Understanding and Comparing the Capabilities of On-Chip Voltage Sensors against Remote Power Attacks on FPGAs

Shayan Moini, Xiang Li, Peter Stanwicks, George Provelengios, Wayne Burleson, Russell Tessier, and Daniel Holcomb
Department of Electrical and Computer Engineering, University of Massachusetts Amherst
Email: {smoini, xiang, pstanwicks, gprovelengio, burleson, tessier, dholcomb} @ umass.edu

***Abstract*—This paper presents a study of two types of on-chip FPGA voltage sensors based on ring oscillators (ROs) and time-to-digital converter (TDCs), respectively. The performance of these sensors is evaluated in the presence of circuits that deliberately waste power, resulting in localized voltage drops. The effects of FPGA power supply features and sensor sensitivity in detecting voltage drops in an FPGA power distribution network (PDN) are evaluated for Xilinx Artix-7 and Zynq UltraScale+ FPGAs. We show that the two sensor types are both able to detect supply voltage drops, and that their measurements are consistent with each other. However, we find that TDC-based sensors are more sensitive and can detect voltage drops that are shorter in duration, while RO sensors have a higher dynamic range and are easier to implement because calibration is not required.**

I. INTRODUCTION

Field Programmable Gate Arrays (FPGA) are now used in a wide variety of computing platforms, including the cloud. There is increasing interest in sharing cloud FPGAs across multiple users simultaneously, creating a *multi-tenant* scenario [1]. Major cloud providers including Amazon AWS provide remote access to powerful FPGA platforms that make a multi-tenant scenario more plausible. This opens the door to a new class of threats, namely, on-chip side-channel voltage analysis attacks [2]. In these attacks an adversary that shares the FPGA with the victim, even assuming total logic resource isolation, can instantiate sensors to monitor voltage fluctuations on the shared Power Distribution Network (PDN) of the FPGA that are caused by activity in the victim's circuit. The FPGA circuits used for sensing supply voltage fluctuations are typically either time-to-digital converters (TDCs) or ring oscillators (ROs). Both circuits exploit propagation delay as a proxy for measuring supply voltage, as lower supply voltage is known to cause an increase in propagation delay.

Time-to-digital converters detect voltage changes in the FPGA PDN by sensing the changing delay of a propagating signal through a chain of buffers or other logic [3], [4]. Schellenberg et al. [5] use TDC sensors to conduct side-channel power analysis attacks against AES and RSA modules. TDC sensors can also be used as receivers for covert communication from information-leaking hardware Trojans in the victim circuit. Gnad et al. [6] demonstrate an 8 MBit/s covert channel between a ring oscillator transmitter that modulates power consumption, and a TDC receiver that senses the resulting voltage fluctuations at a different location on the same FPGA. Giechaskiel et al. [7] extend this concept to an RO transmitter and TDC receiver on separate FPGAs that share a common power supply.

Ring-oscillator based sensors can also be used to monitor the supply voltage of an FPGA PDN [8] because the propagation delay through the RO, which depends on supply voltage, can be observed by measuring oscillation frequency. Zhao et al. [9] use on-chip RO sensors to recover keys from an RSA accelerator. Provelengios et al. [2] reconstruct the voltage gradients on the chip from a network of RO-based sensors. They deploy this approach to diagnose voltage drops caused by a large number of ROs that operate as malicious power-consuming circuits which overwhelm the FPGA PDN to induce timing faults in co-resident victim circuits; similar attacks can be launched with alternative power wasting circuits [10]–[12].

In this work, we study and quantify the capabilities of TDCs and ROs as supply voltage sensors on FPGAs. To evaluate the sensors we conduct experiments using two types of dummy power consumption circuits that cause controllable fluctuations on the PDN. We compare the measurements from the two sensors in terms of detection sensitivity, range, and stability. The supply voltage is also measured directly for ground truth using ChipWhisperer CW305 platform's [13] analog-to-digital converter (ADC). Overall, comparative data is collected from two boards: the ChipWhisperer CW305 board with a Xilinx Artix-7 FPGA (xc7a100tftg256-2), and a ZCU104 board [14] with a Xilinx Zynq UltraScale+ FPGA (xczu7ev-ffvc1156-2-e).

The experimental results show a high correlation in how each sensor responds to major voltage drops, but that TDC sensors better detect short voltage drops, while RO sensors have a higher dynamic range and require no calibration. We also show that shunt resistors, which are commonly used for monitoring current into the chip, can play an important role in increasing the supply voltage fluctuations observed in the on-chip sensors. The insights provided by this paper can be used by researchers in designing on-chip voltage sensors, choosing FPGA platforms and power supply configurations to improve resilience against attacks, and creating dummy power waster circuits for studying how an FPGA PDN responds to fault injection scenarios.

II. METHODOLOGY

This section presents the architecture and circuit details of the power wasters, sensors, and trace collection. An overview of our system architecture is shown in Fig. 1. The user accesses the FPGA through a JTAG-to-AXI module to control the wasters and sensors. Sensor measurements are logged to an on-chip FIFO during each experimental trial and recovered by the user after the trial is complete. The same architecture is implemented on the ChipWhisperer CW305 and Xilinx ZCU104 evaluation boards. The CW305 is specifically designed for evaluating side-channel power analysis attacks against cryptographic circuits. It includes a 250 mΩ shunt resistor inline between the voltage regulator and the FPGA that allows an ADC to collect voltage measurements on both sides of the shunt. All decoupling capacitors that would otherwise be connected to the supply voltage to filter out voltage fluctuations have been removed.

A. Power Consumption Circuits

Two types of on-chip power wasting circuits are examined in this work to create voltage fluctuations on the FPGA PDN that are then measured using the voltage sensors. The two designs are a flip-flop (FF) waster (Fig. 2a) and a ring-oscillator (RO) waster (Fig. 2b). Each type of power wasting circuit is parameterized so that its impact can be varied.

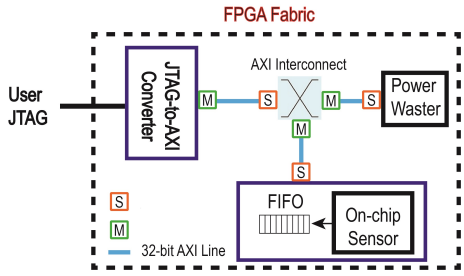


Fig. 1: Overview of the implemented architecture

1) FF waster: The FF waster (Fig. 2a) is a flip-flop with a high fanout load on its output. The number of fanouts is the adjustable parameter of this circuit, and we vary this value between 0 and 7,000. When the output of the first flip-flop switches from 0 to 1, it charges a large output capacitance and therefore consumes power. This type of power wasting circuit creates a temporally-short switching event on a single clock edge, although it consumes less power than our second design.

2) RO waster: The RO waster (Fig. 2b) comprises a 3-inverter chain that is enabled and disabled by a multiplexer. This circuit continuously consumes power, unlike the instantaneous power consumption on the rising clock edge in the FF-based waster. The number of enabled ROs is the changeable parameter of this circuit, and it is varied between 0 and 1,000. The RO power wasters oscillate at a high frequency and consume much more power than the FF-based power wasters.

B. Sensor Circuits

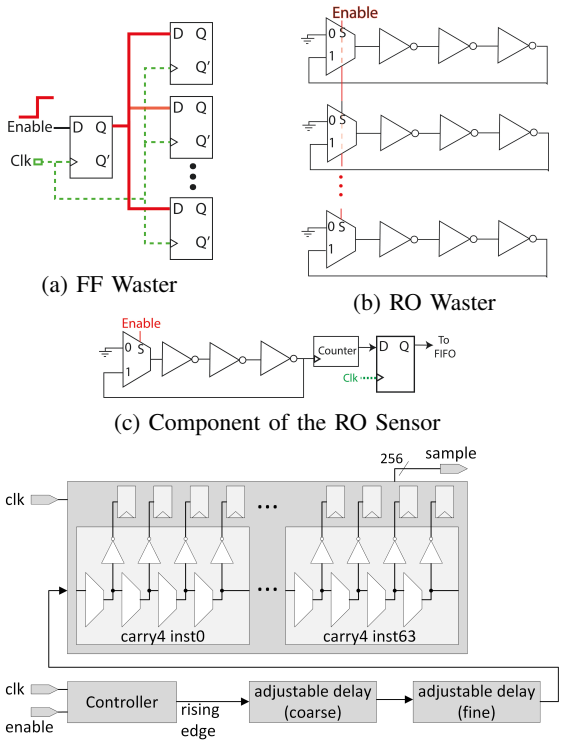
The two types of voltage sensors we use are ring oscillators circuits (RO sensors) and time-to-digital converters (TDC sensors). Both types of sensors log their data to FIFOs during experimental trials, as shown in Fig. 1.

1) RO sensor: The RO sensor is composed of 16 instances of a ring oscillator and counter circuit that increments on each rising edge of the oscillator (Fig. 2c). The value of the counter is stored to flip-flops at each Clk rising edge. The counter is then reset to zero. This approach allows for counting the number of oscillations in each Clk clock cycle. In this work, data from the 16 separate RO sensors are averaged to create each data-point that serves as our RO sensor measurement.

2) TDC sensor: The TDC sensor (Fig. 2d) is composed of a configurable delay line leading to a series of 64 CARRY4 primitives, which are fixed logic components provided by Xilinx for performing fast carry propagation in arithmetic operations. A rising edge is transmitted through the delay line and into the carry chain. The 64 CARRY4 primitives result in a delay line with 256 taps, and each tap is attached to the data input of a flip-flop. The Hamming weight of the values captured in these flip-flops on the clk clock edge is the output value of the TDC, and it reveals how far up the carry chain the rising edge has propagated during the clock cycle. If the propagation delay of logic slows down due to a lower supply voltage, then the Hamming weight will decrease, which allows the TDC to be used as a voltage sensor. Unlike the RO sensor, the TDC sensor needs careful manual placement and calibration to assure its delay is matched to the clock period.

III. EXPERIMENTS

Experiments were conducted to evaluate how well the TDC sensors and RO sensors can detect voltage drops on the FPGA PDN that are caused by the power wasting circuits.



(a) FF Waster (b) RO Waster

(c) Component of the RO Sensor

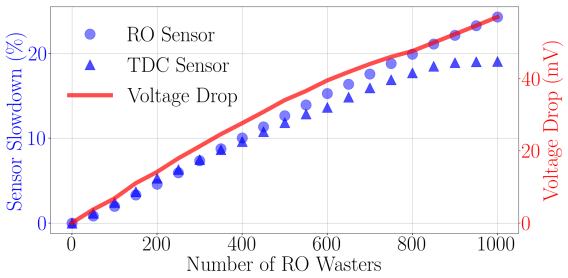
(d) TDC Sensor

Fig. 2: Detailed view of the power waster and sensor circuits

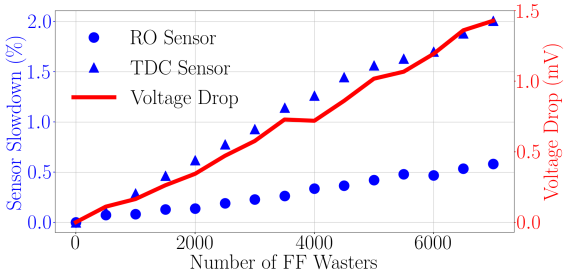
A. Consistency Between RO and TDC Sensors

In each run (trial) of the first experiment, power wasters are activated while the sensor data is being logged. Because the minimum sensor values of each run coincide with the voltage drop caused by the power wasters, we extract the minimum RO count or TDC Hamming weight, depending on sensor type, for each run. At the same time, we measure the external voltage of the FPGA using the ChipWhisperer capture board. While making these measurements, the number of activated power wasters is swept from 0 to 1,000 for the RO wasters and from 0 to 7,000 for the FF wasters. The TDC sensor experiments use a 50MHz clock, and the RO sensor experiments use a 10MHz clock. The slower clock is used for RO sensor experiments to reduce the variation in the trace that arises when the number of RO oscillations per cycle is small; the RO sensors have a mean frequency of 356MHz under nominal conditions. Each experiment is repeated 100 times and the results are averaged to reduce the impact of noise and better show the trend. The data from the RO sensor and TDC sensor are mapped from their nominal units (count and Hamming weight, respectively) into a common unit of slowdown – which is the fractional change in propagation delay (in the RO or TDC's delay line) that would cause the observed change in output values. Converting both measurements to slowdown allows for comparing the sensor outputs in a common unit.

Fig. 3a shows the sensor slowdown when different numbers of RO-based wasters are enabled, and also the externally-measured voltage drop. As more power wasters are activated, the voltage drops, and this induces a similar slowdown in both types of sensors. Note that, when more than 800 RO wasters are activated, the voltage drop saturates the range of the TDC sensor, meaning that the TDC outputs a Hamming weight of 0, and is therefore unable to show a further reduction in Hamming



(a) RO Waster



(b) FF Waster

Fig. 3: Sensor slowdown under varied power consumption

Sensor Type	Precision
RO sensor; 10 MHz clock	2.8%
RO sensor; 50 MHz clock	14.9%
TDC sensor; 50 MHz clock	0.12%

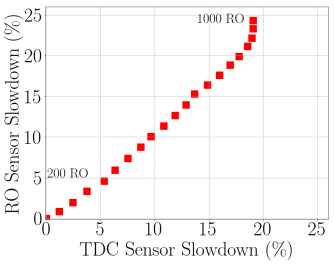
TABLE I: Comparison of sensors' resolution

weight as the voltage continues to drop. This causes the TDC slowdown curve to flatten out.

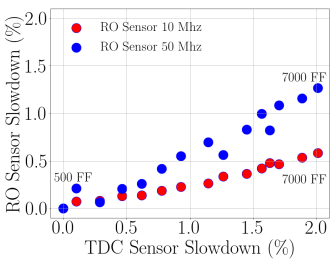
Fig. 3b shows the sensor slowdown and voltage when the FF wasters are turned on, which induces considerably less voltage drop than the RO wasters. Notable in this case is that the RO sensor experiences a smaller slowdown than does the TDC sensor. This occurs because the voltage drop from the FF wasters has a short temporal duration and the RO sensor has a relatively long integration period of 100ns at 10MHz clock. The FF wasters only affect the RO sensors during the portion of the integration period for which the voltage is reduced.

B. Sensitivity

To study the sensitivity of the two sensors, we re-use the data from Fig. 3 to generate the scatter plots in Fig. 4. Fig. 4a shows the data from the RO wasters; the data falls along the 45-degree diagonal, which indicates that the two sensors are in agreement. As mentioned in the prior section, and now observable in Fig. 4b, the RO sensors are poorly suited to detecting the short-duration voltage drop from the FF wasters, especially at a slow clock period such as 10 MHz. Table I compares the resolution of sensors. Here, resolution is defined as the amount of slowdown that will change the output value of the sensor. For the RO, this value is determined by the amount of slowdown needed to change the number of oscillations occurring within the integration period, which is determined by the clock period. In the TDC this value is determined by the amount of slowdown needed to make the rising edge reach one fewer stage in the TDC circuit. The TDC sensor, therefore, enjoys a higher resolution compared to the RO sensor, and the resolution of RO sensor drops with an increase in clock frequency.

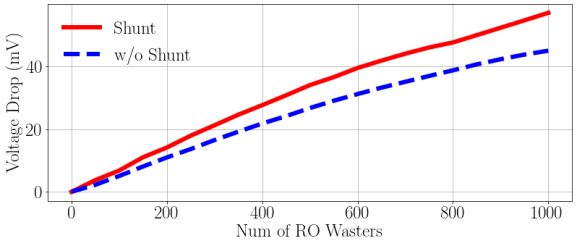


(a) RO Waster

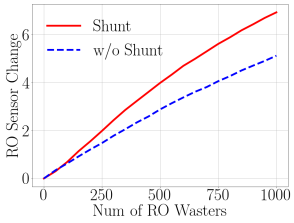


(b) FF Waster

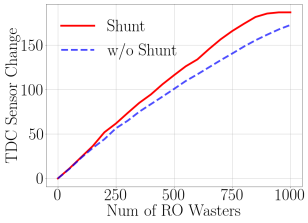
Fig. 4: Comparison of sensors' relative sensitivity



(a) Voltage Drop



(b) RO Sensor Change



(c) TDC Sensor Change

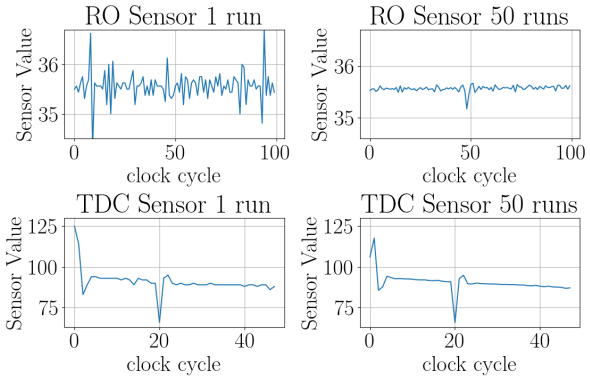
Fig. 5: Effect of bypassing shunt resistor with RO wasters.

C. Effect of the Shunt Resistor

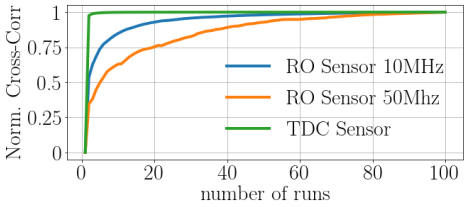
As mentioned in Section II, the ChipWhisperer board includes a shunt resistor for the evaluation of power-based side-channel attacks. In this subsection, we study the effect of the shunt resistor. Increasing the number of activated wasters results in more current flowing into the FPGA. This action increases the IR voltage across the shunt resistor and causes a voltage drop at the FPGA supply voltage pin. The series shunt resistor can be bypassed using a jumper header which reduces resistance from 250 mΩ to less than 10 mΩ. Fig. 5 shows how bypassing the shunt resistor reduces the onboard voltage drop as observed by the RO sensors and TDC sensors. The voltage drop at the low voltage side of the shunt resistor when the RO wasters are enabled is shown in Fig. 5a. As one might expect, the shunt resistor causes the sensors to observe a larger change when the RO wasters are enabled. This result is observed for the RO sensor in Fig. 5b and for the TDC sensor in Fig. 5c. Since shunt resistors are often used as part of circuits for measuring power consumption, this finding implies that these resistors may benefit attackers and should be carefully considered.

D. Noise and Stability

As mentioned in Section III-A, our experiments were run multiple times and the average of the traces was used to obtain results with limited noise. Fig. 6a shows the recovered RO- and TDC-based sensor traces for different numbers of runs; 6,000 FF wasters were activated in cycle 50 and cycle 20 of the



(a) Sensor traces with and without averaging



(b) Correlation increasing with averaging

Fig. 6: Sensor data converges with more runs

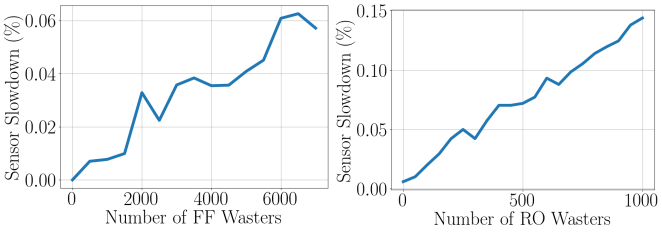
RO sensor and TDC sensor experiments respectively, at which points we expect to see the sensor values drop. The figure shows that the TDC sensor detects the power wasters clearly even with just a single run, but the RO sensor is noisy and requires many traces to average out the noise and show the expected finding. Fig. 6b shows the normalized cross-correlation between the average of n traces and the average of 100 traces, as a way of showing how quickly the average traces converge. The TDC sensor is able to achieve 99% correlation after only 3 runs, whereas the RO sensor at 10MHz and 50MHz clock periods require 60 and 95 runs, respectively. This result shows a stability advantage of the TDC over the RO sensors.

E. Experiments with the Zynq Board

To evaluate the effectiveness of the TDC sensors on a board that is fully populated with decoupling capacitors and does not have a shunt resistor, a Xilinx ZDU104 evaluation board featuring a Zynq UltraScale+ FPGA was used for experimentation. The UltraScale+ is the FPGA family used in the Amazon AWS F1 cloud-based instances. Due to FPGA architectural differences, the TDC was implemented using 32 Carry8 elements instead of 64 Carry4 elements, and the clock cycle was set to 120 MHz due to the higher speed of the logic elements. Figures 7a and 7b show the TDC sensor slowdown plotted against the number of activated FF and RO wasters. Although the slowdown on this platform is less significant than on the ChipWhisperer, the figure shows that the sensors can still detect the voltage fluctuations arising from power consumption, which can facilitate power side-channel attacks.

IV. CONCLUSION

In this paper, an analysis of on-chip voltage sensors based on ring oscillators and time-to-digital converters is presented. Two FPGA power wasters based on ring oscillators and flip-flops were used to compare the sensitivity of the sensors on a ChipWhisperer board. The experiments show that the sensor values are consistent with each other in terms of detecting



(a) FF-Based Waster (b) RO-Based Waster

Fig. 7: TDC sensor slowdown on ZCU104

circuit slowdown. The TDC sensor has higher sensitivity in detecting small voltage drops, while the RO sensor has a larger range. The effect of the ChipWhisperer shunt resistor in accentuating the voltage drop was also studied. Consistent with prior work [3], our findings show that the TDC sensors are generally better suited for high-speed applications and detecting short transient drops such as those in side-channel attacks. Experiments using a Xilinx Zynq UltraScale+ board show that voltage drops are more difficult to detect on a later generation FPGA. Our findings can be used by researchers in developing countermeasures against remote side-channel attacks that use FPGA voltage manipulations.

ACKNOWLEDGMENT

This research was funded in part by NSF grants CNS-1902532 and CNS-1563829.

REFERENCES

[1] A. Khawaja, J. Landgraf, R. Prakash, M. Wei, E. Schkufza, and C. J. Rossbach, "Sharing, protection, and compatibility for reconfigurable fabric with AMORPHOS," in *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, 2018.

[2] G. Provelengios, D. Holcomb, and R. Tessier, "Characterizing power distribution attacks in multi-user FPGA environments," in *29th International Conference on Field Programmable Logic and Applications (FPL)*. IEEE, 2019, pp. 194–201.

[3] K. M. Zick, M. Srivastav, W. Zhang, and M. French, "Sensing nanosecond-scale voltage attacks and natural transients in FPGAs," *International Symposium on Field Programmable Gate Arrays (FPGA)*, pp. 101–104, 2013.

[4] D. R. Gnad, F. Oboril, S. Kiamehr, and M. B. Tahoori, "Analysis of transient voltage fluctuations in FPGAs," *International Conference on Field-Programmable Technology, FPT*, pp. 12–19, 2016.

[5] F. Schellenberg, D. R. Gnad, A. Moradi, and M. B. Tahoori, "Remote inter-chip power analysis side-channel attacks at board-level," in *International Conference on Computer-Aided Design*, 2018, pp. 1–7.

[6] D. R. Gnad, C. D. K. Nguyen, S. H. Gillani, and M. B. Tahoori, "Voltage-based covert channels in multi-tenant FPGAs." *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 1394, 2019.

[7] I. Giechaskiel, K. Rasmussen, and J. Szefer, "C3APSULe: Cross-FPGA covert-channel attacks through power supply unit leakage," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2020.

[8] K. M. Zick and J. P. Hayes, "Low-cost sensing with ring oscillator arrays for healthier reconfigurable systems," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 5, no. 1, 2012.

[9] M. Zhao and G. E. Suh, "FPGA-based remote power side-channel attacks," in *IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 229–244.

[10] M. M. Alam, S. Tajik, F. Ganji, M. Tehranipoor, and D. Forte, "RAM-Jam: Remote temperature and voltage fault attack on FPGAs using memory collisions," in *2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2019, pp. 48–55.

[11] K. Matas, T. M. La, K. D. Pham, and D. Koch, "Power-hammering through glitch amplification–attacks and mitigation," in *IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, 2020, pp. 65–69.

[12] G. Provelengios, D. Holcomb, and R. Tessier, "Power wasting circuits for cloud FPGA attacks," in *30th International Conference on Field Programmable Logic and Applications (FPL)*, 2020.

[13] C. O'Flynn and Z. D. Chen, "Chipwhisperer: An open-source platform for hardware embedded security research," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*, 2014, pp. 243–260.

[14] *ZCU104 User's Guide*, Xilinx Corporation, Oct. 2018.