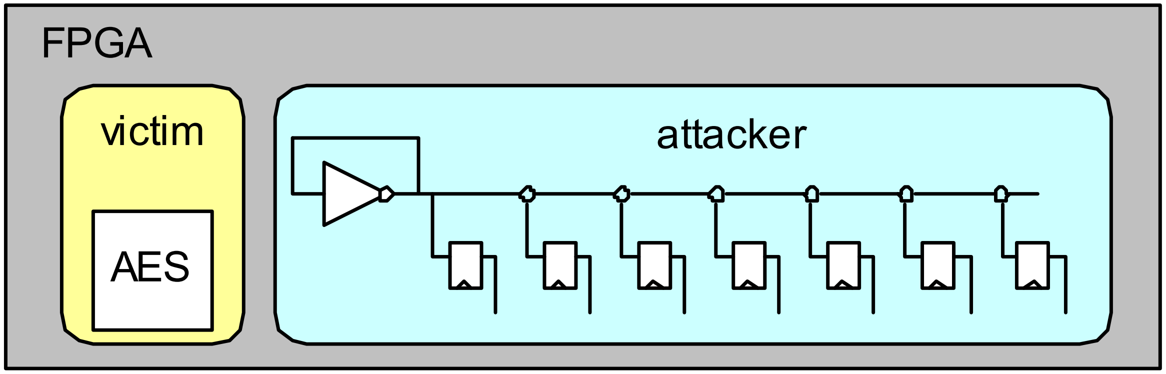
rFAS
–
reconfigurable FPGA Accelerator Sandboxing

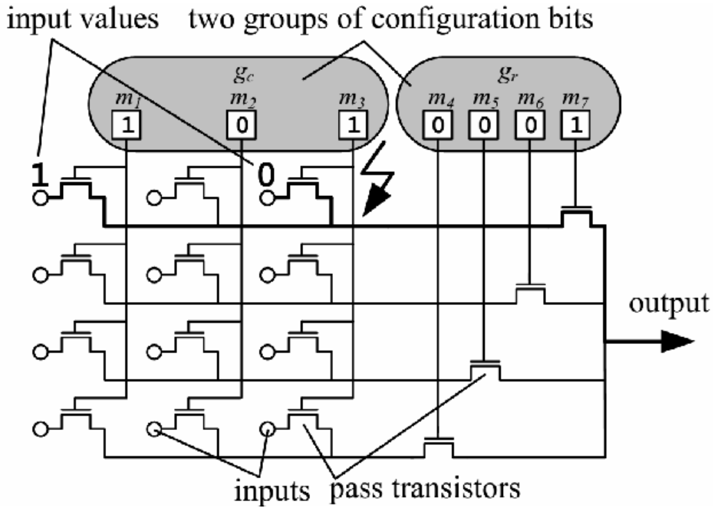
Dirk Koch, Tuan La, Khoa Pham
{dirk.koch,tuan.la,khoa.pham@manchester.ac.uk)
Depatment of Computer Science
The University of Manchester

rFAS - FPGA Accelerator Sandboxing

FPGAs have a huge surface of attack!

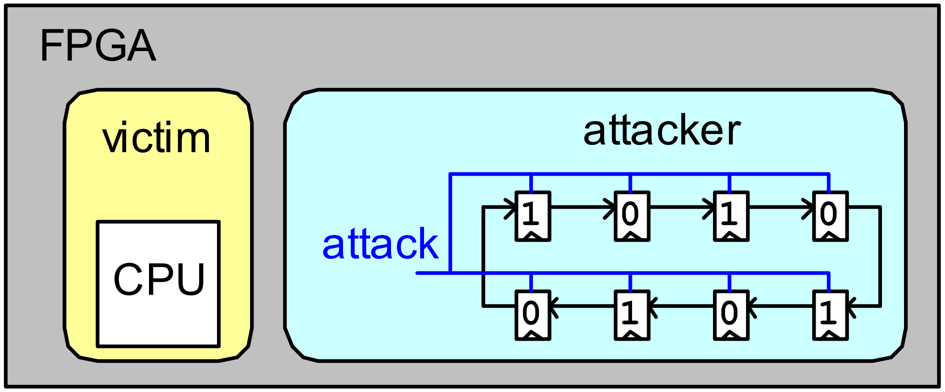
- **Remote DPA attacks**



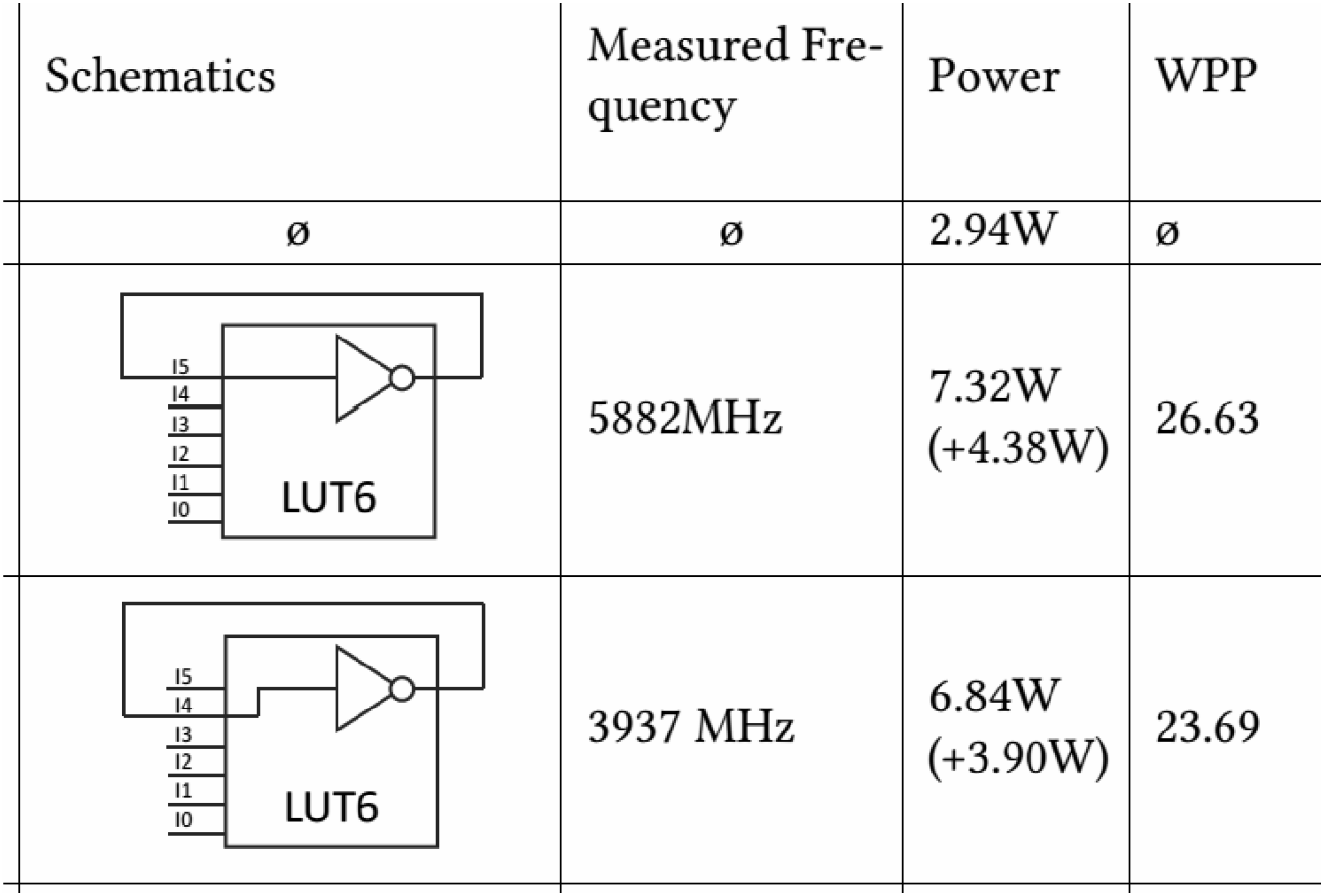


- **Destroy or age FPGA hardware through corrupted bitstream (we have shown that!)**

- **Power hammering attacks**



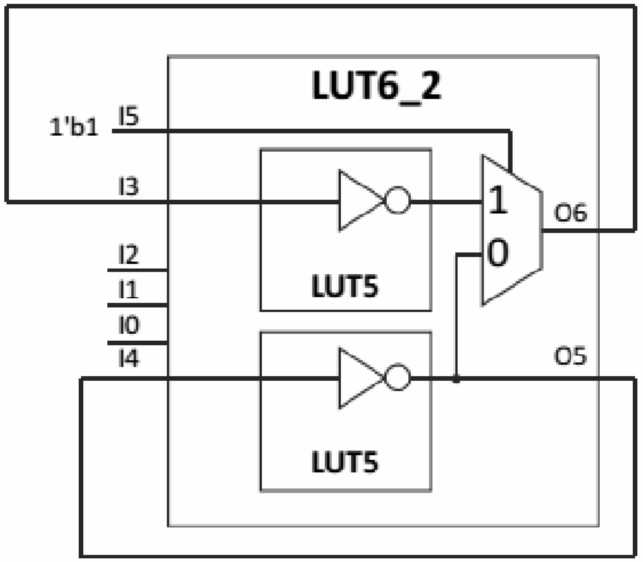
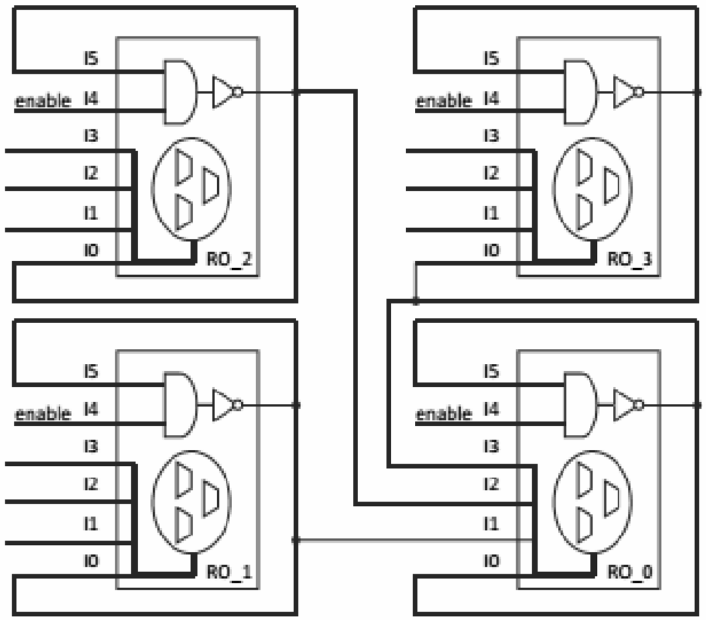
Study on Ring-Oscillators

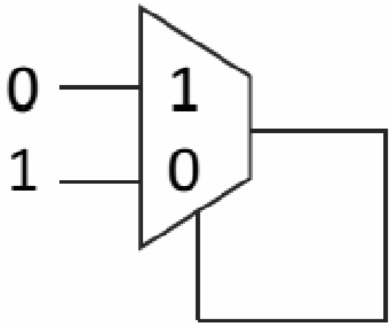
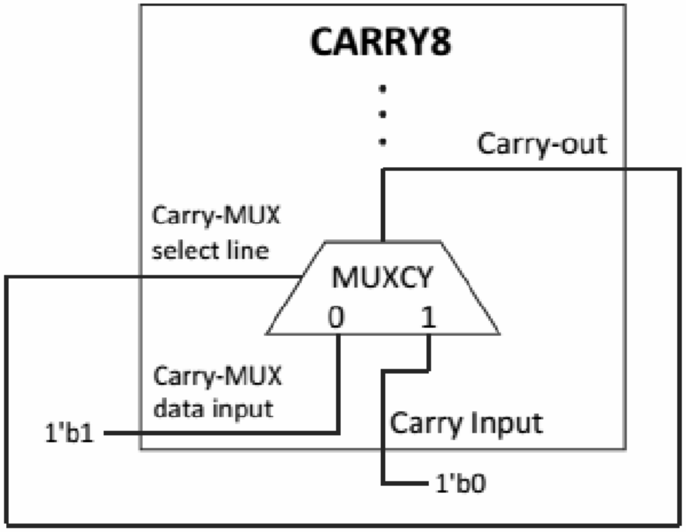
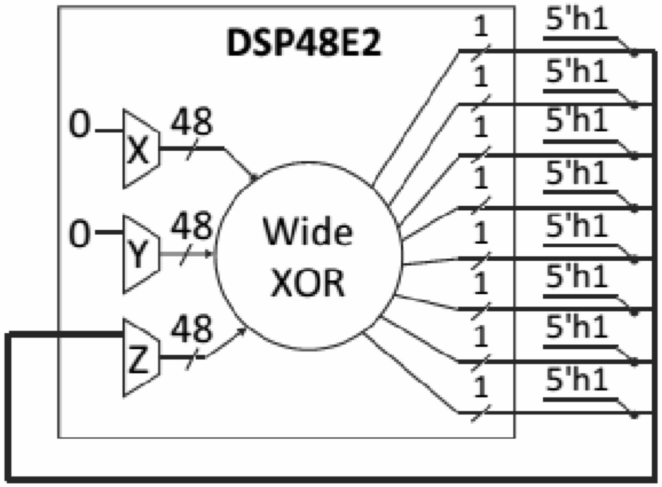


Schematics	Measured Frequency	Power	WPP
ø	ø	2.94W	ø
	5882MHz	7.32W (+4.38W)	26.63
	3937 MHz	6.84W (+3.90W)	23.69

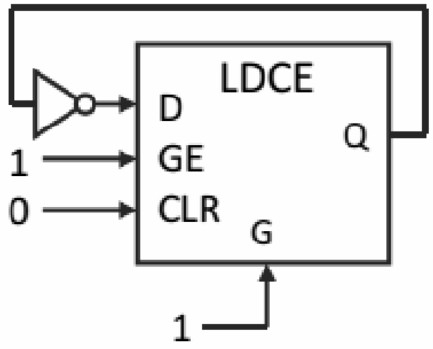
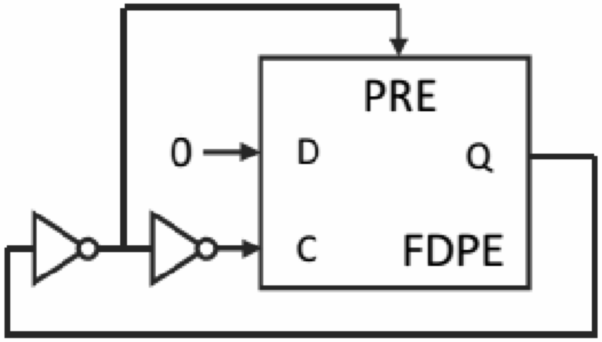
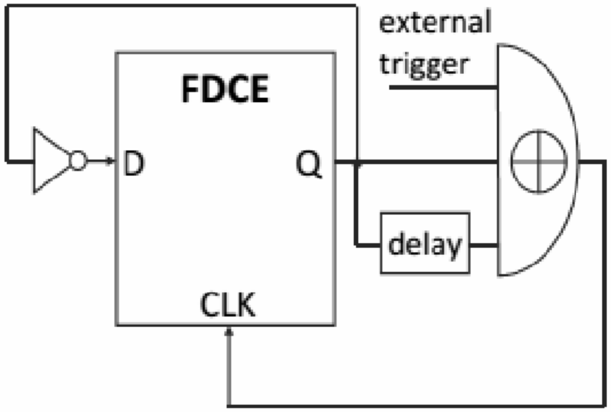
I5
I4
I3
I2
I1
I0
LUT6
I5
I4
I3
I2
I1
I0
LUT6

Study on Ring-Oscillators

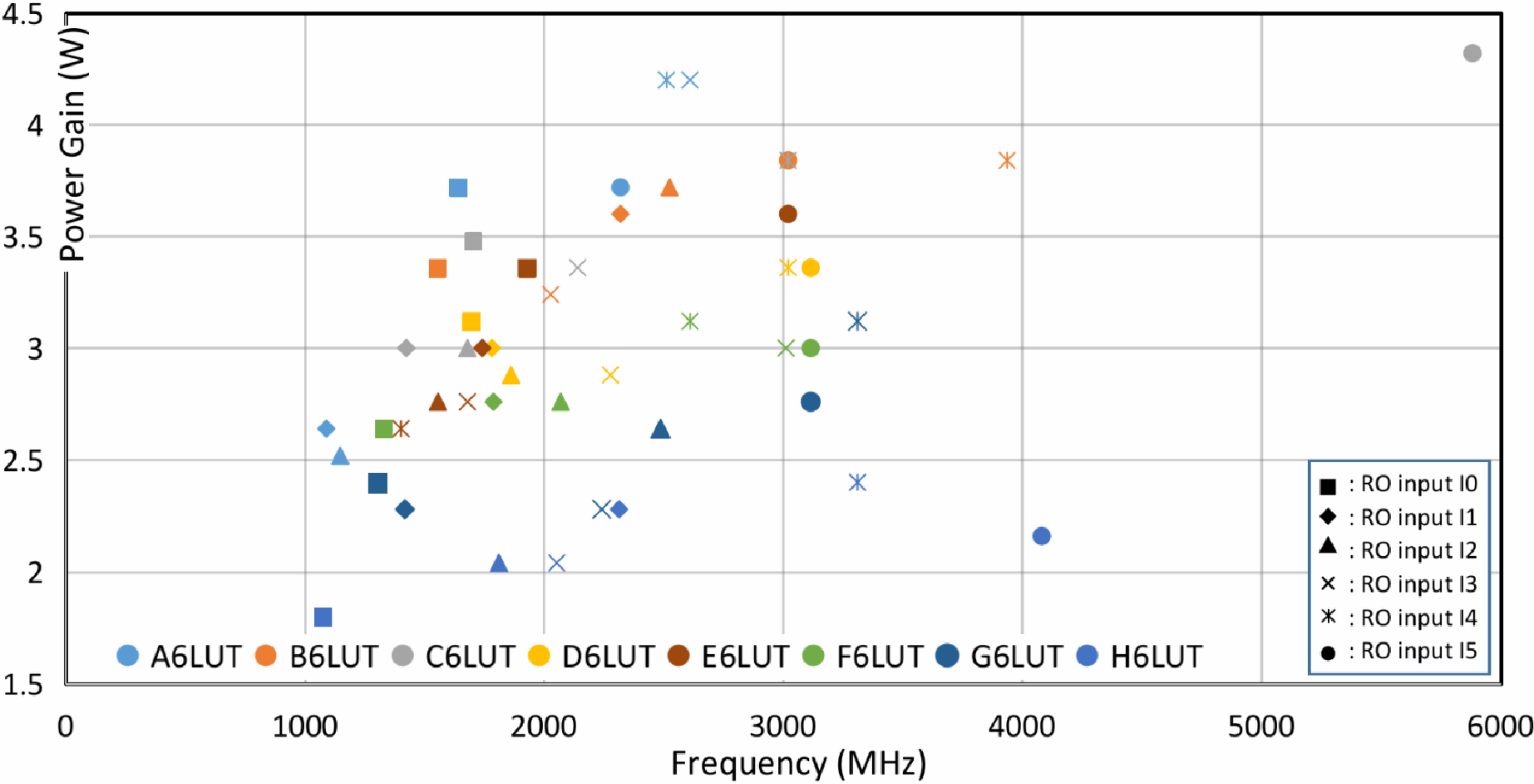
	O5: 1235MHz O6: 2439MHz	8.04W (+5.10W)	31.00
	1779MHz	9.61W (+6.66W)	40.54

	1681MHz	4.04W (+1.10W)	1.67
 CARRY8 Carry-out Carry-MUX select line MUXCY 0 1 Carry-MUX data input 1'b1 Carry Input 1'b0	1109MHz	5.14W (+2.19W)	1.67
 DSP48E2 0 X 48 0 Y 48 Z 48 Wide XOR 1 5'h1	585MHz	4.53W (+1.59W)	0.27

Study on Ring-Oscillators

	1706MHz	5.14W (+2.19W)	13.35
	555MHz	5.26W (+2.32W)	7.05
	481MHz	8.05W (+5.10W)	10.35

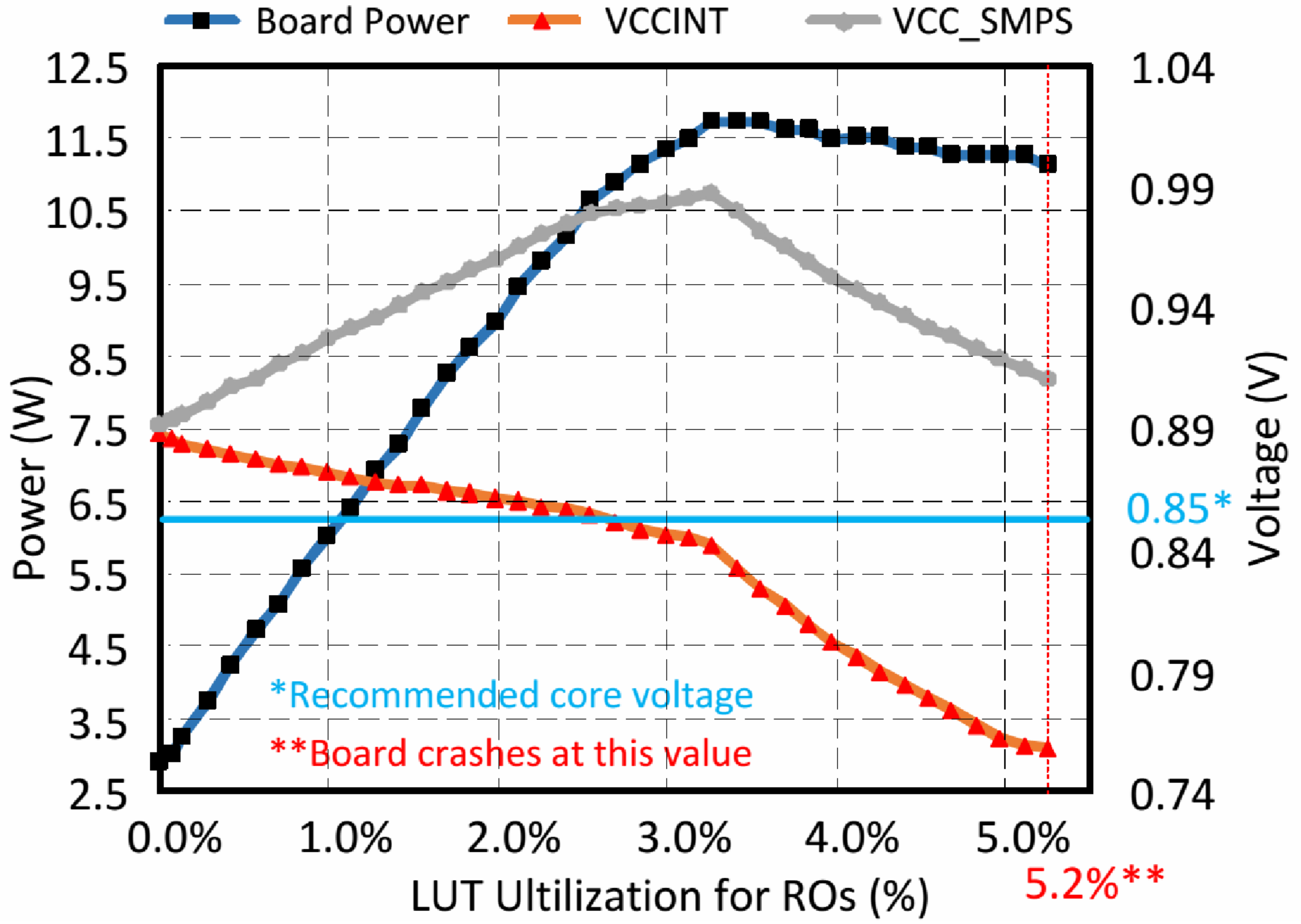
Study on Ring-Oscillators



Experiment: 2K LUTs on a Ultra96 Board (Xilinx Zynq UltraScale+)

- **The fastest oscillators do not necessary burn most power**
- **Fast oscillators are better for power analysis attacks**

Study on Ring-Oscillators



Study on Ring-Oscillators

We carried out first experiments on an Alveo U200*

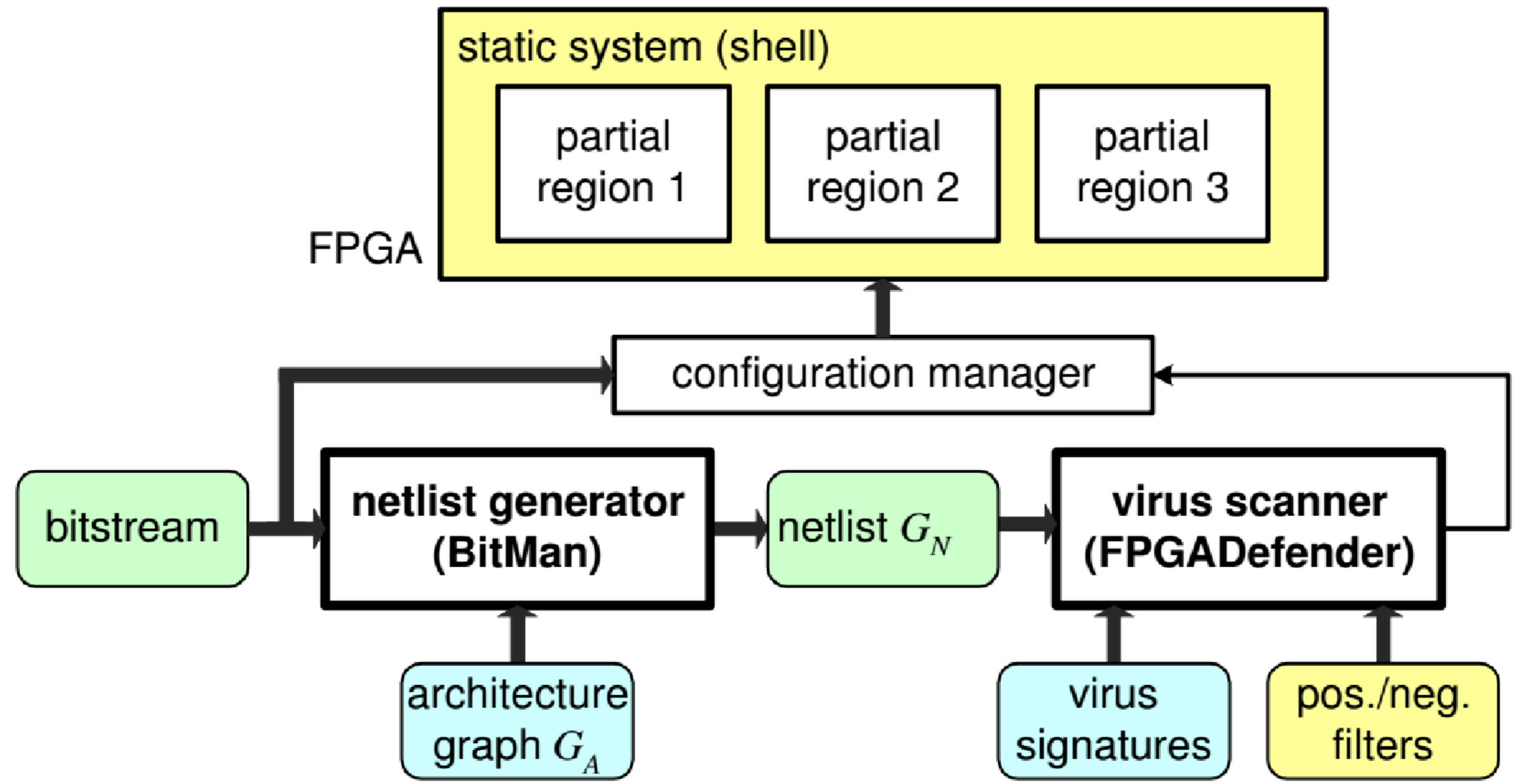
datacenter FPGA → 10% LUTs draw 350W !!!

(* same specification as used in Amazon F1)

- **x KW Power-hammering potential!**
- **Many of our circuits are not spotted by the vendor tools!**
  (Design Rule Checks (DRCs) & power analyzer tool)
- **We tested power-hammering attacks on Amazon F1 instances:**

  → can be deployed!
- **Oscillators allow power analysis attacks**
  (finger printing (PUFs), temperature, attack triggers, …

FPGADefender Virus Scanning for FPGAs



- **Detects probably any kind of self-oscillating circuits**
- **Scans bitstream encoding (short circuits), high fan-out nets, wire tapping, module bounding boxes (all at bitstream level)**
- **more to come …**

31st IEEE ASAP 2020

July 6-8, 2020

Manchester, UK

https://asap2020.cs.manchester.ac.uk/

rFAS - FPGA Accelerator Sandboxing

Major outcome:

FPGADefender

(spinoff???)

People:

Tuan Minh La	{tuan.la@postgrad.manchester.ac.uk}
Khoa Dang Pham	{khoa.pham@manchester.ac.uk}
Kaspar Matas	{kaspar.matas@manchester.ac.uk}
Nikola Grunchevski	{nikola.grunchevski@manchester.ac.uk}
Dirk Koch	{dirk.koch@manchester.ac.uk}