Master’s Thesis Engineering Technology

2019-2020

Remote power analysis attacks on reconfigurable cloud resources

Dominique Meus

Master of Electronics and ICT Engineering Technology

Abstract

Field-programmable gate arrays (FPGAs) are highly customizable devices which make them interesting devices to deploy in the cloud. To optimally use the hardware, multiple users could share a portion of one FPGA. The customizability is also a risk, as several side-channel attacks have been developed that use the reconfigurable fabric of the FPGA as sensors to gather information on other tenants or even other devices sharing the same power supply. These sensors often rely on time-to-digital converters to measure power consumption at nano-second scale. If one tenant is using such an FPGA as a cryptographic accelerator, another tenant could use power analysis to recover a secret key.

Currently, encryption cores running up to 100 MHz have been attacked using a tapped delay line (TDL) sensor. There are two main limitations to this design, one disadvantage is that the TDL has less time to measure the side-channel leakage as frequency goes up. Another disadvantage is that the TDL has to be calibrated for each device and for clock speed.

This thesis contains measurements of ring oscillators, registers, and AES core activity at 25 and 50 MHz on a Xilinx VC707 board. The results show that the side-channel leakage decreases as the frequency goes up. However, the effect of a single AES core is too small to perform power analysis on.

Results

To test the sensor, a set of ring oscillators were enabled and disabled.

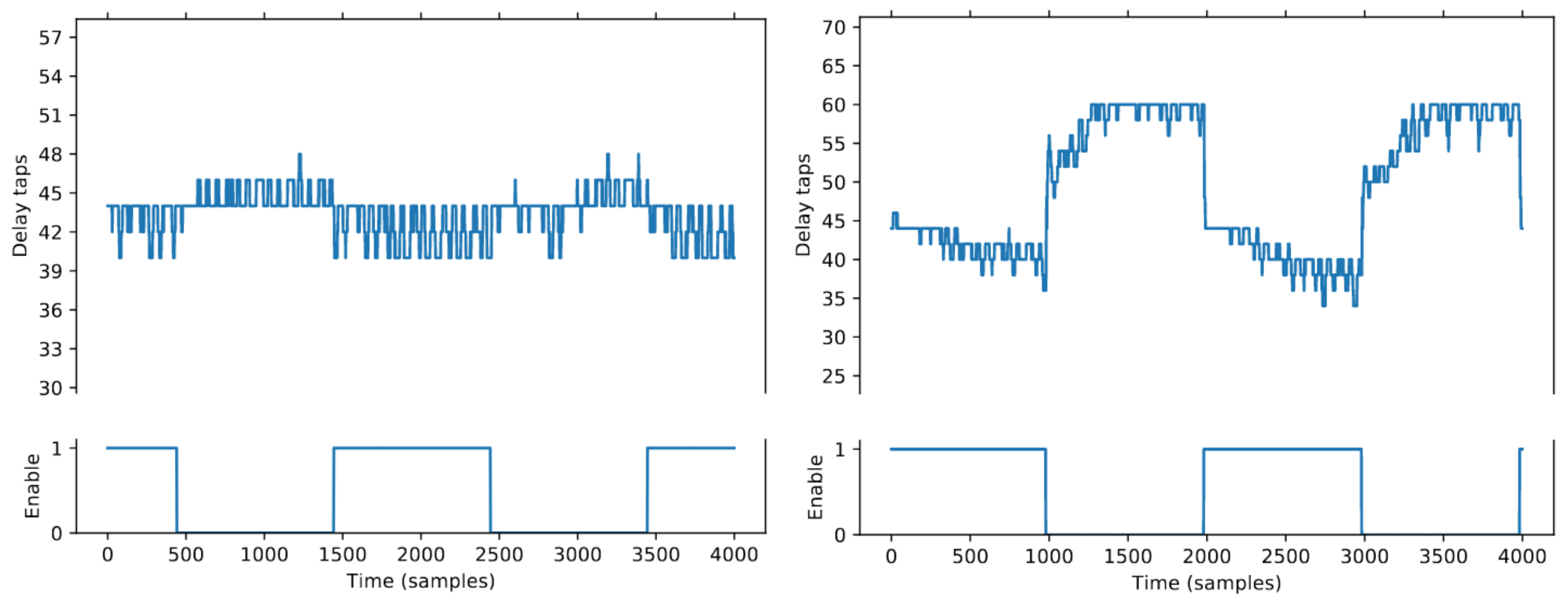

Figure 2: delay measurement of 250 (left) ring oscillators on the left and 2500 (right) ring oscillators on the right at 50 MHz.

The effect of the ring oscillators being active is clearly visible in the measurement. However, ring oscillators draw a large amount of current compared to a circuit that performs encryption. Thus, an AES core was measured.

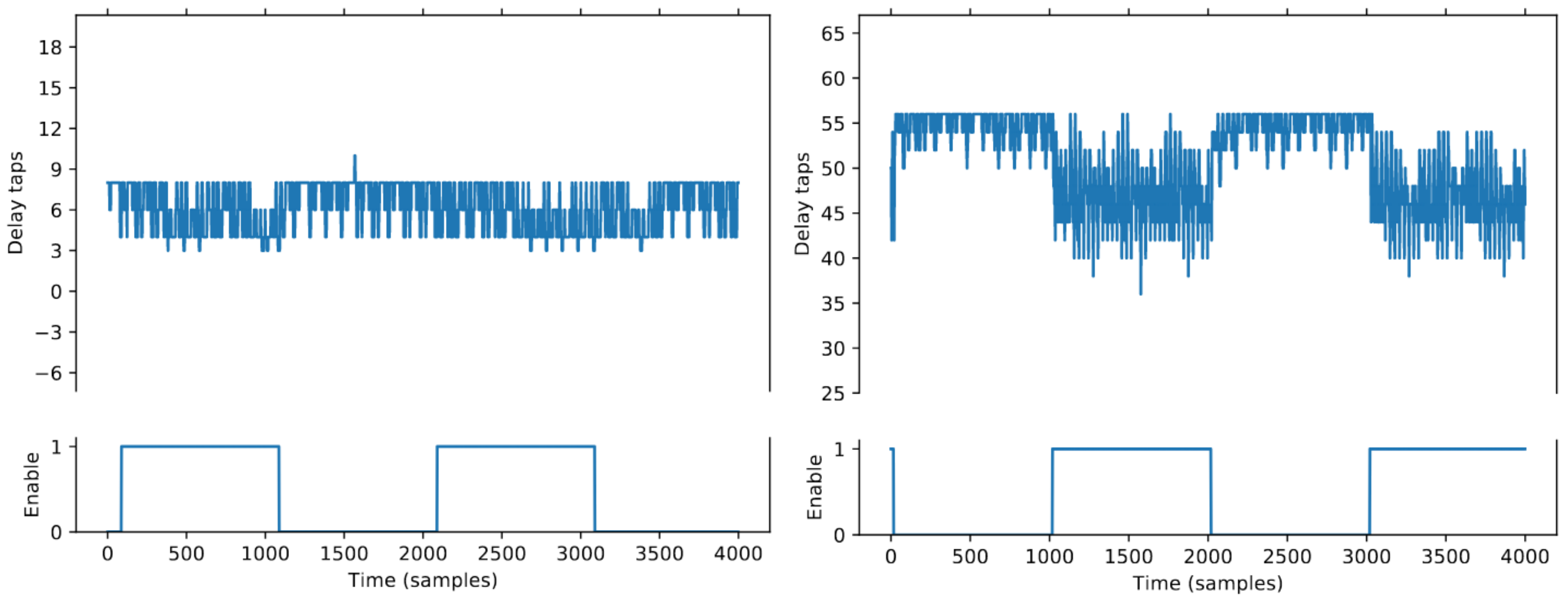

Figure 3: delay measurement of 1 (left) and 10 (right) AES cores at 25 MHz.

The effect of a single AES core turned out to be too small to perform power analysis on.

Method

In order to perform power analysis attacks on an FPGA, the power usage has to be measured at a high frequency. One way to do this, is to measure the propagation delay of the gates in the FPGA. This can be done by using a time-to-digital converter, more specifically a tapped delay line sensor.
A tapped delay line sensor with calibration was implemented as illustrated in figure 1. The sensor consists of an initial delay line to the left and an observable delay line to the right. A signal passes through the sensor and the state of the observable delay line gets captured in flip flops before the signal reaches the end. By having a very consistent delay between the start and stop signal, the speed at which the signal passes through the delay line can be measured.
To the very left, the start signal passes through a long chain of latches denoted by LD. The length of this chain can be varied by choosing an enable signal. This signal then passes through a chain of CARRY4 elements on the right side. CARRY4 primitives provide consistent routing and good resolution. Finally the value of the delay line between each carry chain gets captured in a pair of flip flops. The additional flip flop reduces metastability issues.
The values captured in the flip flops are a relative measurement for the propagation delay of the delay line and the power consumption of the FPGA during the measuring period.

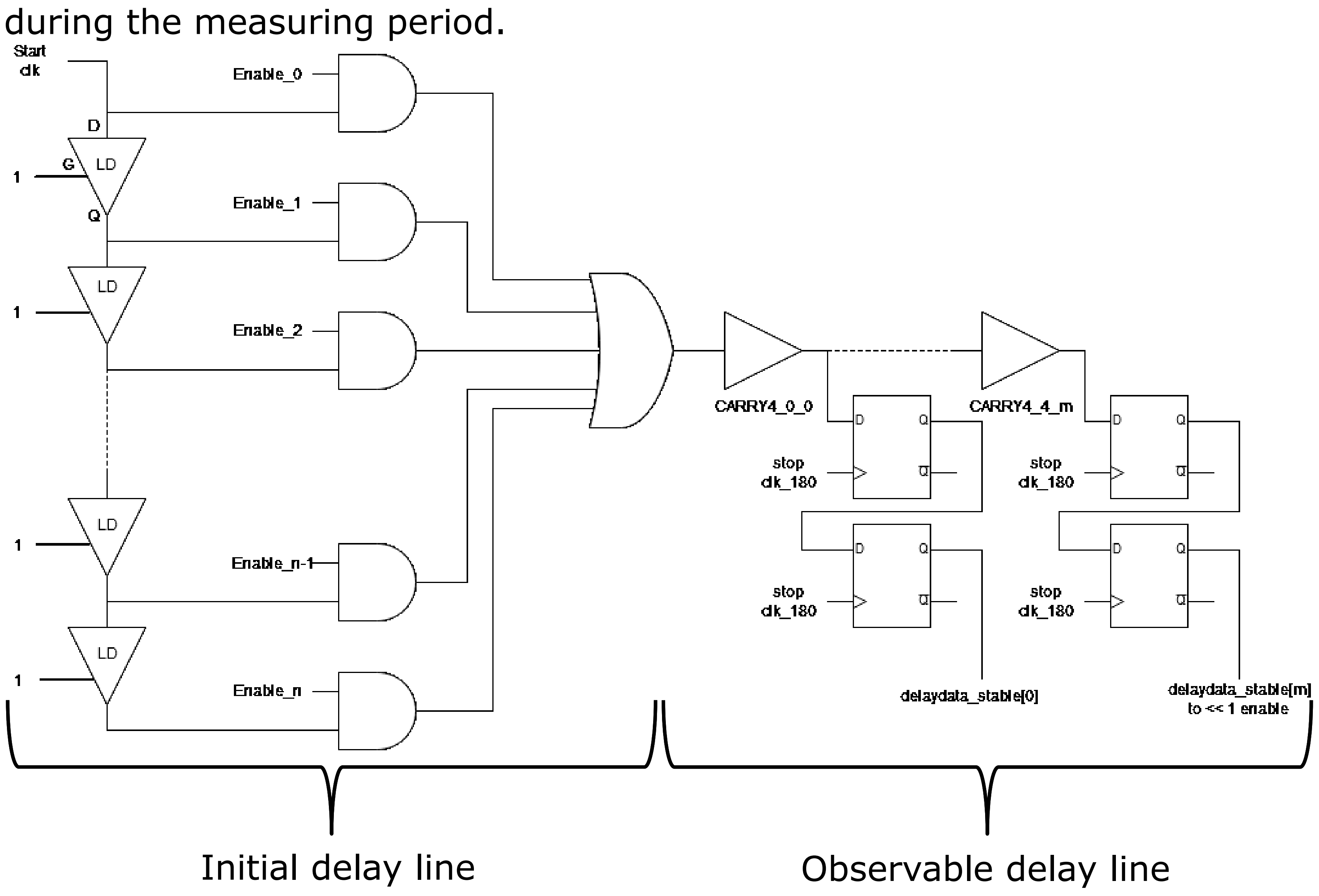

Figure 1: tapped delay line sensor

Conclusion

A tapped delay line is able to detect FPGA power usage at high frequencies. As the frequency goes up, the sensor becomes less effective. Xilinx Virtex series FPGAs are relatively large compared to the Spartan and Artix FPGAs used in the literature [1-2]. My hypothesis is that the larger VC707 board is less sensitive to side channel attacks compared to the smaller FPGAs.

References

[1] F. Schellenberg, D. R. Gnad, A. Moradi, and M. B. Tahoori, “An inside job: Remote poweranalysis attacks on FPGAs,” in2018 Design, Automation & Test in Europe Conference &Exhibition (DATE), (Dresden), pp. 1111–1116, IEEE, Mar. 2018.
[2] F. Schellenberg, D. R. E. Gnad, A. Moradi, and M. B. Tahoori, “Remote inter-chip poweranalysis side-channel attacks at board-level,” inProceedings of the International Conferenceon Computer-Aided Design - ICCAD ’18, (San Diego, California), pp. 1–7, ACM Press,2018.

Supervisors / Cosupervisors: prof. dr. ir. Nele Mentens
dr. ing. Jo Vliegen