Ring-Oscillator based power side channel attack in FPGAs

The University of Manchester

Tuan Minh La, Michael Yonli, Khoa Dang Pham, Dirk Koch

Email: tuan.la@postgrad.manchester.ac.uk, michael.yonli@student.manchester.ac.uk, {khoa.pham, dirk.koch}@manchester.ac.uk

INTRODUCTION

- Security threats in FPGAs are increasing rapidly along with an upward trend of using FPGAs in data centres for cloud computing.
- This work aims at power side-channel attacks using ring oscillators (RO) in latest Xilinx UltraScale+ FPGAs.

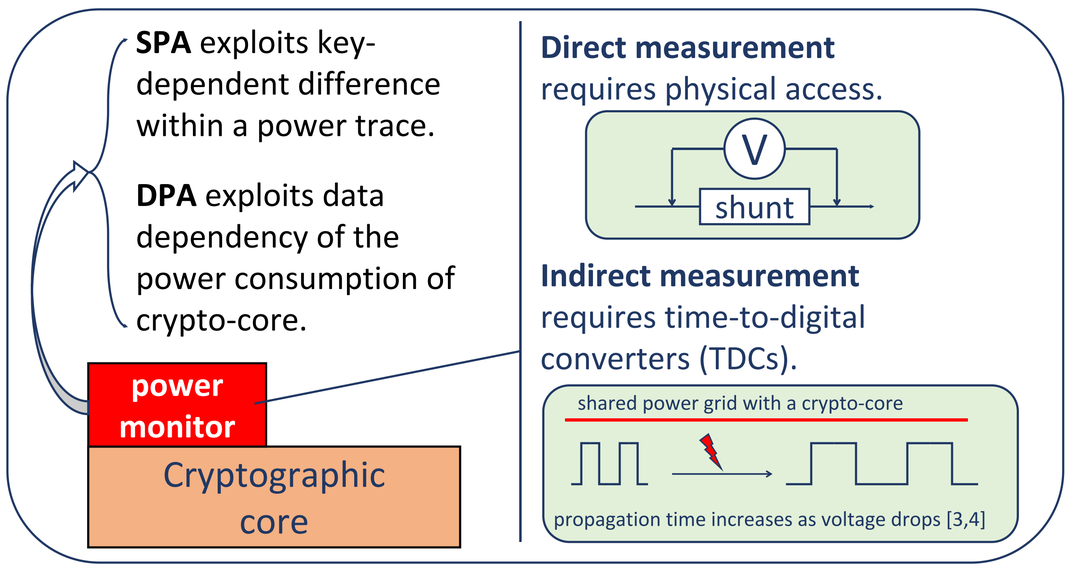


Figure 1: Power Analysis attack scheme.

OBJECTIVES

- Carry-chains were commonly used for implementing precise TDCs which are not available in UltraScale FPGAs.
- Recent attacks only performed on older FPGA families and at low clock speed (e.g., 24MHz [2]).
- **Goal of this work:** attack fast running AES cores (>100MHz) on recent FPGA architectures.

IMPLEMENTATION

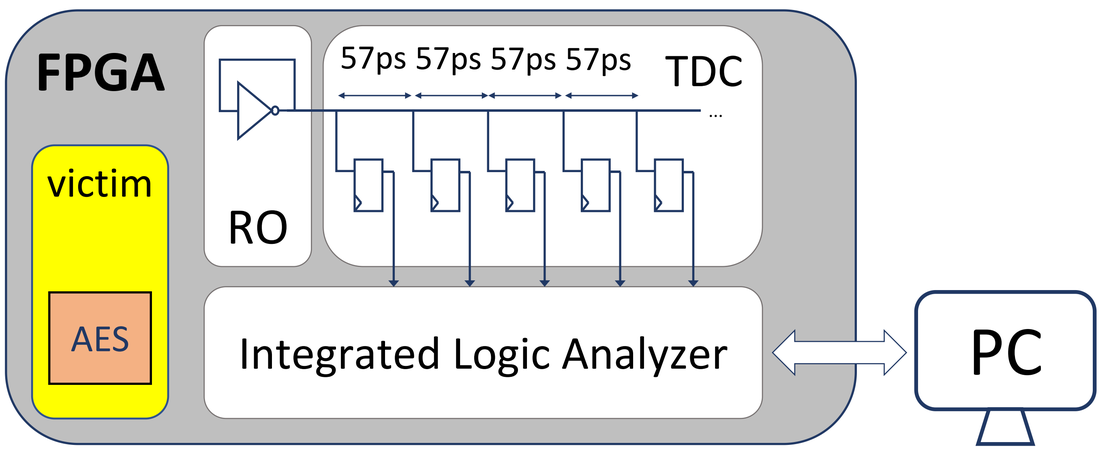


Figure 2: DPA attack scenario.

1. AES core: Standard core from NIST @ 100MHz.

2. Ring-oscillator: Single-stage RO is used which is built upon a lookup table (LUT6) primitive inside an FPGA (runs at about 2.8GHz).

3. Time-to-digital converter: Xilinx UltraScale+ optimised design only using local routing and flip-flops.

PRELIMINARY RESULTS

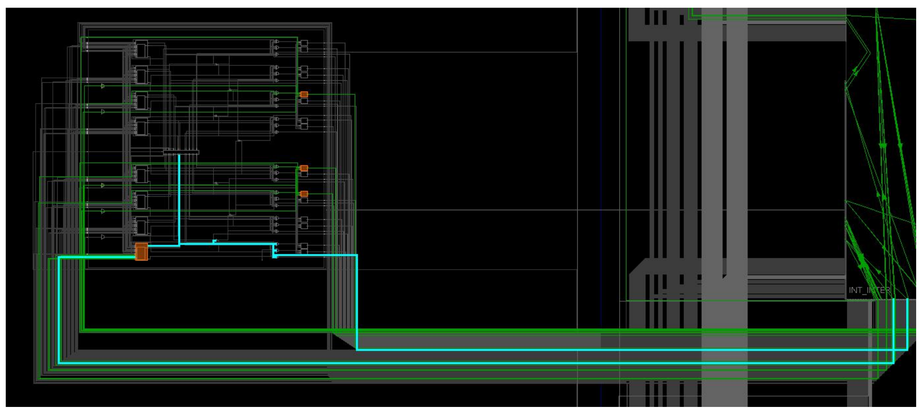


Figure 3: Ring-Oscillator's implementation.

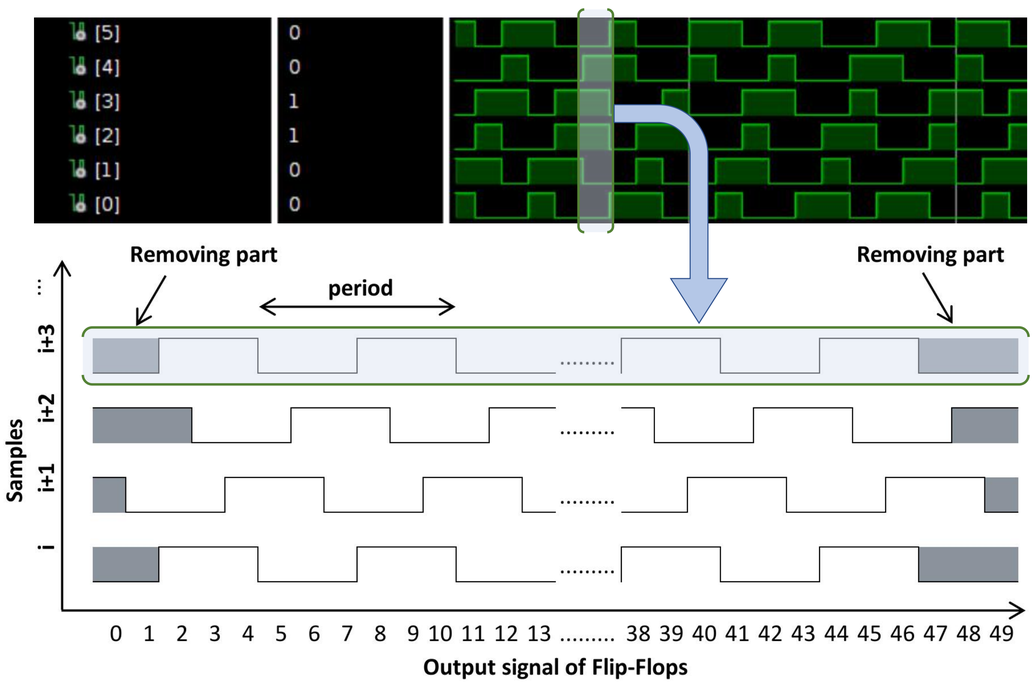
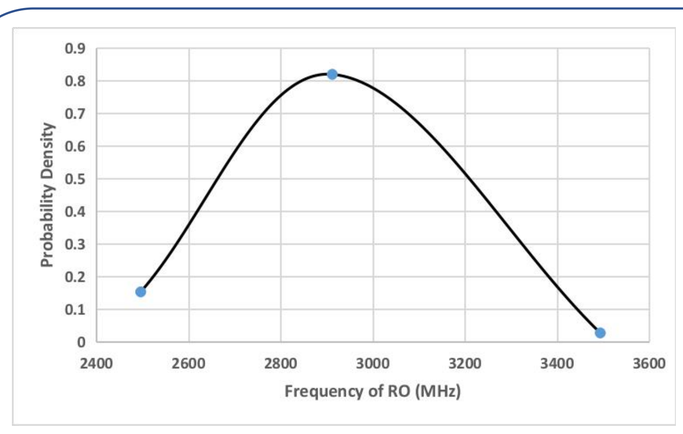


Figure 4: TDC response.

We created a voltage sensor and can measure the frequency of a RO at an idle state with the resolution of ~ 57ps. The response of the TDC is shown in **Figure 4**. The period can be calculated by:

$$f_{RO} = \frac{1}{T_{RO}} \approx \frac{1}{N_{flops} * t_{delay}}$$

Where f_{RO} is the frequency of RO, T_{RO} is the period of RO, N_{flops} is the number of flops representing one cycle, and t_{delay} is the average delay segment.



The mean frequency of the RO in an idle state is 2864MHz with stadard deviation of 0.82.

Figure 5: RO's frequency in idle state.

REFERENCES

[1] Kocher, Paul, et al, "Differential power analysis.", CRYPTO, 1999.

[2] Schellenberg, Falk, et al, "An inside job: Remote power analysis attacks on FPGAs.", DATE, 2018.

[3] Pant, Sanjay. "Design and Analysis of Power Distribution Networks in VLSI Circuits." (2008).

[4] Zick, Kenneth M., et al. "Sensing nanosecond-scale voltage attacks and natural transients in FPGAs.", ACM/SIGDA, 2013.

ACKNOWLEDGEMENT

The project *rFAS - reconfigurable FPGA Accelerator Sandboxing* is kindly supported by the National Cyber Security Centre of the UK under grant agreement 4212204/RFA 15971.