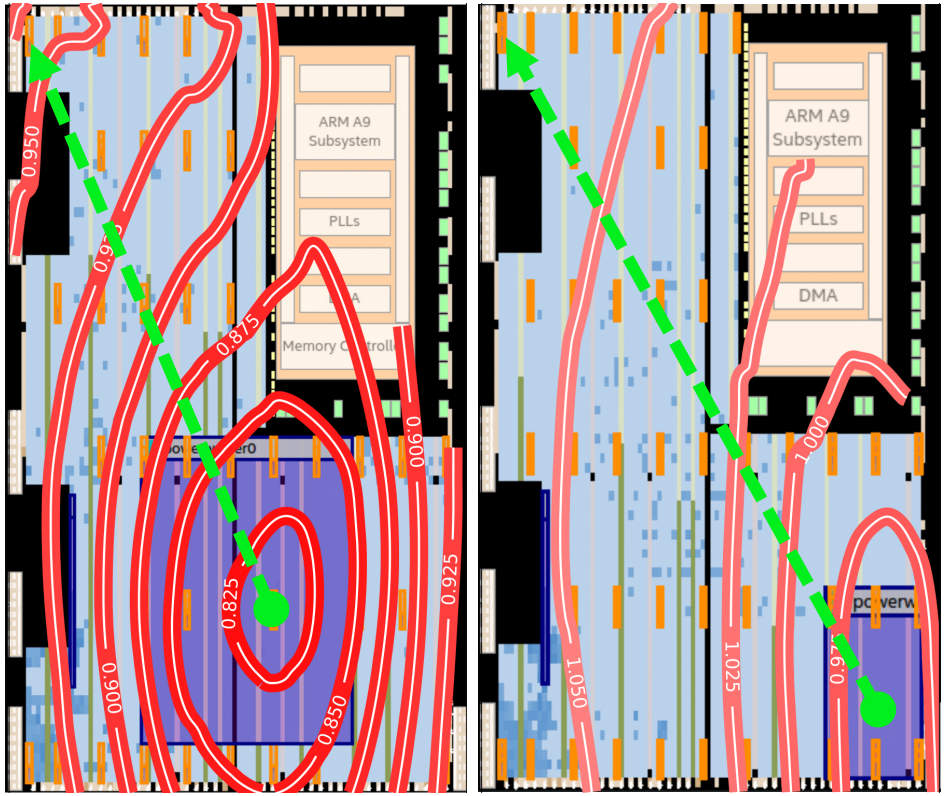
- 12K PWs randomly placed in an area of 1,408 LABs (44x32)
- Examine different distances in respect to attack center:
  - 22, 26, 30, 35, 38, 42, 47, 50, and 54 LAB columns away
  - Sensitize different path lengths: 49, 54, 59, 64, 69, and 74
- Faults occurred even in 42 columns away





Mapping the on-chip voltage drop

- Using 46 on-chip sensors for deriving the voltage contours of the chip
- Varying the magnitude of disturbance and location of attacker
- Center of attack:
  - 12K PWs: 825mV
  - 3.2K PWs: 975mV
- Farthest corner of the chip:
  - 12K PWs: 975mV
  - 3.2K PWs: 1.050V

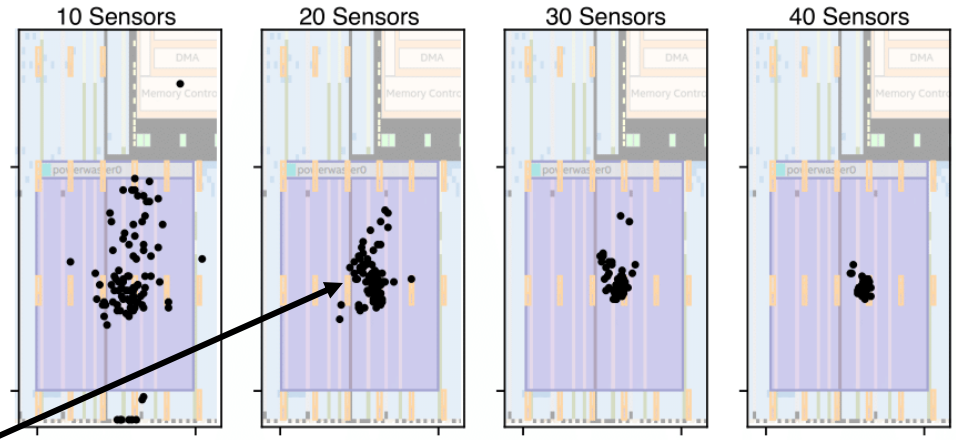


(A) 12K power waster attack

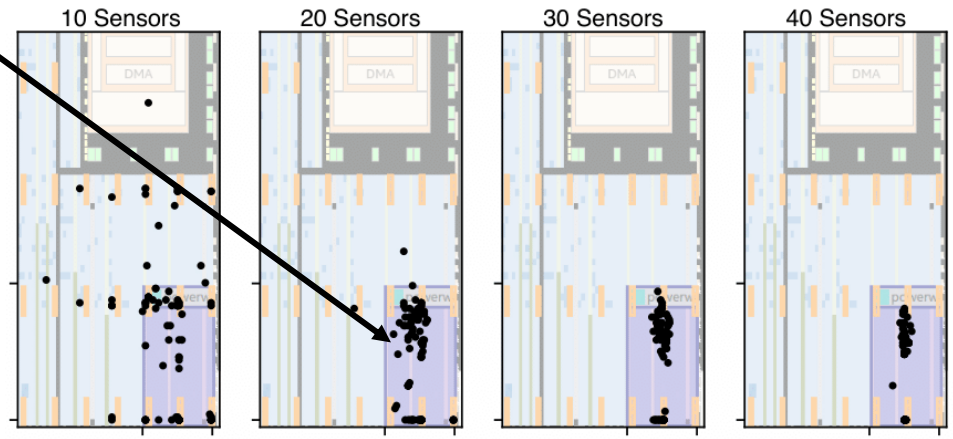
(B) 3.2K power waster attack

Locating the attack area

- The disturbance of the shared PDN reveals the location of the attacker
- Evaluate how many sensors required to find its location
- 20 sensors are sufficient to identify the attacker



(A) 12K power waster attack



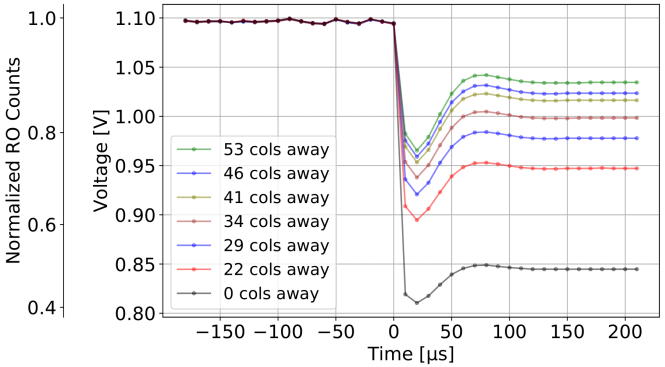
(B) 3.2K power waster attack

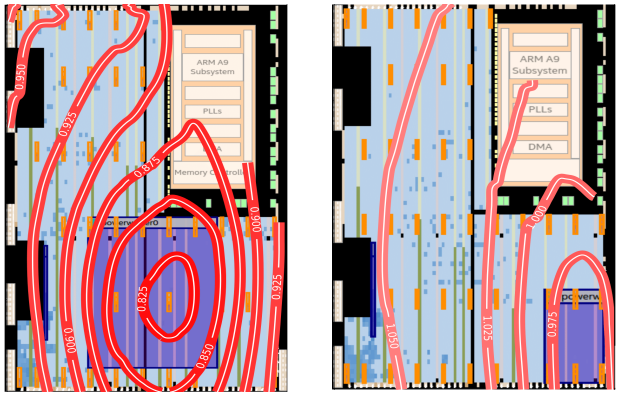
Resource utilization: Cyclone V 5CSEMA5F31C6

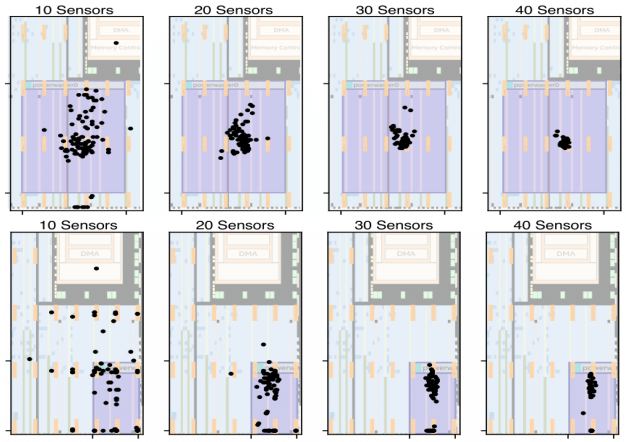
Num. RO Sensors	ALMs (Avail.:32,070)	Flip-flops (Avail.: 128,280)
10	390 (1.2%)	200 (<1%)
20	780 (2.4%)	400 (<1%)
30	1,170 (3.6%)	600 (<1%)
40	1,560 (4.9%)	800 (<1%)
46	1,794 (5.6%)	920 (<1%)
Controller	430 (1.3%)	111 (<1%)

Summary

- Using a small number of RO-based on-chip sensors we characterized on-chip FPGA voltage attacks
- Combining *iR* voltage drop with drop caused by inductance can be used to attack circuits far from the power wasting area
- Spatial isolation between tenants is insufficient for protecting against PDN attacks
- A malicious tenant cannot mask its identity and can be located with less than 5% of FPGA logic







Thank You

Questions?

- Using a small number of RO-based on-chip sensors we characterized on-chip FPGA voltage attacks
- Combining *iR* voltage drop with drop caused by inductance can be used to attack circuits far from the power wasting area
- Spatial isolation between tenants is insufficient for protecting against PDN attacks
- A malicious tenant cannot mask its identity and can be located with less than 5% of FPGA logic