Voltage Sensor Implementations for Remote Power Attacks on FPGAs

SHAYAN MOINI, University of Massachusetts Amherst, USA
ALEKSA DERIC, University of Massachusetts Amherst, USA
XIANG LI, University of Massachusetts Amherst, USA
GEORGE PROVELENGIOS, University of Massachusetts Amherst, USA
WAYNE BURLESON, University of Massachusetts Amherst, USA
RUSSELL TESSIER, University of Massachusetts Amherst, USA
DANIEL HOLCOMB, University of Massachusetts Amherst, USA

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. It has previously been shown that these sensors are often used to extract side-channel information from FPGAs without physical access. The performance of the 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, Zynq 7000, and Zynq UltraScale+ FPGAs. We show that both sensor types are able to detect supply voltage drops, and that their measurements are consistent with each other. Our findings show that TDC-based sensors are more sensitive and can detect voltage drops that are shorter in duration, while RO sensors are easier to implement because calibration is not required. Furthermore, we present a new time-interleaved TDC design that sweeps the sensor phase. The new sensor generates data that can reconstruct voltage transients on the order of tens of picoseconds.

CCS Concepts: • **Security and privacy** → **Side-channel analysis and countermeasures**; • **Hardware** → *Reconfigurable logic applications*; **On-chip sensors**.

Additional Key Words and Phrases: Multi-tenant FPGA, On-Chip Voltage Sensor,Ring Oscillator, Side-channel Attacks, Time-to-Digital Converter

1 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 among multiple users simultaneously, creating a *multi-tenant* scenario [11]. Major cloud providers including Amazon Web Services (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 [20]. 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

Authors' addresses: Shayan Moini, smoini@umass.edu, University of Massachusetts Amherst, Amherst, Massachusetts, USA, 01003; Aleksa Deric, University of Massachusetts Amherst, Amherst, Massachusetts, USA, 01003, aderic@umass.edu; Xiang Li, University of Massachusetts Amherst, Amherst, Massachusetts, USA, 01003, xiang@umass.edu; George Provelengios, University of Massachusetts Amherst, Amherst, Massachusetts, USA, 01003, gprovelengio@umass.edu; Wayne Burleson, University of Massachusetts Amherst, Amherst, Massachusetts, USA, 01003, burleson@umass.edu; Russell Tessier, University of Massachusetts Amherst, Amherst, Massachusetts, USA, 01003, tessier@umass.edu; Daniel Holcomb, University of Massachusetts Amherst, Amherst, Massachusetts, USA, 01003, dholcomb@umass.edu.

Preprint of paper appearing in ACM TRETS

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 changes in the delay of a propagating signal through a chain of buffers or other logic [9, 33]. Schellenberg et al. [23] 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. [8] 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. [5] 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 [32] because the propagation delay through the RO, which depends on supply voltage, can be observed by measuring oscillation frequency. Zhao et al. [30] use on-chip RO sensors to recover keys from an RSA accelerator. Provelengios et al. [20] reconstruct the voltage gradients on an FPGA 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. These power wasters overwhelm the FPGA PDN to induce timing faults in co-resident victim circuits; similar attacks can be launched with alternative power wasting circuits [1, 16, 22]. Networked sensors can be used to identify the source of a power attack and mitigate its impact [21], if they are able to respond quickly enough.

In this work, we study and quantify the capabilities of TDCs and ROs as supply voltage sensors in FPGAs. The paper improves and extends our previous conference paper on the same topic [17]. To evaluate the sensors we conduct experiments using two types of parameterized dummy power consumption circuits that cause controllable voltage fluctuations on the PDN. We compare and contrast the measurements from the two sensors in terms of detection sensitivity and stability. The supply voltage is also measured directly for ground truth using an ADC on a capture board which is connected to a ChipWhisperer CW305 board [19]. Overall, comparative data is collected from three boards: the ChipWhisperer CW305 board with a Xilinx Artix-7 FPGA (xc7a100tftg256-2), a ZCU104 board [28] with a Xilinx Zynq UltraScale+ FPGA (xczu7ev-ffvc1156-2-e), and a Digilent Zybo Z7-20 board [4] featuring a Xilinx Zynq-7000 FPGA (XC7Z020-1CLG400C).

The experimental results show a high correlation in how each sensor responds to major voltage drops. TDC sensors better detect short voltage drops, while RO sensors require no calibration. We also show that TDC sensors can be extended to use time-interleaved sampling, which allows for characterization of transient voltage fluctuations at sub-clock cycle timescales. 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.

The remainder of this paper is structured as follows. Section 2 provides an overview of previous work on on-chip voltage sensors and voltage attacks. Section 3 discusses our methodology for inducing power fluctuations and sensing. Section 4 compares and contrasts the two types of delay-based sensors. Section 5 considers sensing of transient voltage fluctuations, and Section 6 covers post-processing to enhance quality of sensor data. Section 7 outlines future directions and concludes the paper.

2 RELATED WORK

FPGA voltage sensor implementation and voltage attacks have been widely studied. S. Zhao et al. [31] used a TDC-based on-chip voltage sensor to extract electrical characteristics of the FPGA power distribution network including its DC

resistance and frequency bands with high impedance. K. M. Zick et al. [33] used TDCs to measure voltage drops. They showed that a TDC is able to sense nanosecond-scale voltage variations. D. Gnad et al. [9] used a TDC to characterize transient voltage fluctuation caused by toggling flip-flops. O. Glamočanin et al. [7] deployed a TDC to record voltage fluctuation and recover advanced encryption standard (AES) keys on an Amazon EC2 F1 instance. Similarly, M. Zhao et al. [30] used ROs as power monitors to perform a power analysis attack on an RSA module. Trade-offs between ROs and TDCs including sampling frequency, achievable power resolution and robustness are explored, although no quantitative comparison between the two sensor types is given. G. Provelengios et al. [20] calibrated and arranged RO-based voltage sensors on a Cyclone V FPGA to monitor voltage attacks on the PDN and locate the attacker circuit. To improve sampling resolution, interleaved TDCs have also been studied. Z. Yin et al. [29] developed a TDC system with four multi-phase clocks generated by a phase-locked loop on a Virtex-4 FPGA. With this implementation, the sampling resolution of a TDC can reach one-quarter of a clock cycle and time interpolation within a clock cycle is achieved. Similarly, A. Balla et al. [2] implemented 4× oversampling using a digital clock manager (DCM) on an Virtex-5 FPGA. In our work, we improve the TDC quantization step by using a mixed-mode clock manager (MMCM) to generate fine-grained clock phase shifts which can be adjusted dynamically and can increase the sampling rate over 560x.

FPGA-based power wasters used in voltage attacks have also been widely studied. D. Gnad et al. [10] demonstrated a denial-of-service attack using ROs which was able to crash three different types of Xilinx FPGAs. L. Shen et al. [24] created transient generators and tested them on FIR and DFT benchmarks using Cyclone IV FPGAs. They reported a 25% reduction in benchmark maximum operational frequency. A. Boutros [3] et al. attacked a deep learning accelerator on an Intel Stratix 10 FPGA using three types of power wasters. Even with their most sophisticated setup, the attack did not compromise its prediction accuracy at the safe operating frequency. J. Krautter et al. [13] performed differential fault analysis of an AES core on FPGAs using voltage-based fault injection with ROs. They successfully recovered key bytes from AES on Cyclone V and Lattice FPGAs. None of papers above analyze power wasters and voltage comparisons in a systematic way.

3 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, Zybo Z7-20, and Xilinx ZCU104 evaluation boards. Among these three, the Zybo Z7-20 and Xilinx ZCU104 are standard boards, whereas 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. An analog-to-digital converter (ADC) located on a capture board which is connected to the ChipWhisperer board using a cable is used to directly measure the voltage on the supply voltage pin of the FPGA. For the ChipWhisperer board, all decoupling capacitors that would otherwise be connected to the supply voltage to filter out voltage fluctuations have been removed. The other evaluation boards contain decoupling capacitors.

3.1 Power Wasting 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.

3.1.1 FF waster. The FF waster (Fig. 2a) includes 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, all capacitance between the Q output of the first flip-flop and the D-input of all fanout flip-flops is charged, which consumes power. This capacitive charging occurs through a distributed collection of repeaters and drivers along the net, and is not all sourced through a single gate at one position. This type of power wasting circuit creates a temporally-short switching event on a single clock edge, limiting its power-wasting capability.

3.1.2 RO waster. The RO waster (Fig. 2b) comprises a single-stage inverter chain that is enabled and disabled by a multiplexer. An RO waster oscillates at a high frequency and continuously consumes power, unlike the FF-based waster that exhibits instantaneous power consumption on the rising clock edge. The number of enabled ROs is a changeable parameter of this circuit, and it is varied between 0 and 10,000 in our experimentation. The RO wasters are implemented using FPGA look-up table (LUT) primitives.

3.1.3 Other power waster circuits. Although ROs have legitimate FPGA uses for voltage [20] and temperature [32] sensing, their association with malicious attacks makes them a target for cloud FPGA vendors. For example, the compilation software for Amazon EC2 F1 examines candidate netlists for ROs and flags them without generating an FPGA bitstream [6, 26]. As a result, several researchers have investigated circuits that consume high power similar to an RO, but do so by using FPGA circuits that would not be flagged; two such examples are high-speed sequential circuits with a clock generated from an on-FPGA phase-locked loop (PLL) [12], and unrolled block ciphers with long combination paths that inherently generate a large amount of glitching [22]. Krautter et al. [13], introduce another example of power waster circuits that evade netlist examination techniques by using apparently benign logic. They show successful examples of using multiple copies of an over-clocked AES encryption circuit as well as a generic ISCAS'89 benchmark circuit as malicious power wasting circuits for fault injection attacks. It is shown in [14] that many FPGA primitives can be used to generate power wasters that are not flagged by an analysis tool. These circuits include combinational loops made of multiplexer elements (MUX7 and MUX8), latch elements (LDCE), and carry logic (CARRY4). Because our objective in this work is understanding the effect of aggressive power consumption, we do not take any steps to make our power consumption circuits evade detection.

3.1.4 Waster Power Consumption. We compare the power consumption of FF and RO wasters. Previous researchers have either approximated the power consumption of RO wasters during synthesis or measured it in an experimental setup [14, 22]. Since the Xilinx power estimation tool (XPE) has low accuracy in estimating the power consumption of combinational logic circuits, we did not use it to estimate RO waster power consumption. The power consumption of the RO waster is approximately 1 milliWatt (mW) per instance based on measurements made by previous work [14]. We use the Vivado software power report to approximate the dynamic power consumption of the 3,000 FF wasters. We do so by toggling the wasters every clock cycle, and then estimating the total dynamic power consumption using the Vivado power report. We approximated the dynamic power consumption of a single FF waster to be 16 microWatts for the ChipWhisperer board. Therefore, a single RO power waster consumes as much dynamic power as approximately 63 FF power wasters. This large difference is due to the high toggling frequency of the combinational loop present in the RO waster which causes it to have a substantially higher dynamic power consumption.

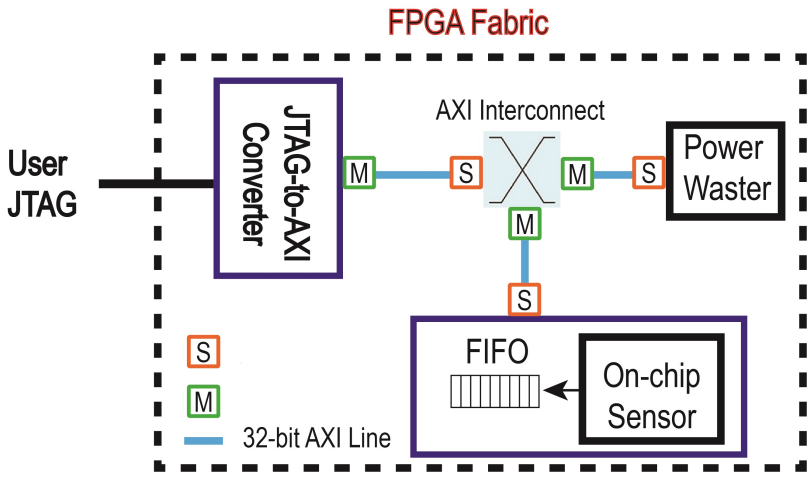


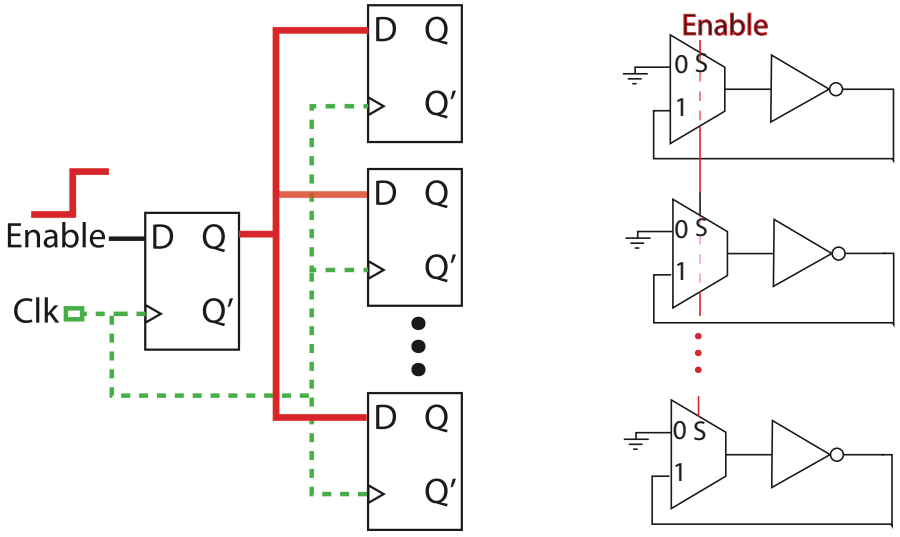
Fig. 1. Overview of the implemented architecture

3.2 Sensor Circuits

The RO sensors and TDC sensors that we use both log their data to FIFOs during experimental trials, as shown in Fig. 1.

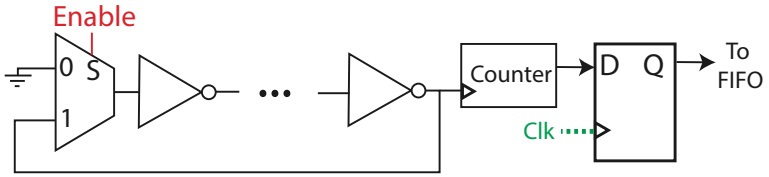
3.2.1 RO sensor. The RO sensor comprises an n-stage ring oscillator and an m-bit counter circuit that increments on each rising edge of the oscillator (Fig. 3a). The value of the counter is stored to flip-flops at each rising edge of the system clock, and the recorded sensor value is the difference, modulo 2^m to handle overflow, between the current and previous count. The sensor value therefore represents the number of oscillations that occurred during the preceding clock cycle.

3.2.2 TDC sensor. The TDC sensor (Fig. 3b) is composed of a configurable delay line leading to a series of CARRY4 (7-series) or CARRY8 (UltraScale+) 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 CARRY4 or CARRY8 primitives form a delay line with m taps, and each tap is attached to the data input of a flip-flop. At the rising edge of the system clock, each flip-flop samples the value from its tap in the carry chain. The Hamming weight of the m samples forms the output value of the TDC. The sensor output therefore indicates how far along the carry chain the rising edge has propagated during the preceding clock cycle. If propagation delay increases due to a lower supply voltage, then the rising edge will not travel as far along the chain during the clock cycle, and the Hamming weight will decrease. Compared to the RO sensor, the TDC sensor needs more careful manual placement and calibration to assure its delay is matched to the clock period, or else its output value can saturate to 0 or m. In this work, we use a TDC with 256 taps. The adjustable delay is adopted from our previous work [15] including fine and coarse adjustable tuning elements which have larger delay than CARRY4. If the output of TDC sensors saturates, the adjustable delay elements are able to tune Hamming weight close to the middle, which is 128 in our design, to achieve maximum margin from either end. The delay between each two TDC taps for the ChipWhisperer board that includes CARRY4 elements is approximated to be 25 ps based on timing reports generated by the Vivado software. Additionally, the delay of each coarse delay element is approximated as 300 ps, and the delay of each fine delay element is approximated as 50 ps.

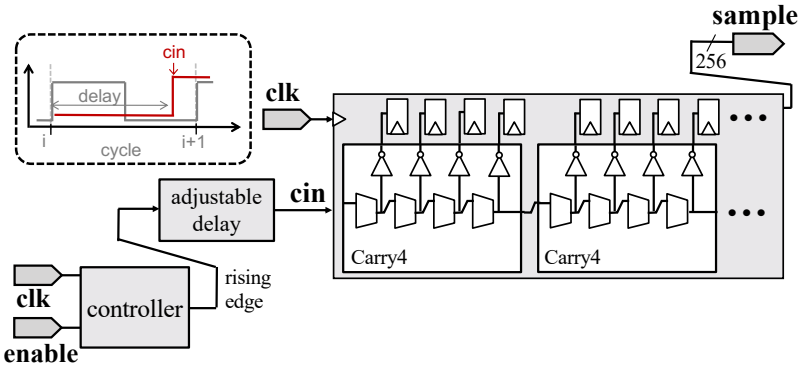


(a) FF Waster (b) RO Waster

Fig. 2. Schematic view of the power waster circuits



(a) Component of the RO Sensor



(b) TDC Sensor

Fig. 3. Schematic view of the sensor circuits

4 SUPPLY VOLTAGE SENSORS

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. First, we reconcile the sensor readings to externally measured voltage values. This comparison is made on the ChipWhisperer CW305 because that board is instrumented to allow voltage measurement, as shown in Fig. 4.

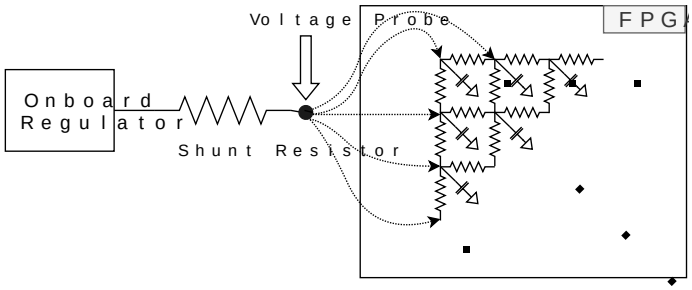


Fig. 4. PDN and measurement point for the ChipWhisperer CW305 board. Voltage measurements for the ChipWhisperer are obtained using an ADC on the capture board which is connected to the CW305 board via a cable.

Fig. 5 shows the values captured by the sensors during the time when RO power wasting circuits are active. The RO, TDC, and off-chip measurements are all affected in similar ways. Activation of the power wasting circuits causes a voltage drop, which is observed in three ways: the RO sensor value decrease, the TDC sensor values decrease, and a lower voltage is observed through the external voltage probe. To better show the response of the sensors and diminish noise, the plotted timeseries values of the TDC and RO are the averages over 500 repetitions of the experiment. The voltage measurements are from a single trial.

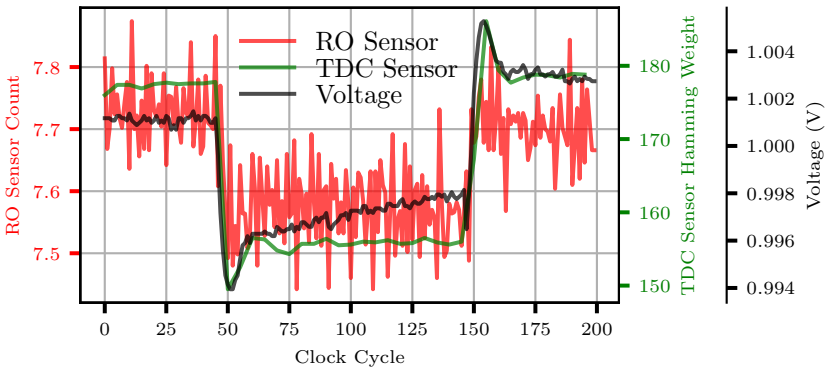


Fig. 5. Time series measurements from TDC sensor, RO sensor, and voltage measurements made by the ADC on the ChipWhisperer capture board when 100 RO power wasters are enabled at cycle 50 and disabled at cycle 150.

4.1 Principle of operation

Both the RO and TDC voltage sensors are based on the relationship between supply voltage and propagation delay in CMOS logic. Physically, this relationship exists because a reduction of supply voltage will reduce the MOSFET currents

that charge node capacitances, which in turn causes node voltages to change more slowly. As shown in Fig. 6, the sensor circuits that convert a continuously changing voltage into a sequence of quantized digital measurements can usefully be understood and modeled by decomposition into its constituent parts.

The first part of each sensor is a memory-less mapping from instantaneous supply voltage to instantaneous signal propagation velocity. Propagation velocity (distance along a path traversed per time) is simply the inverse of propagation delay (the amount of time to traverse a path segment). We assume for simplicity that each chip model has a single relationship between normalized velocity and voltage.

The RO and TDC sensors each utilize a signal that propagates, at a continuously varying velocity according to voltage fluctuations, along a path for a given time duration. In the RO sensor, this signal is the rising edge propagating around the oscillator loop. In the TDC sensor, this signal is the rising edge propagating through the carry chain. Integrating the propagation velocity of the signal over the measurement period yields the distance traveled by the signal through the circuit.

Finally, the circuit instantiated for the sensor creates a digital output based on the distance traversed by the signal during the measurement period. In an RO sensor, the digital output is the number of times the propagating rising edge passes the counter, which occurs once per $2n$-gates where n is the number of gates in the oscillator. In a TDC sensor, the digital output is the number of taps in the carry chain that are passed by the signal. Note that we can now observe why a TDC is more sensitive than an RO sensor; the distance traversed in order to increment the TDC sensor output has a typical delay on the order of 10ps at nominal voltage, equal to the delay of one carry stage in the carry4/carry8 element, while the distance traversed to increment the RO output has a typical delay on the order of 1ns (100x larger) at nominal voltage.

On-chip voltage sensors provide certain benefits compared to off-chip supply voltage measurements. The first benefit is the availability of on-chip voltage sensors in a remote FPGA setting where physical access to the FPGA and subsequently to the supply voltage is not available. Additionally, a TDC voltage sensor enjoys a very high measurement frequency (>200 MHz) which is limited in off-chip measurements. Finally, while the off-chip measurement is only limited to the supply voltage pin of the FPGA, on-chip sensors can be instantiated anywhere on the FPGA floorplan, and as close to the source of measurement as possible. This spatial advantage can allow the TDC sensor more closely follow the voltage fluctuation of different phenomena.

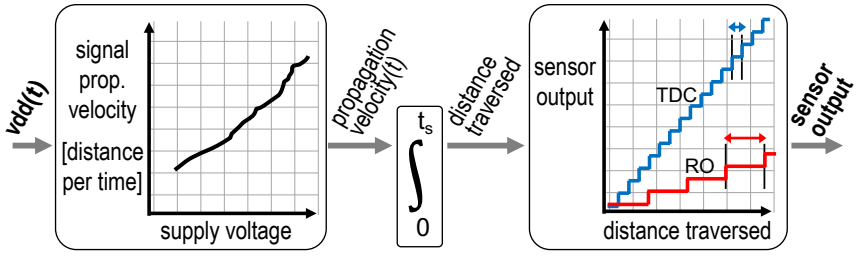


Fig. 6. Operating principle of delay-based voltage sensors. Voltage changes influence signal velocity, and the distance traveled by a signal within a fixed period determines the sensor output. Relative to the TDC, the RO sensor requires a signal to travel a larger distance for each increment in sensor output.

4.2 Sensor Calibration

The sensor operating principle that maps voltage to sensor values (Fig. 6) can also be used to map observed sensor values to voltages. However, as can be seen from Fig. 6, there are two important limitations to performing this latter mapping. First, when mapping the sensor output to the distance the signal has traversed to induce a change in value, there are a range of distances that correspond to the observed value due to quantization. Second, because the sensor value is based on the integration of signal propagation over a time period, we can only estimate a single representative value of the voltage that, if it were held constant during the measurement duration, would induce the observed output. Voltage fluctuation on a shorter timescale is not considered. This point is further addressed in Section 6.

To calibrate the relationship of voltage to sensor values, we use ROs with an extended integration time to minimize the impact of quantization error, and design the calibration experiment to rely only on the steady-state voltage that can reasonably be expected to remain constant over the integration time. By creating different steady-state voltages using activated wasters, and then measuring the sensor values and the voltage probe values during the steady state, we obtain corresponding values of voltage and sensor output. The obtained relationship is shown in Fig. 7. The voltage measurements for the ZCU-104 and Zybo Z7-20 boards are measured using the FPGA on-chip analog to digital converter (XADC) and recovered using the Xilinx system monitor software. For the ChipWhisperer, an ADC on the attached capture board is used for external voltage measurement. Our calibration approach is based on the assumption that the externally measured voltage is the same as the voltage at the location of the on-chip sensor. However, a voltage drop due to PDN resistance may cause the sensor voltage and external voltage to deviate somewhat. More precise calibration can be performed by varying the FPGA chip voltage using an external power supply [20]. However, that approach requires a destructive board modification, so we avoid it here.

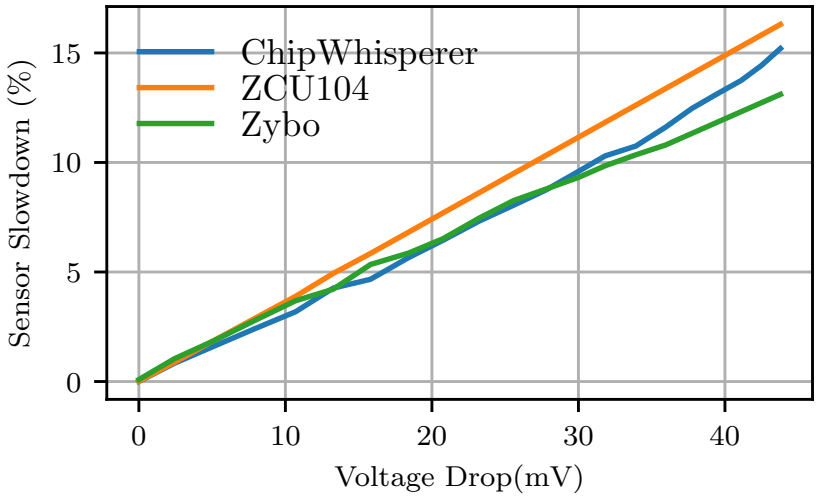
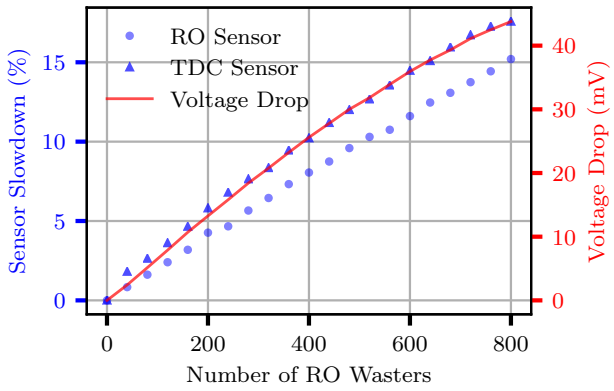


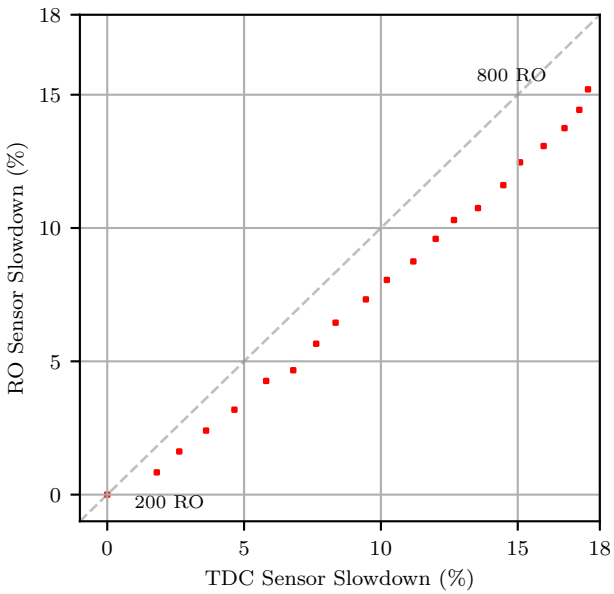
Fig. 7. Characteristic relationship between normalized delay and supply voltage. Normalized change in RO sensor delay is plotted against the measured supply voltage drop.

4.3 Consistency between sensors

We assess both ROs and TDCs to determine whether sensor readings are consistent when voltage is in a steady state (i.e. after the RO wasters are on for a period of time). Experimental results are shown in Fig. 8a. As more power wasters are activated, the voltage drops, a characteristic reflected similarly in the TDC and RO sensors. Fig. 8b shows a scatter plot of delay (representing voltage) from the RO and TDC sensors; the data falls near the 45-degree diagonal, which indicates that the two sensors are in agreement.



(a) Steady-state voltage measured by scope, RO, and TDC as the number of PWs is increased.



(b) Comparison of sensors' change in delay (representing voltage) when different numbers of ROs are activated shows good agreement between the sensor types.

Fig. 8. Slowdown of Sensors

4.4 Role of Shunt Resistor

As mentioned in Section 3, the ChipWhisperer board includes a shunt resistor for the evaluation of power-based side-channel attacks. In this subsection, we study the effects 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. 9 shows how bypassing the shunt resistor reduces the onboard voltage drop as observed by the RO sensors and TDC sensors. Different numbers of RO and FF wasters are turned on in two scenarios, with the shunt resistor present, and with the shunt resistor removed. For each experiment, the TDC and RO sensor measurements are collected and used to calculate sensor slowdown. This slowdown is converted into voltage drop, as shown in Fig. 7. The voltage drop for each experiment is also collected using the ChipWhisperer capture board ADC. While it is clear that the shunt would cause a larger voltage drop measured by the scope, it is interesting to confirm that the larger voltage change from the shunt is also detectable in the on-chip sensor measurements. 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. Likewise, minimizing the PDN impedance is helpful for preventing on-chip sensor-based measurement of power consumption.

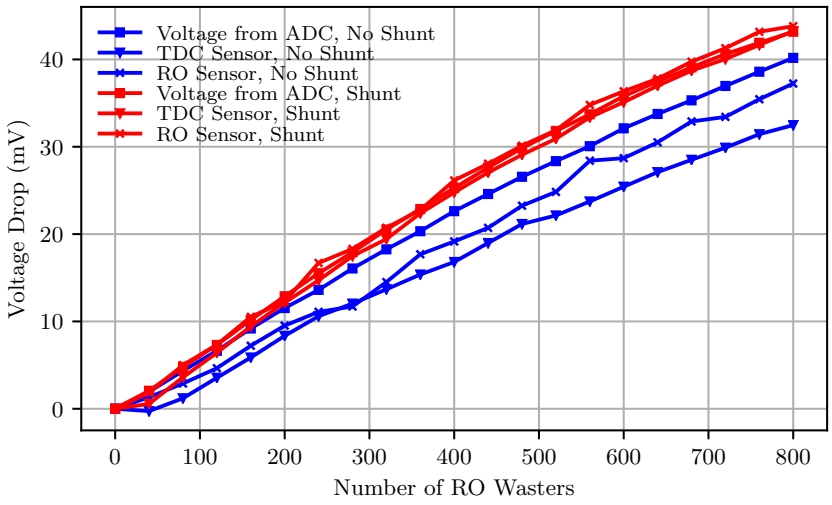


Fig. 9. Effect of bypassing shunt resistor with RO wasters. Measurements taken with shunt included show a lower voltage due to the voltage drop across the shunt. The voltage measurements are performed using the ADC on the ChipWhisperer capture board.

5 USING SENSORS TO MEASURE TRANSIENT VOLTAGES

The prior section showed that TDC and RO measure the same quantity and produce comparable results for DC voltages. In this section we show that the sensors have differing effectiveness in measuring transient voltage changes that occur over a very short time span. We run our experiments on FPGA platforms used in standard commercial applications, and, therefore, omit the ChipWhisperer board. In this section the experiments are performed using the Xilinx Zybo

Z7-20 evaluation board and the Xilinx ZCU104 evaluation board. Unlike the ChipWhisperer, both boards have a full complement of decoupling capacitors and lack a shunt resistor. The architecture shown in Fig. 1 was implemented on both ZCU104 and the Zybo z7-20 evaluation boards. The TDC in the ZCU104 was implemented using 32 Carry8 elements. The TDC in the Zybo z7-20 used 64 Carry4 elements. The clock frequency for both boards was set to 120 MHz.

5.1 Transient Voltage Behavior

In this section, the behavior of the FPGA-based TDC and RO sensors on the two production boards is compared. For each experiment, we collect measurements from both the RO and TDC sensors during power wasting experiments and calculate the sensor values during each clock cycle. Then, we use the data from Fig. 7 to convert the sensor slowdown into the sensed voltage drop. Each experiment is repeated 500 times and the average of the sensor measurements is used for slowdown calculation.

A total of 10,000 RO wasters for the ZCU104 board and 6,000 RO wasters for the Zybo Z7-20 board are turned on for 100 clock cycles each. The voltage regulation circuitry on the ZCU104 board is more resilient to voltage changes, and therefore requires a higher number of RO wasters to observe measurable effects. For the experiments with the FF wasters, a fanout of 10,000 was used by both boards. Like the RO waster experiments, the instantaneous voltage drop is captured using both TDC and RO sensors.

Fig. 10 shows the sensed voltage when each type of power waster is activated. Both sensors show similar performance in detecting the voltage drop caused by the RO wasters. However, with FF wasters, the RO sensor observes no voltage drop while the TDC sensor observes a small voltage drop. This difference in performance can be explained using the principle of operation of each sensor (Section 6). The integration time is defined as the time-span during which the voltage level of the FPGA affects the sensor components (t_s in Fig. 6). For the RO sensor, the temporal duration of the voltage drop caused by the FF waster is very small compared to the integration time of the sensor (8.3 ns with the 120 MHz clock). Therefore, the RO sensor is unable to sense the voltage drop caused by the FF waster even with multiple repetitions. The TDC sensor does not suffer from this limitation, since it has a shorter integration time, and its carry chain components are more sensitive to the delay caused by the voltage drop generated by the FF wasters.

This experiment highlights a fundamental problem of RO sensors in detecting short transient voltage drops caused by instantaneous switching of FPGA elements. The TDC sensor performs better, first due to a shorter integration time, and second because a smaller fractional change in the delay can change its output measurement. If needed, the integration time of the TDC sensor can be increased by either using a very long carry chain, or by taking many samples in consecutive clock cycles and merging them in a post-processing step. The second approach is more practical with a lower overhead.

5.2 Effect of Repeated Measurements

For both TDC and RO sensors, and for each type of power waster used, averaging values across different runs can increase the stability of the sensor measurements. In this section, we compare the speed with which sensor measurements, in the presence of FF wasters, converge after multiple repetitions using the ChipWhisperer board. Fig. 11a shows the recovered RO- and TDC-based sensor traces for different numbers of runs in the presence of 7,000 FF wasters activated at cycle 20. The TDC plots show that the TDC sensor detects the power waster activation even with just a single run. The RO plots show that the RO sensor is noisy and requires many traces to eliminate noise and show the expected finding.

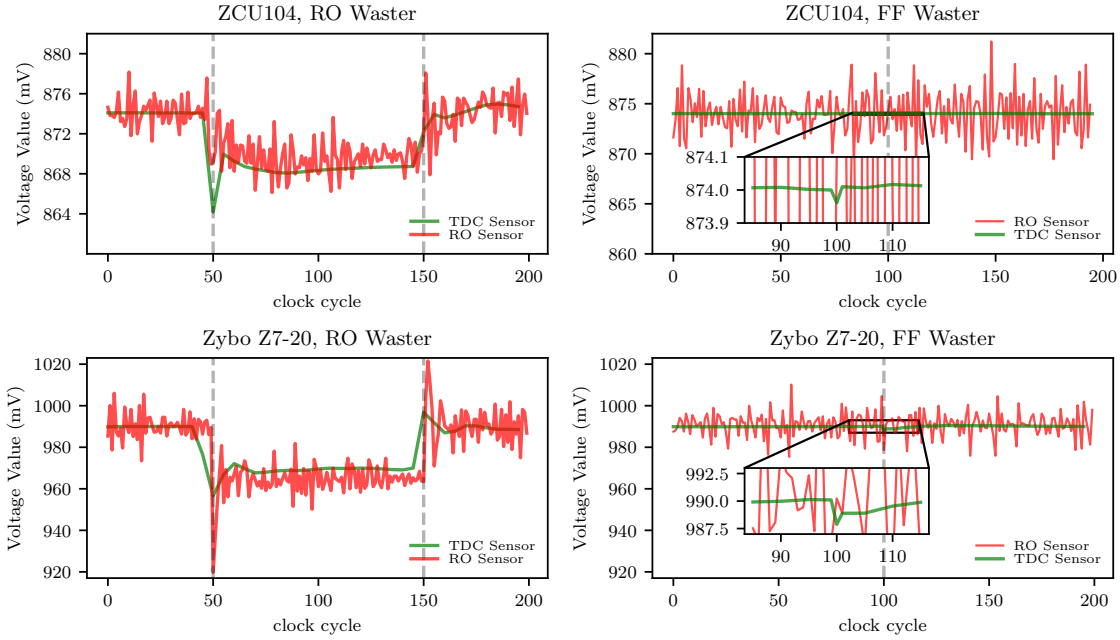
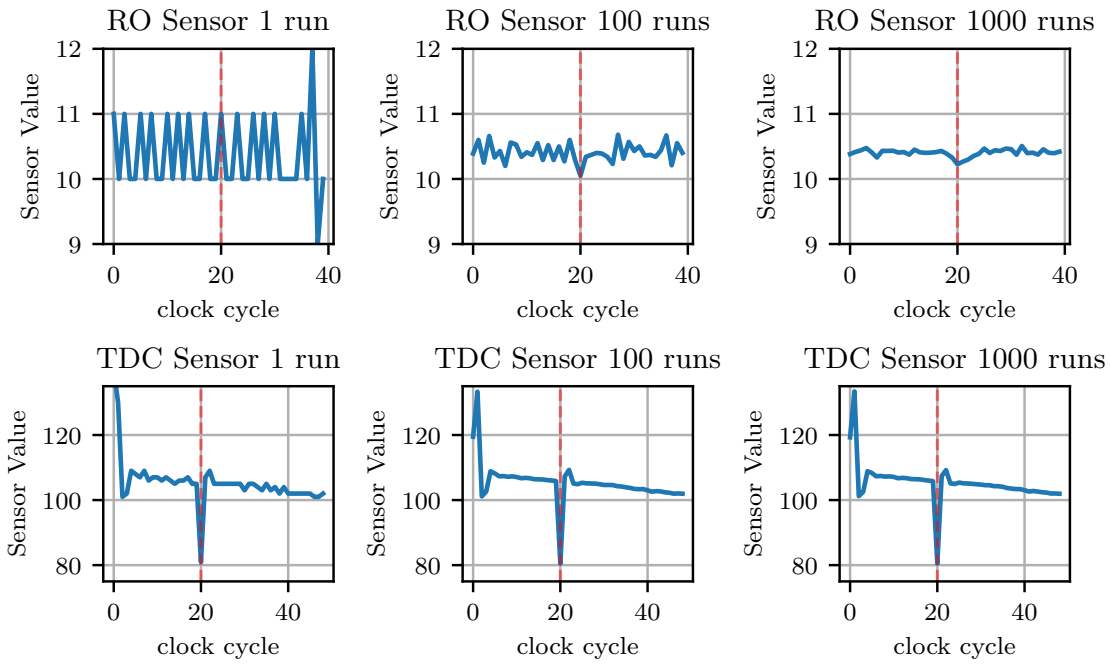


Fig. 10. Measuring voltage transients from each type of power waster using each type of sensor targeting two evaluation boards. The RO waster experiments use 10,000 RO wasters for ZCU104 and 6,000 RO wasters for Zybo Z7-20. The wasters turn on at clock 50 and turn off at clock 150. The FF waster experiments use 10,000 FF wasters that turn on at clock cycle 100. Each experiment is repeated 500 times.

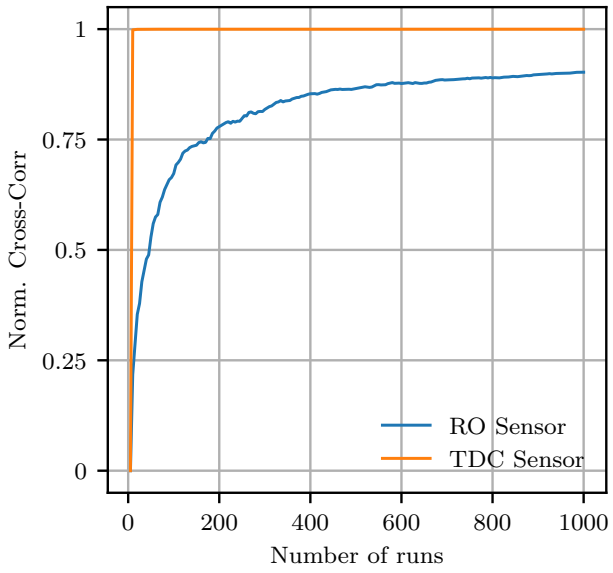
To quantify the speed of convergence, we compare the value of each sensor after different numbers of runs with a golden model, which is generated from running a separate experiment 1,000 times, and then averaging the resulting traces. We use a normalized cross-correlation metric for comparison. Fig. 11b shows the normalized cross-correlation between the average of n traces and the golden model, to demonstrate how quickly the average traces converge. The TDC sensor is able to achieve 99% correlation after only three runs, whereas the RO sensor does not reach this level of correlation even after 1,000 runs. This result shows the stability advantage of the TDC over the RO sensors.

6 TIME-INTERLEAVED TDC

Whereas the time resolution of the basic TDC and RO sensors is limited to one sample per clock cycle, we now propose an extension for characterizing sub-clock cycle transient supply voltage fluctuations. The sub-clock cycle time resolution is accomplished by using a TDC sensor to perform time-interleaved sampling. In the time-interleaved approach, we replay power attack scenarios multiple times, each time sampling the supply voltage at a different phase of the clock cycle. Although samples collected at different phases come from different trials, we treat them as if coming from a single trial and splice them in post-processing to reconstruct a single high-resolution time series of the supply voltage, as depicted in Fig. 12a. Splicing together data from different trials is possible because the supply voltage response to a given power wasting stimulus is observed to be consistent across trials as evidenced by Fig. 13. We call this sensor a *time-interleaved TDC*. A schematic of the implemented circuit is shown in Fig. 12b.



(a) Sensor traces averaged across different numbers of runs



(b) Correlation increasing with averaging

Fig. 11. Sensor data convergence with increased trial (run) count, (a) 7,000 FF wasters are turned on at clock cycle 20. The comparison in (b) is made with a golden model generated from running the experiment separately with 10,000 runs. These results were obtained with the ChipWhisperer CW305 board.

Because the time-interleaved TDC requires control over the attacking circuits in order to replay attacks, it is suitable for characterization, but not for use in the field where the attacking circuits are outside of the control of the sensing entity. However, we feel that it can nonetheless be an important analytical tool in lab environments where one has the ability to replay attacks or phenomena. Previous work [21], as well as our results using the FF power wasters in Fig. 10, both show the possibility of significant nanosecond voltage fluctuations that must be understood in order to effectively mitigate power attacks. The time-interleaved TDC can also be used to gain insight into side-channels provided that the attacker controls the victim circuit and is capable of replaying specific scenarios.

6.1 Observing detailed phenomena

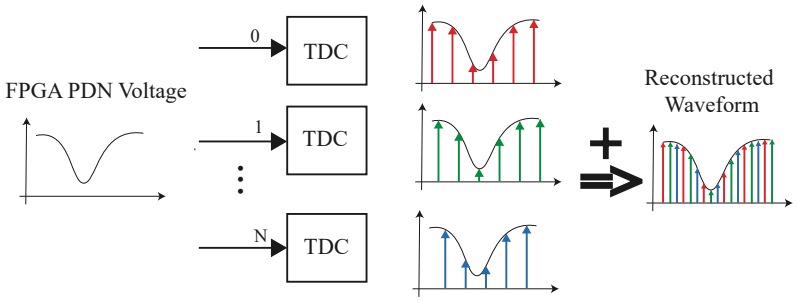
Fig. 14 illustrates the difference in the level of detail between data from an ordinary TDC and data from a time-interleaved TDC. Initially disabled with the circuit in idle state, 1600 RO power wasters are activated at time 2.56 μs causing a voltage drop which manifests itself on the TDC sensors as a drop in the Hamming weight of the samples. Using an ordinary TDC that samples at the frequency of the system clock (100 MHz, 10ns sample interval) the initial drop can be observed as a single data point before the voltage settles into its new steady state. However, the time-interleaved TDC takes measurements at small intervals between successive clock edges and therefore creates a much clearer picture of how the voltage changes in response to the attack. It achieves this by repeating the experiment 560 times and shifting the TDC clock phase for each experiment. The size of the phase shift is determined by the MMCM primitive which is capable of shifting its input clocks in increments of $1/56^{\text{th}}$ of the period of the voltage controlled oscillator (VCO). Therefore, when the VCO frequency is 1 GHz, as is in our case, each phase step represents a 17.857 ps shift. With this level of accuracy not only is the initial drop visible in more detail but also the smaller fluctuations following the main drop as the voltage stabilizes.

6.2 Frequency response and filtering

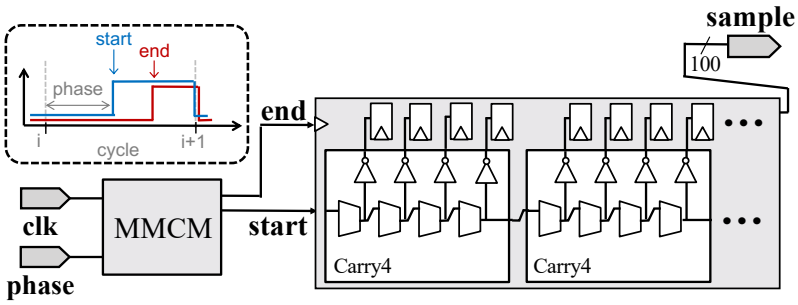
The usefulness of the time-interleaved TDC is not limited to just observing active phenomena. Fig. 15a shows time series measurements taken by a TDC and a time-interleaved TDC over a 100 ns period during which nothing of interest is happening on the chip. The different time resolutions of the two sensors allow for observing different sources of undesirable measurement noises. While the regular TDC sensor allows one to see voltage fluctuations in the order of kHz to low MHz in the frequency domain, the sub-clock cycle resolution of the time-interleaved TDC reaches into the GHz range. Most interestingly the time-interleaved TDC is able to pick up the frequency at which the rest of the logic on the chip is running. Even without any complex processing, just by averaging multiple traces from the time-interleaved TDC and finding the running average of the resulting mean trace, the ripples caused by the logic being switched by the system clock become clearly visible in Fig. 15a. The same can be observed by taking the Fourier transform of the time series, as shown in Fig. 15b. where the spike at 100 MHz corresponds to the the system clock frequency while the rest of the spectrum is less noisy overall compared to that of the regular TDC.

6.3 Potential effects of temperature change on the time-interleaved TDC measurements

It is important to consider whether temperature variations across samples collected at different phases may affect the time-interleaved TDC in a way that results in a subpar reconstruction of the high-resolution trace. The effect of temperature on on-chip voltage sensors has been studied previously. In Tian and Szefer [27], the temporal effects of temperature on the measurements of an RO sensor were examined. Their experiments show that ring oscillator-based heaters (implemented with 8,000 FPGA ALMs) require 1 minute to increase the temperature of an Intel Stratix



(a) Sample splicing in time-interleaved TDC sensor.



(b) Design uses clock management primitive to control phase.

Fig. 12. Operation of time-interleaved TDC sensor

V FPGA by 2° C, resulting in a 0.5% sensor slow down. TDC sensors have a behavior similar to RO sensors in the presence of temperature changes due to similarities in the way they translate logic path delay into digital values. Our controlled experiments with the time-interleaved TDC keep the power wasters on for less than 50 μs during each sample, and provide enough time between samples (after each phase change) for cooling, to assure the aggregate heating has a negligible effect on the final reconstructed TDC result. If the time-interleaved TDC is used in an uncontrolled environment, temperature may fluctuate from an extended period of power waster activity or different environments across experiments. It would be then necessary to evaluate and compensate for potential distortions in TDC measurements, which is beyond of the scope of this paper and can be addressed in future work.

6.4 Time-based correction in TDC

A practical limitation of any TDC, because TDCs use propagation delay as a proxy for supply voltage, is that the delays between TDC taps are non-uniform. The staircase pattern at the right side of Fig. 6 is actually less regular than what is depicted there. This can introduce error in TDC-based voltage estimates if no correction is applied.

We use code density test [25][18] to measure the bin width of each TDC stage. To perform the code density test, we add an inverting feedback loop from `cout` of the final TDC stage, back to `cin` of the first TDC stage, such that it becomes a free-running oscillator through the carry chain. We then repeatedly sample the TDC on the system clock to capture snapshots of the oscillator state. Because the oscillator is free-running and uncorrelated to the system clock, its phase when the sample is taken should be uniformly distributed. Under this assumption, a rising edge may be found at any position within a sample. If a rising edge is frequently found in a bin demarcated by two particular taps, that will

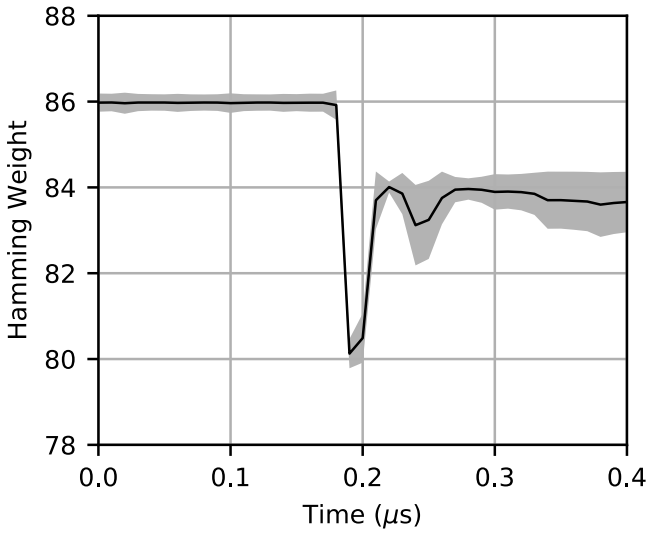


Fig. 13. TDC sensor response to a power attack. The shaded region represents all the samples that fall within one standard deviation of the mean response over 9800 separate trials.

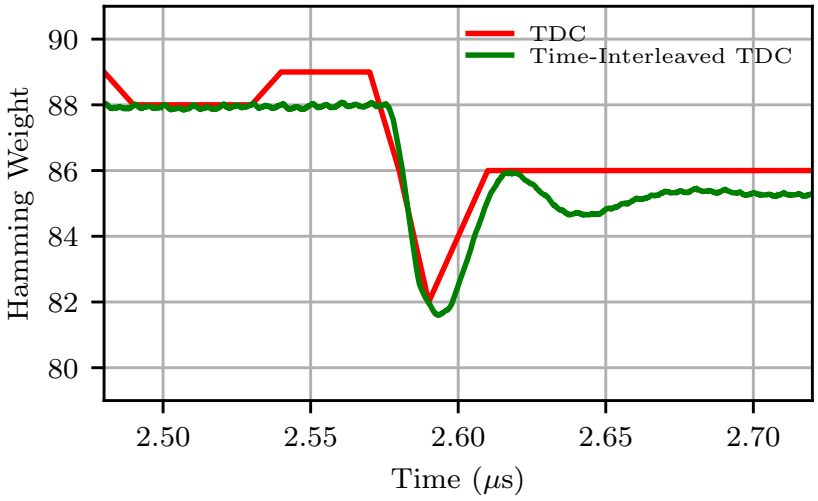
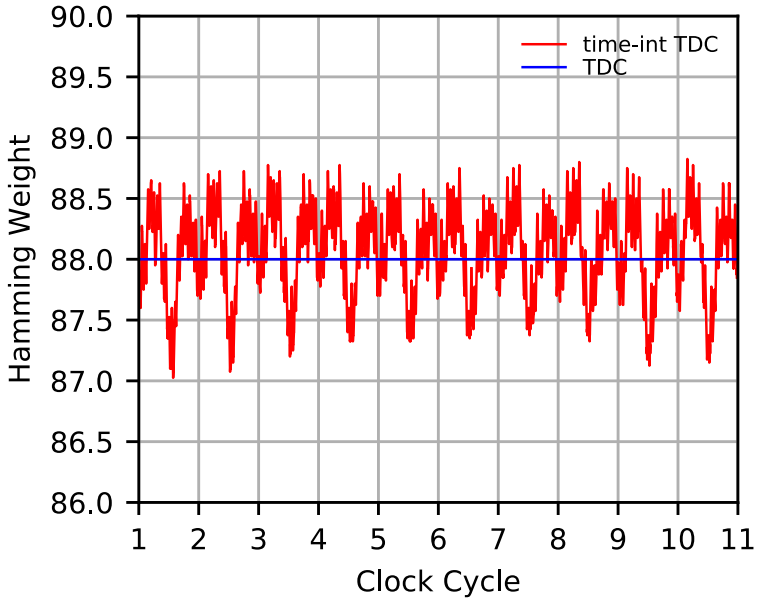
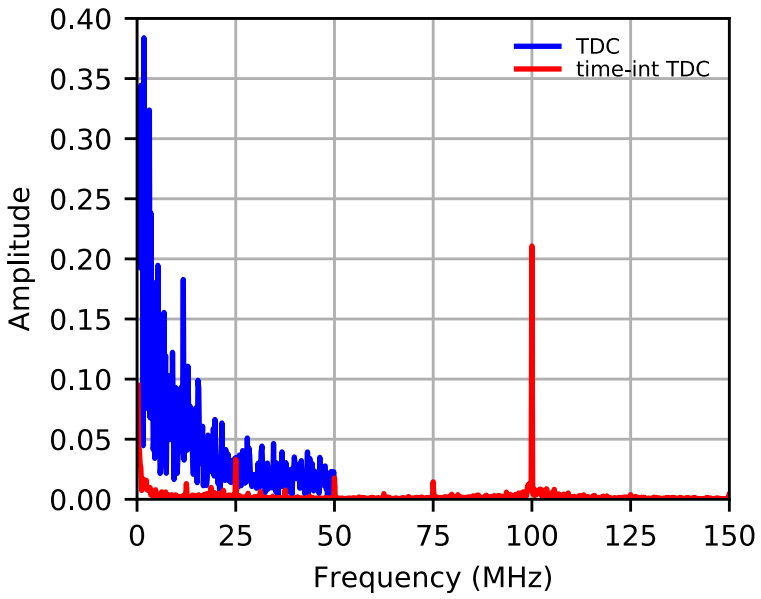


Fig. 14. Fine-grained response to an oscillator-based power attack as measured by TDC and time-interleaved TDC.

indicate a high delay between the taps, which is causing high probability of randomly finding the rising edge to be there. Likewise, bins that rarely capture the rising edge are expected to have a low delay between taps. In this way, one can learn the bin widths from statistical analysis of the samples.



(a) Regular TDC and time-interleaved TDC sensor data captured during an idle period.



(b) Fourier spectra of TDC and time-interleaved TDC data reveal that only the time-interleaved TDC can pick up periodic voltage fluctuations at frequencies higher than the main clock. The spike observed at 100 MHz corresponds to the clock frequency of on-chip logic.

Fig. 15. Idle sensor data and its frequency breakdown

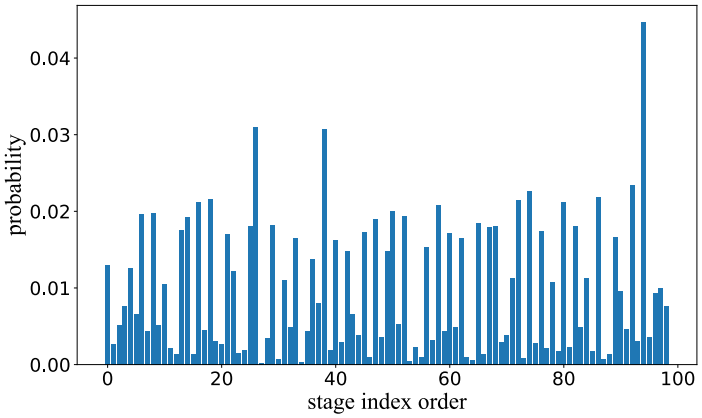


Fig. 16. Uneven bin sizes of TDC stages.

Because our code density analysis uses only the rising edges, we consider as valid only trials in which a rising edge is found within the sample, and discard other trials. The samples with rising edges are identified by having the earliest stage capture a 1-value and the latest stage capture a 0-value. The stages between will necessarily have a transition from 1 to 0 at some intermediate bin, which is the bin hit by the rising edge. After 1,000,000 trials, the probability of each stage being hit is shown in Fig. 16. This result does indeed reveal the delays to be non-uniform, which is known to be due largely to non-uniform routing between the carry chain and the d inputs of the corresponding flip-flops that collect the samples [15].

The results of the code density test are used to correct TDC-based voltage estimates on the Zybo Z7-20 board. To test the accuracy of the measurements, we instantiate various numbers of RO power wasters to induce voltage fluctuations, and we collect as ground truth the voltage sensed by the on-chip XADC, which is a 12-bit ADC that provides precision on the order of 1mV. We only use steady-state voltages when comparing TDC to XADC, in order to accommodate the low sample rate of the XADC. The number of activated RO power wasters is varied from 0 up to 6,000 in steps of 200. The start and stop signal are separated by 20 degrees of phase, which corresponds to 2.22 ns given the 25MHz frequency system clock.

To make a fair comparison, we convert the TDC output to slowdown using a conversion based on Hamming weight, and also make the same conversion based on the code density test results from Fig. 16. In both cases, the slowdown is mapped to voltage using the relationship shown in Fig. 7. The result comparing the two TDC-based voltage estimates to the XADC ground truth is shown in Fig.17. As can be observed in that plot, the code density test is closer to the ground truth than is the result based on Hamming weight alone. This finding indicates that the calculation from code density test shows a more accurate voltage measurement, when compared with use of Hamming weight alone.

7 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

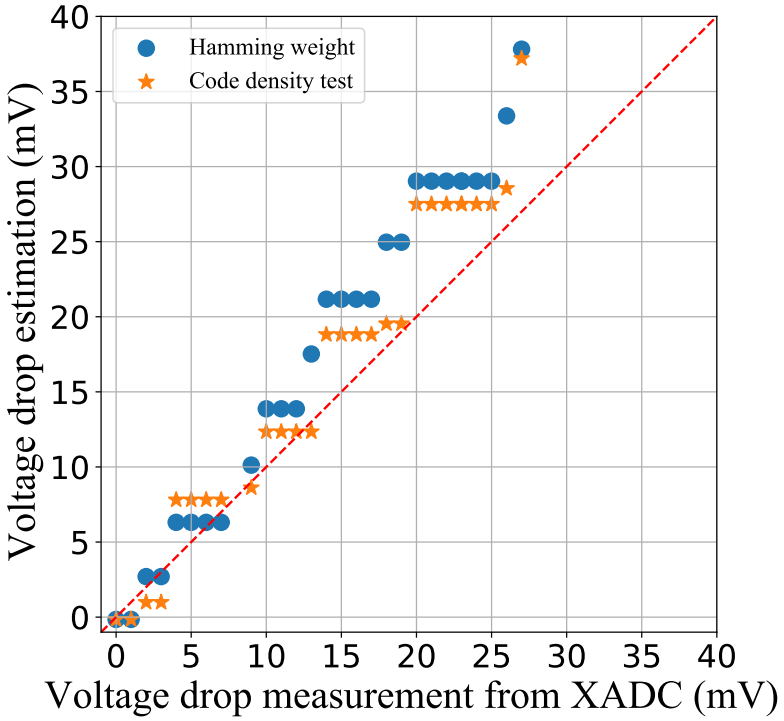


Fig. 17. Voltage measurement comparison.

detecting circuit slowdown. The effect of the ChipWhisperer shunt resistor in accentuating the voltage drop was also studied. Based on experiments targeting a Xilinx Zynq UltraScale+ and a Xilinx 7-series Zynq evaluation board, the TDC sensor has higher sensitivity in detecting small voltage drops. Consistent with prior work [33], 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. Furthermore, we show that for characterization experiments, the TDC can be used in a time-interleaved manner to reconstruct sub-clock cycle voltage fluctuations. In future work, experimental evaluation of temperature-related changes in TDC measurements during extended use of power wasters and compensation methods to address potential issues can be studied. 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, CNS-1749845, and CNS-1563829.

REFERENCES

[1] Md Mahbub Alam, Shahin Tajik, Fatemeh Ganji, Mark Tehranipoor, and Domenic Forte. 2019. RAM-Jam: Remote Temperature and Voltage Fault Attack on FPGAs using Memory Collisions. In *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. 48–55.

[2] Alessandro Balla, Matteo Mario Beretta, Paolo Ciambrone, Maurizio Gatta, Francesco Gonnella, Lorenzo Iafolla, Matteo Mascolo, Roberto Messi, Dario Moricciani, and Domenico Riondino. 2014. The characterization and application of a low resource FPGA-based time to digital converter. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 739 (2014), 75–82.

[3] Andrew Boutros, Mathew Hall, Nicolas Papernot, and Vaughn Betz. 2020. Neighbors from Hell: Voltage attacks against deep learning accelerators on multi-tenant FPGAs. In *2020 International Conference on Field-Programmable Technology (ICFPT)*. IEEE, 103–111.

[4] Digilent Inc. [n. d.]. Zybo Z7 Reference Manual. https://reference.digilentinc.com/reference/programmable-logic/zybo-z7/reference-manual

[5] Ilias Giechaskiel, Kasper Rasmussen, and Jakub Szefer. 2020. C3APSULe: Cross-FPGA covert-channel attacks through power supply unit leakage. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*. 1728–1741.

[6] Ilias Giechaskiel, Kasper Bonne Rasmussen, and Jakub Szefer. 2019. Measuring long wire leakage with ring oscillators in cloud FPGAs. In *International Conference on Field Programmable Logic and Applications (FPL)*. 45–50.

[7] Ognjen Glamočanin, Louis Coulon, Francesco Regazzoni, and Mirjana Stojilović. 2020. Are cloud FPGAs really vulnerable to power analysis attacks?. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 1007–1010.

[8] Dennis RE Gnad, Cong Dang Khoa Nguyen, Syed Hashim Gillani, and Mehdi B. Tahoori. 2019. Voltage-based Covert Channels in Multi-Tenant FPGAs. *IACR Cryptol. ePrint Arch.* 2019 (2019), 1394.

[9] Dennis R.E. Gnad, Fabian Oboril, Saman Kiamehr, and Mehdi B. Tahoori. 2016. Analysis of transient voltage fluctuations in FPGAs. In *International Conference on Field-Programmable Technology*. 12–19.

[10] Dennis RE Gnad, Fabian Oboril, and Mehdi B Tahoori. 2017. Voltage drop-based fault attacks on FPGAs using valid bitstreams. In *2017 27th International Conference on Field Programmable Logic and Applications (FPL)*. IEEE, 1–7.

[11] Ahmed Khawaja, Joshua Landgraf, Rohith Prakash, Michael Wei, Eric Schkufza, and Christopher J. Rossbach. 2018. Sharing, Protection, and Compatibility for Reconfigurable Fabric with AMORPHOS. In *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*. 107–127.

[12] Jonas Krautter, Dennis RE Gnad, and Mehdi B Tahoori. 2019. Mitigating Electrical-level Attacks towards Secure Multi-Tenant FPGAs in the Cloud. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)* 12, 3 (2019), 1–26.

[13] Jonas Krautter, Dennis RE Gnad, and Mehdi B Tahoori. 2021. Remote and Stealthy Fault Attacks on Virtualized FPGAs. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 1632–1637.

[14] Tuan Minh La, Kaspar Matas, Nikola Grunchevski, Khoa Dang Pham, and Dirk Koch. 2020. FPGADefender: Malicious self-oscillator scanning for Xilinx UltraScale+ FPGAs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)* 13, 3 (2020), 1–31.

[15] Xiang Li, Peter Stanwicks, George Provelengios, Russell Tessier, and Daniel E. Holcomb. 2020. Jitter-based Adaptive True Random Number Generation for FPGAs in the Cloud. In *International Conference on Field-Programmable Technology*. 112–119.

[16] Kaspar Matas, Tuan Minh La, Khoa Dang Pham, and Dirk Koch. 2020. Power-hammering through Glitch Amplification–Attacks and Mitigation. In *IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*. 65–69.

[17] Shayan Moini, Xiang Li, Peter Stanwicks, George Provelengios, Wayne Burleson, Russell Tessier, and Daniel Holcomb. 2020. Understanding and Comparing the Capabilities of On-Chip Voltage Sensors against Remote Power Attacks on FPGAs. In *IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*. 941–944.

[18] Manuel Mota and Jorgen Christiansen. 1999. A high-resolution time interpolator based on a delay locked loop and an RC delay line. *IEEE Journal of Solid-State Circuits* 34, 10 (1999), 1360–1366.

[19] Colin O'Flynn and Zhizhang David Chen. 2014. Chipwhisperer: An open-source platform for hardware embedded security research. In *International Workshop on Constructive Side-Channel Analysis and Secure Design*. 243–260.

[20] George Provelengios, Daniel Holcomb, and Russell Tessier. 2019. Characterizing Power Distribution Attacks in Multi-User FPGA Environments. In *International Conference on Field Programmable Logic and Applications (FPL)*. 194–201.

[21] George Provelengios, Daniel Holcomb, and Russell Tessier. 2020. Power distribution attacks in multitenant FPGAs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 28, 12 (2020), 2685–2698.

[22] George Provelengios, Daniel Holcomb, and Russell Tessier. 2020. Power wasting circuits for cloud FPGA attacks. In *30th International Conference on Field-Programmable Logic and Applications (FPL)*. IEEE, 231–235.

[23] Falk Schellenberg, Dennis RE Gnad, Amir Moradi, and Mehdi B Tahoori. 2018. Remote inter-chip power analysis side-channel attacks at board-level. In *International Conference on Computer-Aided Design*. 1–7.

[24] Linda L Shen, Ibrahim Ahmed, and Vaughn Betz. 2019. Fast voltage transients on FPGAs: Impact and mitigation strategies. In *2019 IEEE 27th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*. IEEE, 271–279.

[25] Jian Song, Qi An, and Shubin Liu. 2006. A high-resolution time-to-digital converter implemented in field-programmable-gate-arrays. *IEEE Transactions on Nuclear Science* 53, 1 (2006), 236–241.

[26] Takeshi Sugawara, Kazuo Sakiyama, Shoei Nashimoto, Daisuke Suzuki, and Tomoyuki Nagatsuka. 2019. Oscillator without a combinatorial loop and its threat to FPGA in data centre. *Electronics Letters* 55, 11 (2019), 640–642.

[27] Shanquan Tian and Jakub Szefer. 2019. Temporal thermal covert channels in cloud FPGAs. In *ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*. 298–303.

[28] Xilinx Corporation 2018. *ZCU104 User's Guide*. Xilinx Corporation.

[29] Zhoujiancheng Yin, Shubin Liu, Xinjun Hao, Shanshan Gao, and Qi An. 2012. A high-resolution time-to-digital converter based on multi-phase clock implement in field-programmable-gate-array. In *2012 18th IEEE-NPSS Real Time Conference*. IEEE, 1–4.

[30] Mark Zhao and G Edward Suh. 2018. FPGA-based remote power side-channel attacks. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 229–244.

[31] Shuze Zhao, Ibrahim Ahmed, Vaughn Betz, Ashraf Lotfi, and Olivier Trescases. 2018. Frequency-domain power delivery network self-characterization in FPGAs for improved system reliability. *IEEE Transactions on Industrial Electronics* 65, 11 (2018), 8915–8924.

[32] Kenneth M. Zick and John P. Hayes. 2012. Low-cost sensing with ring oscillator arrays for healthier reconfigurable systems. *ACM Transactions on Reconfigurable Technology and Systems* 5, 1 (2012).

[33] Kenneth M Zick, Meeta Srivastav, Wei Zhang, and Matthew French. 2013. Sensing nanosecond-scale voltage attacks and natural transients in FPGAs. In *ACM/SIGDA International Symposium on Field Programmable Gate Arrays*. 101–104.