NANYANG TECHNOLOGICAL UNIVERSITY

pace
Physical Analysis and Cryptographic Engineering

An FPGA Compatible PLL-Based Sensor Against Fault Injection Attacks

Wei He[1], Jakub Breier[1], Shivam Bhasin[1],
Noriyuki Miura[2], Makoto Nagata[2]

[1]Temasek Labortaries, Nanyang Technological University, Singapore
[2]Graduate School of Informatics, Kobe University, Japan

ASP DAC 2017, Chiba, Japan.
Jan 17, 2017.

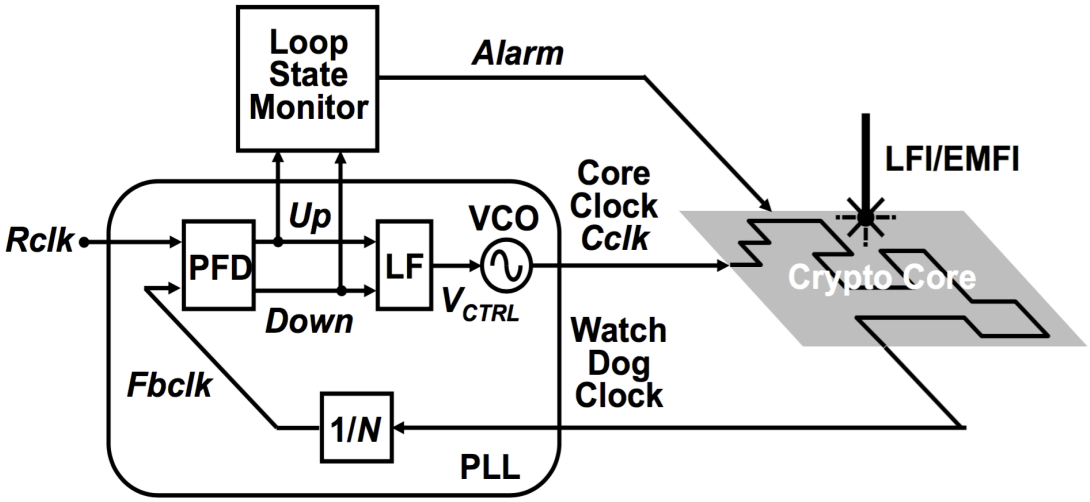
Presentation ID: 1S-18

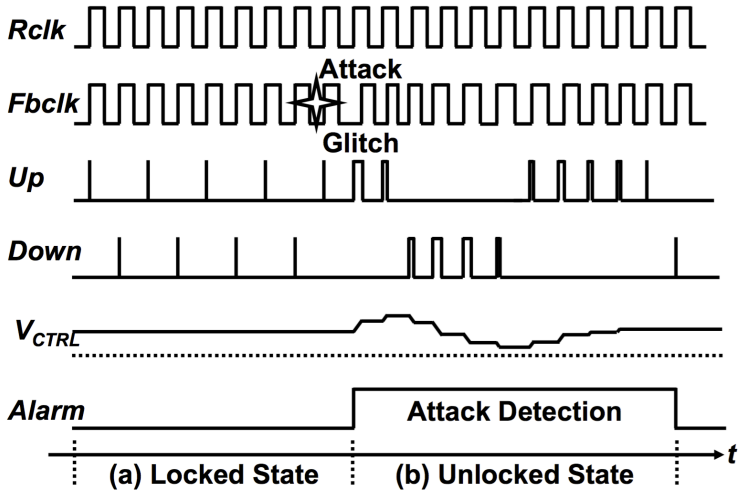
CONTEXT

- Fault Injection Attack (FIA) exploits the intentionally triggered faulty data or physical behaviors from the target devices, in order to extract confidential information about internals.
- Common injection methods are classified: **Global and Local**
- **Global:** Low-cost, easy to implement, low precision (clock tampering, voltage glitch, underpowering, temperature)
- **Local:** Precise and powerful, need expensive equipment, need high expertise (laser, electromagnetic (EM) disturbance)
- We propose a **Phased Locked Loop (PLL) and Ring Oscillator (RO) based sensor capable of detecting Laser and EM.**

LFI/EMFI Sensor: Principle

- Watchdog Ring Oscillator (WRO) senses instantaneous energy injected by Laser or EM.
- The PLL monitors the stability of WRO and reports injection by the "**LOCKED**" output





- WRO routed over sensitive circuit
- **Overheads**
  - Area : 1 PLL + 1 LUT (for WRO), Performance: Nil

Key results

- A **100% fault detection** for EM Fault injection with a huge security margin (Min. Injection Power − Min. Detection Power) of **19 dBm**
- A **92.82% detection rate** with laser injection and a low **failure rate 0.94%** (undetected injections). The security margin is 27% laser power.
- Tested on Virtex-5 and Spartan-6 FPGA from Xilinx.
- Requirement of PLL block can be a limiting factor in low-resource IoT devices.

Thanks for your attention!