AN ABSTRACT OF THE THESIS OF

Daniil Lytikov for the degree of Master of Science in Electrical and Computer Engineering

presented on March 22, 2024.

Title: Investigating Time-Digital-Converters for Hardware Security in FPGAs

Abstract approved: _____

Vincent Immler

In this comprehensive thesis, we present a series of experiments and findings that highlight the critical importance of TDC Voltage Sensors in the hardware security domain. Our research begins by introducing a novel self-calibrating module, demonstrating its efficiency through preliminary calibration tests. We then delve into the Peak-to-Peak tests, which underscore the significance of calibration in achieving optimal quantization levels for glitch detection, while also discussing the trade-offs between delay line lengths. We investigate two types of power consumption devices, RO and SC arrays, revealing their distinct advantages and the need for designers to carefully consider their implementation based on specific requirements. Moving forward, we explore the mapping of TDC Voltage sensors and the effectiveness of power consumption modules across various positions on a circuit board, emphasizing their adaptability and potential threat of using them by malicious actors. Furthermore, our noise test showcases the potential exploitation of SC arrays in fault injection attacks, drawing attention to the need for countermeasures to prevent their misuse. Additionally, we highlight the protective potential of power consumption modules in obscuring sensitive side-channel information. In summary, our research underscores the critical role of TDC delay line-based sensors, calibration techniques, and power consumption arrays in hardware security. These findings advocate for their strategic incorporation into hardware architecture as a preemptive measure against potential design vulnerabilities, ultimately contributing to the advancement of robust hardware security solutions.

Investigating Time-Digital-Converters for Hardware Security in FPGAs

by

Daniil Lytikov

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Master of Science

Presented March 22, 2024
Commencement June 2024

Master of Science thesis of Daniil Lytikov presented on March 22, 2024.

APPROVED:

Major Professor, representing Electrical and Computer Engineering

---

Head of the School of Electrical Engineering and Computer Science

---

Dean of the Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Daniil Lytikov, Author

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF FIGURES (Continued)

Figure Page

LIST OF TABLES

Chapter 1: Introduction

In an era where digital technologies continue to advance at an unprecedented pace, the security of hardware systems has emerged as a paramount concern. With the ever-increasing reliance on digital infrastructure, protecting sensitive data and ensuring the reliability of electronic devices have become critical imperatives. One particularly insidious threat to hardware security is the manipulation of voltage levels, commonly known as Voltage Glitch attacks. These attacks pose significant risks, potentially compromising the integrity of hardware systems and, consequently, the security of sensitive information. The thesis we present here stems from a pressing need to address this looming threat. In our research, we delve into the world of TDC (Time-to-Digital Converter) Voltage Sensors, a promising avenue for detecting and mitigating Voltage Glitch attacks. Our motivation stems from the urgency to develop effective countermeasures against malicious actors who may exploit these vulnerabilities in various contexts. As we navigate the intricate landscape of TDC Voltage Sensors, calibration techniques, and power consumption arrays, our aim is to shed light on their potential and their role in bolstering hardware security. Through a series of meticulously designed experiments and findings, we not only showcase their effectiveness but also underscore the need for careful consideration in their implementation. Our work seeks to empower hardware security developers with the knowledge and tools necessary to safeguard against Voltage Glitch vulnerabilities.This thesis is a testament to the critical importance of proactive hardware security measures in an increasingly interconnected and data-driven world. It is a call to action for researchers, engineers, and practitioners to embrace innovative approaches to protect the very foundation of our digital ecosystem – the hardware itself.

1.1 Related Work

There are two main types of voltage sensors commonly used for measuring power consumption: delay-line based sensors [142, 139, 89, 88, 41, 108, 123] and ring-oscillator based sensors [89, 44, 53, 86, 101, 129, 130] . Both designs utilize propagation delay as a means of measuring supply voltage, as it is well-established that reduced supply voltage leads to heightened propagation delay. In Section 1.1.2 we discuss related works of delay-line based TDCs, and in 1.1.3 TDCs based on ROs.

Afterwards, various hardware security applications and their dependency on TDCs are presented in Section 1.1.4.

1.1.1 Definition of Terms

TDC (Time-to-Digital Converter) - A high-resolution time measurement design capable of measuring time intervals in the nanosecond to the picosecond range, constructed using reprogrammable logic elements of the FPGA that offer versatile configurations for capturing fluctuations in propagation delays of the logic units, thus monitoring variations in the supply voltage.

Calibration - a procedure of ensuring the accuracy and reliability of the time measurements made by the TDC, which depends on various factors such as manufacturing tolerances, temperature variations, and voltage fluctuations.

Calibration (delay line based sensor) - the process of adjusting and fine-tuning settings of the sensor to ensure accurate and reliable measurements. This includes setting the appropriate delay time of the basic elements, phase shift of the reference signals, compensating for any environmental factors that could affect the sensor's performance, and aligning it with a reference standard for dependable comparisons.

Calibration (ring oscillator based sensor) - the process of adjusting and fine-tuning settings of the sensor to ensure accurate and reliable measurements. This involves adjusting factors such as the frequency, period of oscillation, compensating for any environmental conditions that could affect the sensor's performance, and aligning it with a reference standard for dependable measurements.

1.1.2 TDCs: Designs based on Delay-Line

TDCs based on a delay-line, as seen in Figure 1.1, is affected by fluctuations in the FPGA's PDN resulting from the FPGA's switching activity. These fluctuations in turn lead to a delay shift of a signal passing through the sequence of logic elements that comprise the delay-line. Sampling the logic elements within the delay line provides a measurement value that corresponds to the voltage drop within the PDN.

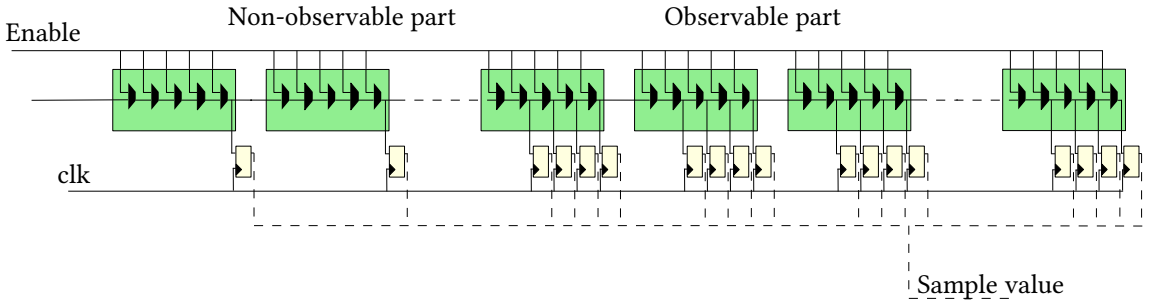

Figure 1.1: TDC delay line sensor schematic

The delay line in TDCs generally consists of both observable and non-observable segments. The non-observable part constitutes the initial segment of the delay line, which is not connected to the registers. It functions as an initial delay and is configured during the calibration process. On the other hand, the observable segment is the portion of the sensor that is connected to the registers, allowing for the monitoring of the signal propagation delay through the line.

When implementing delay line Time-to-Digital Converters (TDCs) on FPGAs, the choice of delay units is one of the primary structural parameters for evaluating their performance and versatility. There are two common delay element implementations are based on Look-Up Tables (LUTs) and Carry 4 units. The selection between LUT and Carry 4 based TDCs hinges on the specific needs of the application, considering factors such as resolution requirements, resource utilization, and desired precision. Both implementations have their unique advantages and trade-offs, making it is essential to carefully assess the project's demands to determine the most suitable delay unit for the delay line based TDC design.

LUT based TDCs leverage the FPGA's configurable logic blocks to create delay elements. The main benefits of this design are the less area overhead, and accessibility, since it is available in any FPGA. Conversely, designs utilizing carry-chain primitives advantages in one of the primary parameters of the sensor resolution. The distance traversed in order to increase the carry output has a common delay on the order 10 ps for fine grain, and 115 ps for coarse grain element at nominal voltage. While the delay between two LUT delay elements is 300ps, based on the Vivado report. Thus, Carry 4 delay line implementations are able to accurately capture the smallest time intervals on the FPGA, enabling precise measurements and higher sensitivity for voltage fluctuations on the chip. To save area of the sensor, having finest resolution per bit Schellenberg et al. [108] suggested a solution of using a combination of Carry 4 delay elements for the observable part, and LUT for the non-observable.

Dynamic range (the number of taps) is another critical parameter in sensor applications. It

defines the range of time intervals that a TDC can measure accurately. Widening the dynamic range is essential for capturing a wide variety of events, from short pulses to long time intervals. Early TDC designs often featured relatively small numbers of taps, limiting their dynamic range and resolution. For instance, a 16-tap delay line would yield a coarser time measurement compared to a 256-tap delay line. Researchers have conducted extensive investigations to understand the relationship between tap count and TDC performance. Chen et al. (2003) [20] and Liu et al. (2015) [76] have explored the impact of varying tap counts on resolution, linearity, and power consumption. Presently, it is common to encounter TDCs with 64 taps [11, 127] and 256 taps [89, 88, 123] delay lines. The 64-tap delay line is suitable for applications where a moderate level of the range is sufficient, while the adoption of 256 taps is motivated by the quest for larger dynamic range. Thus, our design of the sensor has 90 taps, intending to strike a balance between range of the measurement and resource utilization, conserving more area of the FPGA.

TDC linearity is another parameter that can enhance accurate measurements across the entire dynamic range. Linearity in TDC delay line-based sensors pertains to the correlation between the real propagating signal and the resulting values produced by the delay line. Non-linearity, on the other hand, refers to deviations from this ideal linear relationship, introducing errors in the measurements, particularly in applications requiring high accuracy.

In the context of linearity of TDCs LUT based delay line sensors advantages over Carry 4 delay line sensors. LUT based TDCs are fundamentally digital in nature and feature uniform delay intervals between their basic elements. Thus, it provides highly linear responses when properly designed and calibrated. Niu et al. (2018) [96] have explored techniques for achieving high linearity in LUT based TDCs through careful selection of delay elements and calibration methods. In contrast, TDCs based on Carry 4 delay lines may exhibit non-linearities due to the inherent analog nature of the delay elements in the delay line. These delay elements can introduce small variations in delay with temperature, voltage, and process variations, leading to non-linearities in the TDC's response. Research by Zhang et al. (2019) [134] delves into methods to mitigate non-linearity in Carry 4 delay line TDCs, including temperature compensation and digital correction techniques. One common approach to mitigate non-linearity in Carry 4 delay line TDCs is through the use of code density tests using a ring oscillator. In this technique, a ring oscillator is integrated into the TDC design, serving as a stable and known-frequency clock source. A range of input codes, spanning the TDC's measurement range, is applied to initiate time measurements. The TDC records the output codes corresponding to these inputs, effectively capturing the time intervals. By analyzing the distribution or density of these output codes across the measurement range, deviations from ideal linearity can be identified. Through this method,

insights into the nature of non-linearity are gained, and correction algorithms can be developed and applied to the TDC's output codes, ultimately improving its linearity and ensuring precise time measurements across the entire range of operation.

Another crucial factor in delay line-based Time-to-Digital Converters (TDCs) that plays a crucial role in determining the achievable resolution is sampling frequency. This relationship between sampling frequency and resolution is applicable to both LUT and Carry 4 delay line-based TDC designs. Higher sampling frequencies generally enable finer resolution by allowing the TDC to capture shorter time intervals with greater precision.

Some TDC designs [142, 114] prioritize high sampling frequencies, making it 200 MHz and higher, to achieve 5ns scale measurements, while some designs require 100 MHz and less to meet the design specifications [139, 89]. Schellenberg [108] and Uganda [123] illustrate the utilization of different frequency ranges. In the former research, the authors employ frequencies of 24, 48, 72, and 96 MHz, demonstrating successful SCA. In the subsequent paper, the author explores a wider spectrum, covering frequencies ranging from 6 to 120 MHz. Within this range, they effectively execute attacks on AES modules and reveal that the success of these attacks doesn't exhibit significant reliance on the ratio between the sampling frequency and the frequency of the AES module.

Zick et al. [142] in their work were the pioneers in showcasing the application of TDCs for measuring voltage variations on an FPGA. The authors suggested the design of the sensor with the Carry 4 element as a basic delay unit. The sensor has a delay line > 1ns, having 64 stages, with resolution of 10 ps each. Their design enables a sample rate 500x faster than 28 nm Xilinx ADC.

Zick emphasized a notable concern: excessive activity within the fabric logic on the board leads to significant undershoot and overshoot phenomena, surpassing permissible specifications. In a novel approach, the authors recommended employing programmable interconnect points to generate voltage transients due to their substantial capacitance. In an experimental setup, the authors simultaneously activated approximately half of the Programmable Interconnect Points (PIPs), 5 million out of 10 million, on an Xilinx Kintex-7 FPGA. They observed the response using an oscilloscope and noted that these events induced a 31% undershoot, surpassing the allowed 3% fluctuation limit. Moreover, the overshoot reached 14% beyond the nominal value. Upon implementing a sensor-based methodology, the authors demonstrated that by activating only 1% of the fabric PIPs, the sensor detected a range spanning 15 bins. Similarly, with 3% activation, the sensor identified a range spanning 22 bins. It's noted that when applying the same scenarios using an oscilloscope, the fluctuations were dismissed and interpreted as common noise.

Unlike Zick, who implemented Carry 4 elements as the basic delay unit, Schellenberg et al.

[108] in his paper demonstrated the first successful SCA (Side Channel Attack) on an AES-128, implementing a combining delay line. Spanning 23 FPGA slices, the line consisted of two sections: an initial segment of seven slices, which had a longer delay but lower area overhead, using LUT primitives, and a 16-slice observable segment using CARRY 4 primitives, chosen for their superior bit-resolution capability. The uniqueness of the sensor lies in its tapping by transparent latches. Thus even if it's not synchronized with the AES clock, it captures all fluctuations occurring during half of the clock cycle, since the clock travels the delay line half of the clock period in which the latches are enabled. Digital Clock Manager (DCM) was employed to generate the desired clock; the sensor received different frequencies: 24 MHz, 48 MHz, 72 MHz, and 96 MHz, whereas the AES module operated at 24 MHz. A standard Correlation Power Analysis (CPA) attack was conducted on the AES module, positioning the sensor in both proximity and at a distance from the AES core. Initial observations using an oscilloscope revealed a maximum correlation of approximately -0.3. The attacks utilizing traces internally measured by the sensor were also successful, albeit with a slightly lower maximum correlation of about -0.2. Even with the sensor positioned far from the AES core, the successful attack remained possible with only a slight correlation decrease. When comparing the outcomes at varying sampling frequencies, significant deviations are not observed. Also It was noted that having a higher resolution (increased quantization steps) marginally enhances the maximum correlation. The experiment underscored the substantial risks associated with sharing an FPGA among multiple users.

Krautter[66] presented a study that concentrated on investigating the impact of mapping parameters on vulnerability to Side-Channel Analysis (SCA) attacks in multi tenant FPGAs. The research suggested implementing a Time-to-Digital Converter (TDC) sensor that had been previously introduced in [142] and [63], and evaluating the comprehensive effects of noise generation modules, composed of Flip Flops (FFs) and Ring Oscillator (RO) waste circuits. The investigation was carried out using the Xilinx Zynq 7000-based platform. Unlike Schellenberg et al. [108], that used a design that needed to be adjusted for process variations or operating frequencies, Krautter introduced the sensor design, allowing at runtime recalibration depending on temperature level.

Analyzing over 256 experiments of CPA Attacks on an AES FPGA Implementation, the experiment showcased variations in the number of traces (up to 100.000) needed for successful key recovery. The authors demonstrated that the success of the attack is contingent on the relative placement of the attacker and target modules on the board, as well as the specific local arrangement of primitives within the module.

In contrast to Krautter [66], where the adjustable module's design involved configuring coarse and fine units, Udugama [123] proposed an alternative approach. They suggested utilizing an

adjustable module in their self-calibrating on-chip design of VITI sensor.

Table 1.1: TDC based designs and their FPGA core components

Device Type	FPGA core components					
	FF	**LUT**	**Latch**	**Carry 4**	**MMCM**	**MUX***
TDC-Latch [142]	X	Y	Y	Y	X	X
TDC-Filp-Flop [89]	Y	Y	X	Y	X	X
Time-interleaved TDC [88]	Y	Y	X	Y	Y	X
DL-ADC [139]	Y	Y	X	X	X	X
CC-ADC [139]	Y	Y	X	Y	X	X
TDC [108]	Y	Y	Y	Y	X	X
VITI [123]	Y	Y	X	X	X	X
TDC [41]	Y	Y	X	Y	Y	X
RDS [114]	Y	Y	X	Y	X	Y

* Routing MUX

Table 1.2: TDC based designs and their respective characteristics

Device Type	Applications	Structural Features			Frequency, Mhz	Calibration	
		stages	taps	resolution, (assumed)[a]		runtime	type
TDC-Latch [142]	SCA	64	linear	10ps	500	no	initialising
TDC-Flip-flop [89]	SCA	256	linear	?(10ps)[a]	50	yes	coarse and fine modules[d]
Time-Interleaved TDC [88]	SCA	256	code-density	17.857ps	100	yes	coarse and fine modules[d]
DL-ADC [139]	IR-drop[j]	256	linear	4mv/b[b]	10	yes	external sensing[c]
CC-ADC [139]	PDN	256	linear	4mv/b[b]	75	yes	external sensing[c]
TDC [108]	SCA	64	linear	?(10ps)[a]	{24, 48, 72, 96}	no	scalling non-observable part
VITI [123]	SCA	256	linear	?(300ps)[a]	$\{6-120\}$	yes	self-calibrating module[e]
TDC [41]	CC[f]	64	linear	8mb/s[g]	{125, 200}	yes	coarse and fine modules[d]
RDS [114]	RPA	?	tree routing	$\max \lvert d_i - d_j \rvert$[h]	200	yes	calibration algorithm

[a] Possible resolution of the design based on timing charcacteristics of basic elements.
[b] Resolution for DL-ADC/CC-ADC in mv/b.
[c] Integrated within a power management IC.
[d] To calibrate the design, a FSM first adjusts the length of the coarse and then the fine delay line.
[e] To calibrate the design, self calibrating module, implements FSM Calibration Algorithm
[f] Sensor operates as a resiever in covert comunication
[g] To calibrate design, adjusting the clock phase, using LUTs and carry-chain logic.
[h] Delay of global interconnect wire.
[i] d_i,d_j Length of corresponding global interconnect wires
[j] IR-drop compensation
[k] PDN impedance compensation

Self-calibration module operates through an FSM (Finite State Machine) calibration algorithm, enabling VITI automatically tuned for temperature changes, power variations, moving the sensor in faraway locations from the circuit under attack. Results demonstrated recovery of a full 128-bit Advanced Encryption Standard (AES) key with 20,000 power traces, while occupying roughly a quarter of the space compared to the TDC counterpart. The design's checkpoint was implemented on the AWS EC2 F1 platform, which houses a Xilinx Virtex UltraScale+ FPGA boasting 1,182,000 Look-Up Tables (LUTs). During the experimental phase, a substantial dataset consisting of 100,000 power traces was gathered from the VITI sensor. As a result of effectively employing Correlation Power Analysis (CPA), a single key byte was successfully retrieved. This accomplishment was achieved using less than 1% of the available logic resources on the FPGA.

Table 1.3: TDC based designs for SCA and their benefits and drawbacks

Device type	Advantages	Disadvantages
TDC-Latche [142]	· Reset and a sampling operation at the same clock phase · Small area coverage	· Sensitive to low frequency changes of temperature and voltage
TDC-Flip-flop [89]	· High resolution · 3 runs for achieving 99% correlation	· Required calibration and manual placement
Time-interleaved TDC [88]	· Achieving a sampling rate of 1/56*T	· Required reconstructing a single high-resolution time series · Utilized within a laboratory environment, requiring acces to an attack circuit · Temperature variations across samples at different phases affect accuracy. · Required cooling
TDC [108]	· Capturing voltage fluctuations even when not synchronized with the AES clock.	· The absence of self-calibration module
VITI [123]	· Small area coverge · Self-calibrating design · Applicable in constrained locations · High effectivenes in recovering the key from AES module	· Lower resolution compare to Carry 4 design

Differing from the aforementioned papers, which employ a single-sample-per-cycle approach, Shayan [88] implemented a time-interleaved TDC sensor to perform sub-clock cycle time resolution. In this technique the authors replay power attack scenarios multiple times, each sampling voltage with shifting phase of the clock cycle, and in post-processing reconstruct a single high-resolution time series of the supply voltage. The ordinary prototype of such sensor samples at the frequency 100 MHz (10 ns sample interval). The time-interleaved Time-to-Digital Converter (TDC) captures measurements at short intervals between consecutive clock edges. This is accomplished by conducting the experiment 560 times while adjusting the TDC clock phase for each iteration. The

MMCM primitive establishes the minimum phase shift, which equates to 1/56th of the voltage-controlled oscillator's (VCO) period. Given a VCO frequency of 1 GHz, each phase shift equals 17.857 ps. This precision enables the detection of small voltage fluctuations.

Table 1.4: TDC based designs for hardware security countermeasures and their benefits and drawbacks

Device type	Advantages	Disadvantages
DL-ADC [139]	· Not constrained by its position on the board. · An automated self-measurement approach. · Balanced tradeoff between power, area, and linearity.	· Low sampling resolution
CC-ADC [139]	· Improved sampling frequency · An automated self-measurement approach	· Resolution is limited by the delay of one gate · Challenging to implement due to the carry signal skipping mechanism on such FPGA families, such as Cyclone V, Stratix V and 10 from Intel.
TDC with adjustable delay line [41]	· No need for the phase shifte clock tree, subsequently less output noise · Self-calibrating design · On-the-fly calibration, with possible adding of latches · Enabling attacks in the cloud or SoCs, without requiring an individual bitstream for each device.	· Sensitive to manufacturing process variation
RDS for Remote Power Analisys [114]	· Straiforward placement · High effectiveness for breaking AES module · No need for specific placement restrictions · Higher SNR compare to TDC, RO designs · Higher peak-to-peak amplitude of the recovering traces compare to TDC, RO designs	· HRDS, VRDS have low sensetivity

Zhao [139] suggests implementing ADC which are based on TDC delay lines. The first one is based on a delay chain of 256 inverters, allowing a placement on any location on the FPGA. Outputs of inverters are sampled by a set of registers and fed by *clk* ADC, which drives the input of the first inverter. The thermometer code output of the delay-line is encoded into binary, such that sensor output is a digital representation of V_{core}. The authors suggested a technique for calibration of the circuit by looking for relationship between V_{core}, and delay line outputs, sweeping V_0 and recording associate values, consequently a resistance extraction was implemented by recording the two peak current values and two correlated sensor readings. Thus, finding related R_{pdn}, as a relationship between correlated V_{core} values and currents. The authors suggest employing $V_{drop} = I_{ref} \cdot R_{pdn}$ in the power-stage controller to construct a real-time IR-drop compensation system for creating an IR-drop-aware power supply. In further experiment the authors implement AC impedance characterization using a faster and more accurate chain of 256 carry-chain adders delay line, suggesting a sampling rate of 75 MHz, 7.5 times faster compared to the 10 MHz DL-ADC used for the dc resistance measurement. As result, it was shown that R_{pdn} contributes to decreased core

voltage under high current conditions, whereas a high alternating current (AC) impedance causes significant on-chip voltage ripple when the load current aligns with the resonant frequencies of the Power Delivery Network (PDN). Recent studies by Spielmann [114] have shown that implementing the delay line of the TDC sensor can make use of routing resources. The authors have introduced a novel routing delay sensor design that utilizes FPGA technology. This design stands apart from traditional Time-to-Digital Converter (TDC) and Ring Oscillator sensors in its fundamental approach. The design uses routing resources as delay lines, and has three variations: vertically constrained, horizontally constrained, and one free of any constraints. The experiments were performed on the Alveo U200 datacenter card and the Sakura-X side-channel valuation board. The authors argue that to extract a secret key from the full 128-bit key of an AES-128 cryptographic core, on average RDS requires 35% less side channel traces than counterpart TDC sensors. A notable advantage of this proposed design is that it eliminates the need for adversaries to restrict placement resources. This feature streamlines the implementation process across various FPGA boards.

1.1.3 TDCs: Designs on Ring-Oscillator

The delay sensor based on the Ring Oscillator is shown on Figure 1.2 functions by monitoring changes in propagation delay, which are assessed through the oscillation frequency of the RO sensor. An RO module is constructed with an odd number of consecutive inverters, creating a continuous oscillation between two voltage levels by connecting the output of the last inverter back to the first inverter. To implement the measurement of the RO oscillation frequency, designers employ digital counters. A counter is linked to the Ring oscillator output. It counts the RO oscillations and is subsequently read by a register. The oscillation frequency is influenced by the number of inverters in the loop, following the formula $f_{osc} = \frac{1}{(2 \times t_p \times n)}$, where t_p represents the propagation delay of a single element, and n signifies the count of inverters in the loop. Since resolution of the sensor hinges on both the count of oscillations recorded and the sampling frequency employed in the sensor's design, to implement the fastest design of the sensor with maximum possible resolution it is necessary to have the minimum number of elements. Hence, these sensors possess an advantage in minimal spatial requirements when compared to delay line-based sensors. This characteristic leads to lower power consumption, and enhancing cost-effectiveness.

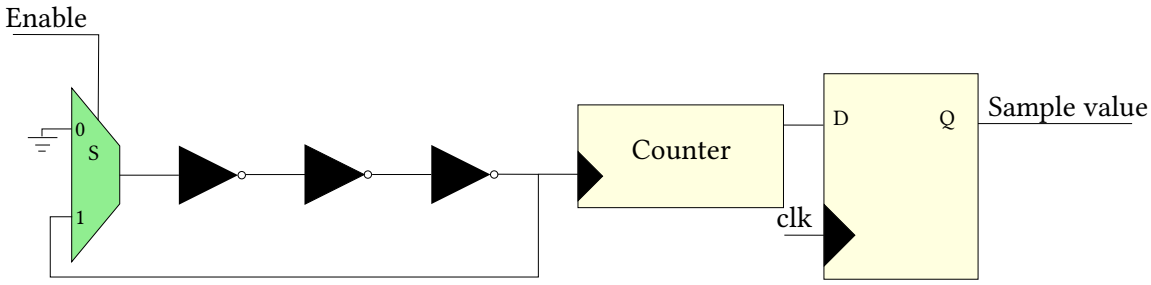

Figure 1.2: RO sensor schematic

Another crucial parameter of the RO sensor is sampling frequency. When an extended sampling period is integrated [44], it becomes possible to accumulate a substantial number of oscillations. Analyzing and capturing this accumulated count yields a highly detailed representation of the fluctuations in propagation delay. Conversely, reducing the sampling frequency leads to a decrease in the number of Ring Oscillator (RO) oscillations counted within a sampling period. This reduction in the oscillation count limits the connection between the counter value and the propagation delay. Consequently, a gradual decrease in the sampling frequency results in a degradation of the sensor's resolution. In essence, lowering the sampling frequency compromises the precision of the sensor's measurements. This fact emphasizes the importance of finding an appropriate balance between sampling rate and the level of detail required for accurate propagation delay assessment.

Ring oscillators implemented on Field-Programmable Gate Arrays (FPGAs) are widely employed in various applications as a means to quantify variations in processes. The initial exploration of using ring oscillators as thermal sensors on FPGAs was undertaken by Boemo et al. [7]. Yu et al. [133] introduced a technique to finely characterize process variations in logic elements and interconnects within FPGAs. Whereas Ruething et al. [105] introduced metrics for assessing the performance and area efficiency of ring oscillators, along with a methodology to quantify these metrics. Barbareschi et al. [4] demonstrated how altering the number of stages in ring oscillators impacts the average frequencies of the oscillators and the extent of variation observed in measured values around these averages. In the realm of hardware security applications, Ring Oscillators (ROs) are employed to measure on-chip voltage fluctuations. Their functions involve power-wasting circuits and act as countermeasures against Fault Injection attacks, which will be discussed in detail in Section 1.1.4.

Gravellier [88] introduced a new design of RO sensor based on Johnson Ring Counter (JRC) which cadenced by the NAND looped gate; data path is structured as a ring, where the inverted output Q of the final flip-flop is looped back to the initial flip-flop's data input D, creating a

complementary feedback loop, tapping each output of flip-flops to the RO register module. The design involves utilizing two non-synchronized clocks for JRC and RO, resulting in a phase shift quantization error. To address this concern, the authors propose a solution by opting for the swiftest configuration of RO, employing a single inverter, and achieving an output frequency of 1.2 GHz. The suggested design sidesteps the exploitation of combinational logic between flip-flops, thereby minimizing timing errors that binary counters typically confront when driven by signals in the GHz frequency range. To ensure that the timing margins of the sensor remain unaffected, implementation utilizes Xilinx low-level primitive templates, guaranteeing that the number of logic gates instantiated in VHDL source file aligns with the number of logic gates employed in the fabric. The sensor instance is composed of just 2 slices, allowing this compact design to be distributed across the fabric without causing area congestion, and more significantly, the overall resolution of the voltage sensor can be enhanced. By improving the sampling frequency and resolution of the sensor, it is empowered by the capability for real-time measurements of voltage fluctuations. A power side-channel attack was executed within an FPGA fabric. A solitary AES encryption operating at 10 MHz was recorded, utilizing 1, 16, and 64 RO-based sensors operating at a 250 MHz sampling rate. Using 16 ROs, it takes around 79,000 traces for the correct candidate to be differentiated from incorrect key hypotheses. In contrast, with 32 and 64 RO-based sensors, the required trace counts drop to 27,000 and 8,000 correspondingly. These findings were compared against the experiments conducted with the TDC-based sensor as outlined in [119]. RO-based sensors, while not achieving the same level of accuracy as TDC-based sensors (approximately 3-4 times less efficient), still exhibit sufficient precision to effectively carry out a CPA. Furthermore, they offer notable implementation benefits. To assess the influence of target speed on CPA outcomes, the study replicated the experiment while altering the AES module frequency from 10 to 200 MHz. However, this increase in frequency did not bring about significant changes in the CPA results.

Masle and Luk [82] devised a power attack detection approach employing a sensor based on ring oscillators implemented on a Spartan-6 LX45 FPGA. With a distribution of 144 one-inverter ring oscillators evenly spread across the FPGA, the voltage sensor samples the circuit at a rate of 8 MHz. The authors establish that such a power monitor is capable of detecting supply voltage fluctuations as minimal as 5 mV. Their work demonstrated that this strategy achieved remarkable performance, with false-positive and false-negative rates both reaching 0%, consuming only 12% of the total FPGA area.

Unlike Masle and Luk, Hoque[53] in his paper suggested using NAND gate based RO, by connecting one input of every stage to the VDD line, the intention is to amplify the design's sensitivity. The researchers showed that Ring Oscillators (ROs) constructed using NAND gates,

when positioned close to the Trojan, exhibit a greater percentage of variation caused by extra circuit activity as opposed to ROs based on NOT gates.

Zhao's work [138], showcased the ring oscillator-based sensor could be implemented without being restricted by place and route constraints. The study illustrated that a sensor has the potential to monitor the power consumption of a CPU and could be utilized to initiate attacks against timing-channel mitigation countermeasures. The sensor was effectively employed to carry out a power analysis attack on an RSA cryptographic module, even when the sensor and the target were situated in distinct regions on an FPGA.

Gattu [32] introduced a real-time SCA detection method using on-chip Ring Oscillator (RO) sensors, using simulation with a detailed model of Power Delivery Network (PDN) and power grid. The proposed technique can identify a least side-channel attack resistance of 1 ohm within 2 microseconds after being inserted at PCB level. Yao [36] suggested versatile RO design - Programmable Ring Oscillator (PRO) with capability to address side-channel fault attacks, as well as injecting a random noise pattern to reduce side-channel leakage of a cipher. The PRO design included several delay units, with each delay cell having two distinct delay paths: one path is formed by inverters, while the second, shortest path bypasses the inverters. Multiplexers are linked to the delay unit in a manner that enables control over the cell's propagation delay. This mechanism empowers the authors to manipulate the Ring Oscillator's (RO) frequency by configuring the input values of the multiplexers (MUXs). The particular design can be fully implemented using a total of 160 slices, which consist of 128 Look-Up Tables (LUTs) and 32 Registers. The authors established an experimental setup incorporating 36 of these PRO designs, encompassing the entire area of the FPGA.

Within a System-on-Chip (SoC) context, designers have the flexibility to incorporate PRO as co-processors. Thus, PROs can be managed by the processor using memory-mapped registers, facilitating the dynamic activation or deactivation of PRO-based countermeasures. As fault injection countermeasure PRO is able to detect: power glitch, EM pulse, time glitch, laser pulse e.g. The counter value of the sensor is evaluated at the end of each monitoring interval and compared with the reference value to get the actual oscillation frequency of the PRO, thus, in the case of fault injection attack or timing faults a deviating value will be detected.

Table 1.5: RO based designs and their respective characteristics

Device type	Applications	Primitives				Structural features			f_s, Mhz
		INV	NAND	AND	MUX	stages	instances	f_{osc}, Mhz	
RO [89]	SCA	Y	X	X	Y	3	16	$\frac{1}{2\times N\times t_{prop}}$	10
RO-JRC [44]	SCA	X	Y	Y	X	1	$\{1, 16, 64\}$	1.2[d]	250
RO-PRO [130]	mult.[a]	Y	X	X	Y	$\{1, 5, 9 \ldots 17\}$[b]	15	$\{22 - 123.44\}$	240[c]
RO [101]	mva[e]	Y	X	Y	X	1	19	130	100[c]
RON [129]	Tr.D[f]	Y	X	Y	Y	5	12	$\frac{1}{2\times N\times t_{prop}}$	?
RO-PLL [86]	EMI[g]	Y	X	Y	X	1	4	$\frac{1}{2\times N\times t_{prop}}$	50
RON-NAND [53]	Tr.D[f]	X	Y	X	Y	4	10	$\frac{1}{2\times N\times t_{prop}}$	?

[a] The given design can provide on-chip side-channel resistance, power monitoring, and fault detection capabilities to a secure design
[b] There are in total 15 frequency configurations consisting of 1, 5, 9, ..., 57 inverters
[c] Khz units
[d] Ghz units
[e] mitigation voltage attack
[f] Trojan Detection
[g] Mitigation EMI

The authors additionally propose the injection of random-frequency noises using the PRO design. This strategy aims to make it significantly more challenging for potential adversaries to eliminate or mitigate the effects of the introduced noise. By employing RO power waste modules for detecting voltage drop by the PRO sensor, there was observed a nearly linear relationship between the number of power wasters and sensor oscillation slowdown, which indicates the effectiveness of PRO as power monitoring sensor. The authors also integrated a Ring Oscillator (RO) power waste circuit to identify voltage drops via the PRO sensor. They utilized UART (Universal Asynchronous Receiver-Transmitter) to retrieve the counter value from the PRO. Consequently, they observed an almost linear correlation between the count of power wasters and the deceleration of sensor oscillation. This relationship underscores the effectiveness of the PRO as a power monitoring sensor.

Zhang [129] proposed using the Ring Oscillator Network to improve the sensitivity of the sensor performance and effectively detect Trojan noise across all areas of the chip, RON consists of the number of ROs that are distributed across the layout of the chip. The number of ROs can be adjusted depending on the sensitivity of the ring oscillators to the gate switching in a predetermined proximity. Thus in the absence of Trojan ICs, if the output of an IC under authentication is not compatible with the expected signature, the IC may contain a Trojan. Architecture generates a distinctive power supply fingerprint, which serves as a mechanism to detect unauthorized modifications. By employing statistical analysis, distinctions are made between the effects of hardware Trojans and variations in manufacturing processes. Consequently, the outcomes of all conducted experiments consistently underscore the remarkable effectiveness of this approach in accurately identifying integrated circuits (ICs) that have been compromised through the insertion of Trojans. In the experimentation phase, a total of 24 Trojan-free FPGAs and 24 FPGAs with inserted Trojans were employed. The RON architecture was established using 12 ring oscillators, each comprising five inverters. A multiplexer module was used to select and enable specific ring oscillators for recording purposes. The findings showcased a detection success rate ranging from 80% to 100% across various locations of the Trojans within the tested environment.

Miura et al. [86] presented a sensor that incorporates both a Phase-Locked Loop (PLL) and Ring Oscillators (ROs) as a countermeasure against EMI. The fundamental concept behind the design is to strategically route the ROs in a manner that ensures their paths traverse through the majority of the chip's components. When an electromagnetic (EM) fault is introduced, the path delay of the ROs becomes altered, leading to shifts in the RO phase.

Table 1.6: RO based designs and their FPGA core components

Device type	FPGA components		
	FF	**LUT**	**PLL**
RO [89]	Y	Y	X
RO-JRC [44]	Y	Y	X
RO-PRO [130]	Y	Y	X
RO [101]	Y	Y	X
RON [129]	Y	Y	X
RO-PLL [86]	Y	Y	Y
RON-NAND [53]	Y	Y	X

The PLL logic is capable of identifying these phase discrepancies and consequently detecting the ongoing fault injection process. The proposed protective scheme has been validated using a Spartan-6 FPGA. The results of the validation demonstrate that the approach successfully detects all faults aimed at compromising the sensitive core, with a notable security margin of 19 dBm.

Considering implementation attacks on providers like Amazon Web Services (AWS), RO-based circuits exhibit clear drawbacks in comparison to Time-to-Digital Converter (TDC) sensors. The measurement approach of these sensors uses combinational loops to measure the delay, which may not be supported in various scenarios, such as on Amazon EC2 F1 instances [10]. To address this challenge, Sugawara et al. [21] implemented Latch-based ring oscillators with a latch (LDCE) in the middle of the loop, that divides the ring oscillator into two distinct combinatorial circuits without a loop. Another solution was a flip-flop-based oscillator that uses a flip-flop element (FDCE). The feedback loop utilizes a flip-flop output Q, which is fed back to the clock port C through a delay line consisting of chained inverters. Upon the arrival of a rising edge at C, the output value on Q toggles. Consequently, another rising edge reaches C after a certain delay, causing the ring oscillator (RO) to oscillate. Checkpoints of these designs and one using a combinatorial loop were implemented by Vivado design tool and submitted to the development flow of AWS. Only the traditional circuit was rejected by suspending the bitstream generation with a message: [DRC LUTLP-1] Combinatorial Loop Alert. This means flip-flop and latched oscillators successfully bypass the DRC. Giechaskiel [37] also tackled the challenge by employing latch and flip-flop based designs to measure the long wire leakage of Virtex UltraScale+ FPGAs, both in laboratory settings and in the Amazon and Huawei FPGA clouds. The study demonstrated that the two new ring

oscillator designs yield nearly identical estimates for the leakage strength compared to traditional ring oscillators. As a result, these new designs enable the measurement of femtosecond-scale changes in the delays of the long wires.

Malicious cloud FPGA user design circuits that intentionally consume excessive power, leading to denial-of-service and fault injection attacks. In response, FPGA cloud services primarily employ a defense strategy centered around scrutinizing designs submitted by users. This scrutiny aims to identify circuit architectures that are recognized for their aggressive power consumption behavior and mitigate the attack.

Provelengios [101] suggested using 19 inverting stages RO voltage sensor design to evaluate a variety of circuit power wasting techniques that typically are not fagged by design rule checks imposed by FPGA cloud computing vendors, and proposing a remediation for mitigating a voltage attack. To measure power consumption the authors suggested using the 19 inverting stages RO voltage sensor design, a new design achieving an average frequency of 130 MHz in the Stratix 10 device. To calibrate a sensor the authors varied the number of RO-based power wasters on the Stratix 10 device from 8,000 up to 30,000, monitoring values from both the on-chip voltage sensor and RO sensors. The efficiencies of the waster module and comparison to other power wasting circuits are evaluated. The single-stage RO waster turns out is much more efficient in wasting power than shift register based waster, AES based, and other two types of combined RO and Flip-flops wasters. Subsequently, the researchers introduced an innovative on-FPGA mitigation strategy. By controlling ARM-based Hard Processor System (HPS), the proposed design regularly gathers voltage measurements from the RO voltage sensor network within each FPGA clock region. These sensor readings are compared against a pre-established threshold to ascertain whether a potential attack might be underway. In the event that the measured voltage within a specific region falls below an acceptable threshold, the clock buffer for that corresponding region is deactivated, effectively impeding the progress of the attack. This technique entails actively gathering real-time voltage measurements from different users (tenants) who are utilizing the same FPGA. In a rapid response to identifying potential malicious activities, this approach is designed to counteract an attack in as little as 21 microseconds. It achieves this by dynamically throttling the clock frequency in areas where suspicious behavior is suspected to be occurring.

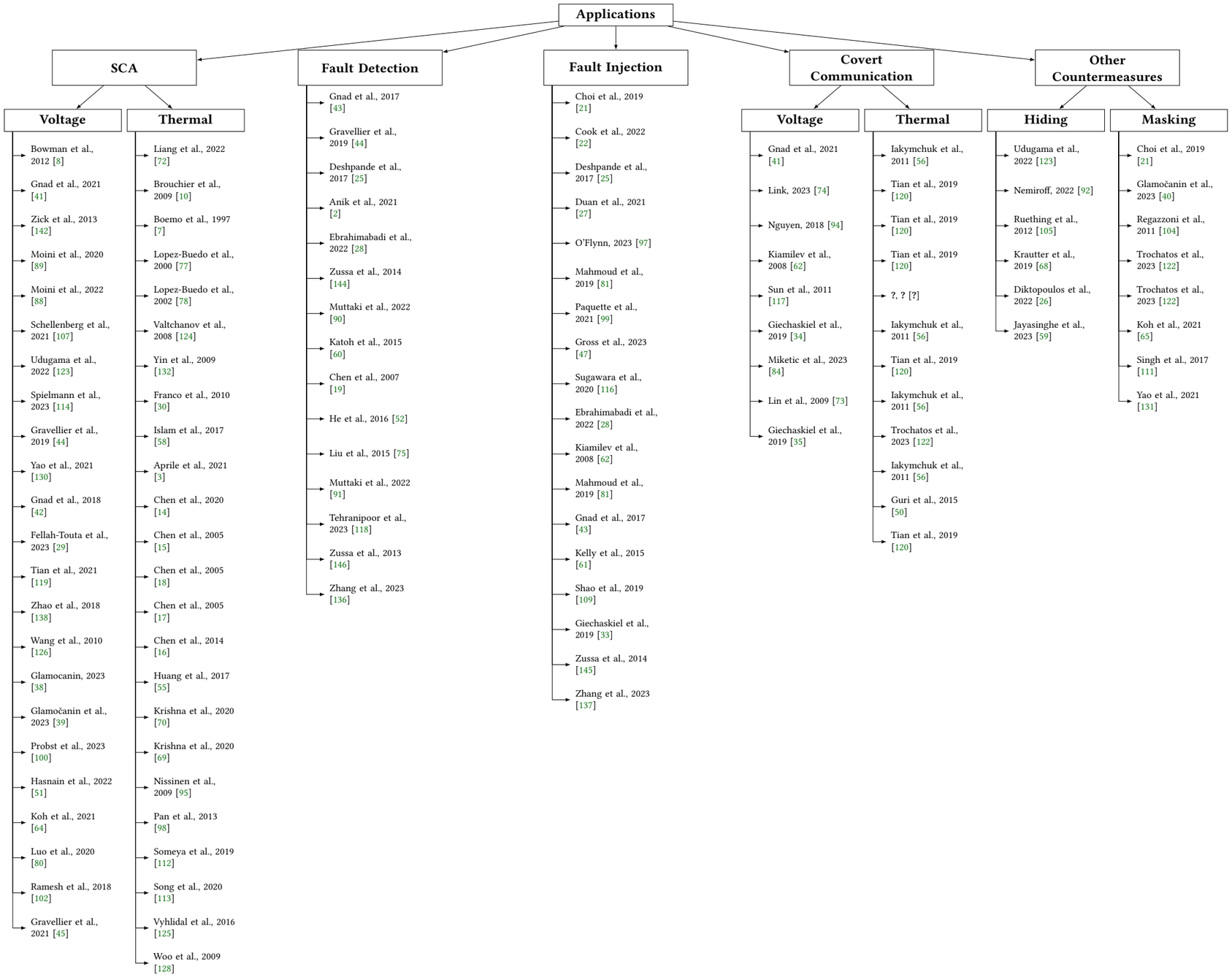

Figure 1.3: Applications of TDC based design sensors

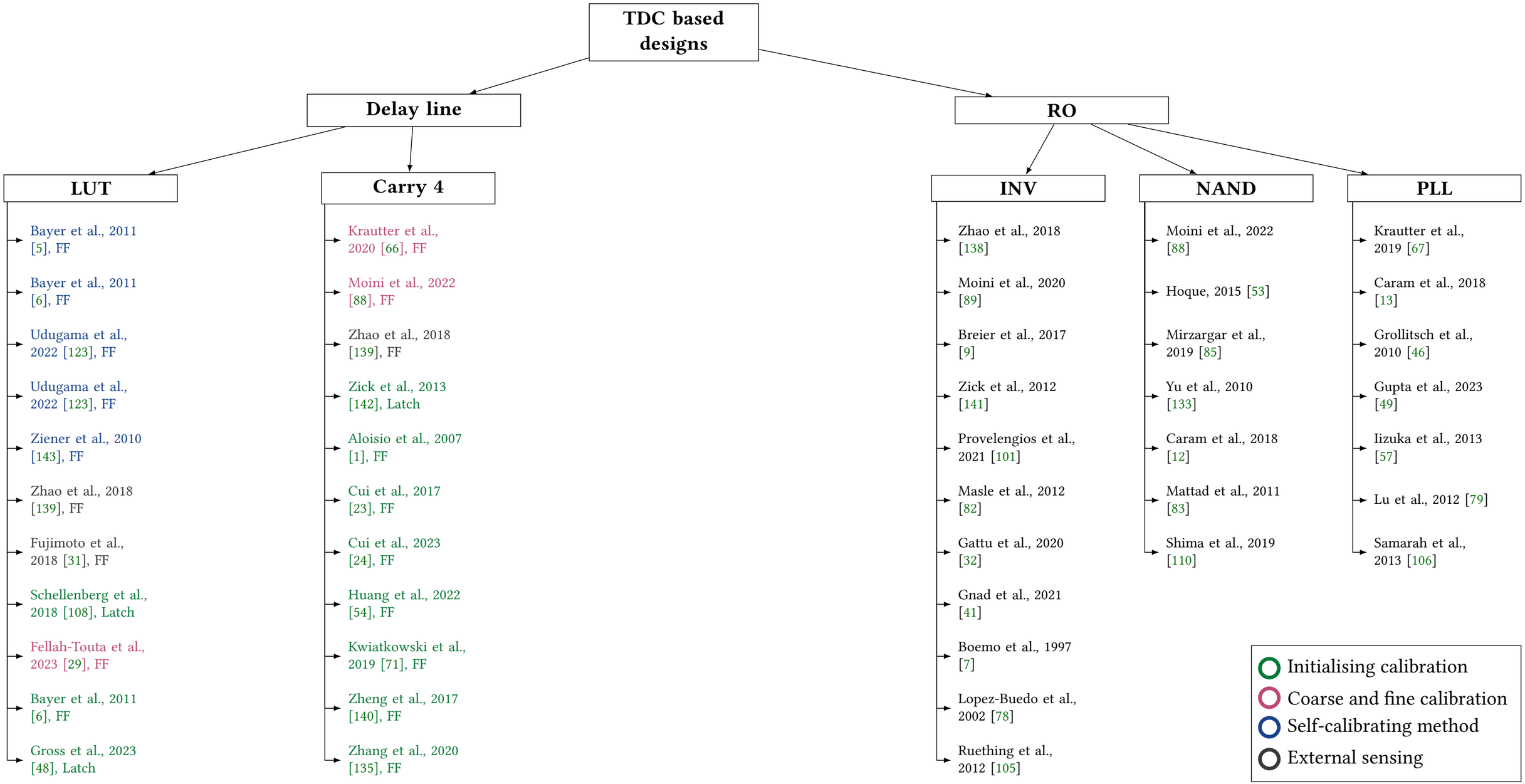

Figure 1.4: TDC based design sensors, their respective characteristics and calibration methods

1.1.4 Applications in the Hardware Security Context

1.1.4.1 Malicious Waster Circuits

Architectures that optimize signal toggling and can be densely located for maximal utilization are excellent contenders for causing power wastage in FPGAs. The figure depicts two primary types of waste circuits: RO's based waster circuit and FF's based circuit, as shown in Figure 1.5.

Moini [88] introduced two types of on-chip power-wasting circuits: the flip-flop (FF) waster and the RO (ring oscillator) waster. The FF waster involves a flip-flop connected to an array of FFs, by this creating a high fanout load on its output. The adjustable parameter in this circuit is the number of fanouts, which can be varied within the range of 0 to 7,000. By enabling the control FF, it charges a significant output capacitance, resulting in large power consumption. This type of power wasting circuit triggers a temporally-short switching event on a single clock edge, but consumes less power than RO design.

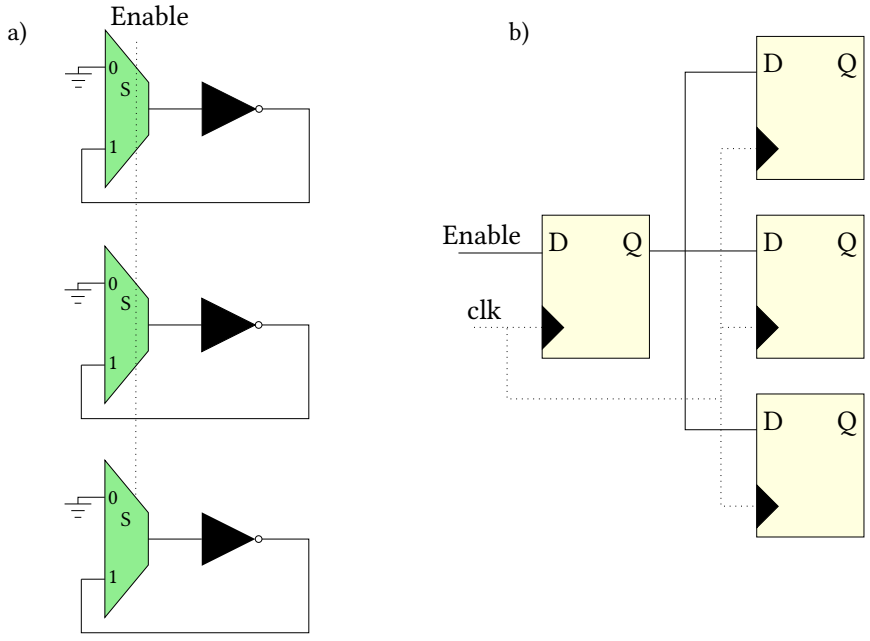

Figure 1.5: RO's and FF's waste circuits

In contrast, the FF-based waster that exhibits power consumption only at the rising edge of the clock signal, the RO enables and disables its operation, constantly consuming power. Waster consists of a three stage inverter chain controlled by a multiplexer, and operating at a high

frequency. The number of active ROs is a parameter that can be adjusted, and it varies between 0 and 10,000. The implementation of the RO wasters is achieved using FPGA lookup table (LUT) primitives.

Provelengios [101] suggested using single-stage RO instances as a power dissipation circuit. Implementing these circuits on Stratix 10, the authors were able to uniformly locate up to 20 such wasters on a single logic array block (LAB). The circuit configuration comprises two interconnected AND gates, with the second input looped back through an inverter. The authors highlighted that as the number of Ring Oscillators (ROs) increases, a localized voltage drop occurs. Thus, the simultaneous activation of 30,000 circuits leads to a disruption in JTAG communication between the PC and the board. This phenomenon was also observed in our experiment when activating an array of 5.000 Short Circuits (SCs) on Artix-7; The PC connection quickly became unstable.

Unlike Sugawara et al. [115] who are using Latch and Flip-Flop based ring oscillators to evade the combinational loop detector in cloud FPGA compilers, Krauter [67] shows an alternative approach using phase-locked loop (PLL). The authors highlight that the maximum power consumption can be achieved with PLL frequency approaching the frequency of a combinational RO, but the effectiveness of these circuits can be observed only while operating in MHz range frequencies.

Table 1.7: Waste circuit designs and their respective characteristics

Device type	**Resources**		**Power consumption**		**Configurability**
	Primitives	**Usage**	**Intensity**	**Type**	
FF waster	DFF(FDCE)	Switching circuit	Low	Transient	Yes
RO waster	LUT LUT	RO chain(inv) Enable gate(nand)	High	Continues	Yes
SC waster	DFF(FDCE) LUT Routing MUX	Short Circuit	High	Continues	Yes

Provelengios [101] executed a comparative analysis employing ten thousand instances of waste circuits. These instances encompassed circuits based on ring oscillators (RO), shift registers, and the Advanced Encryption Standard (AES) with 95 rounds to generate the entries in the table. Among the various approaches, the RO waster circuit demonstrated superior efficiency in power

dissipation. The authors underscored a limitation of using RO + flip-flop (FF) designs on the Stratix 10 FPGA, as the architectural constraints of the logic array blocks (LABs) allow only one such circuit per every 20-logic element LAB due to the utilization of a distinct clock input. The AES-based waste circuit outperformed the shift-register-based approach and remained competitive with the RO + flop design, at higher frequencies. Notably, when all circuits were run at the same clock frequency of 50 MHz, the AES-based waste circuit consumed significantly more power. While the FPGA area occupied by the AES-based power wastes was obviously larger than a single RO, the authors emphasized the importance of employing thousands of RO circuits to effectively assess voltage drop. Our experimentation yielded similar observations when the RO and SC waster module were enabled.

Hoque proposed the implementation of a Trojan design, composed of four stages ROs comprising NAND gates. The initial stage receives an input from the LFSR, while subsequent stages are powered by the output of their preceding stage. The architecture ensures partial activation during circuit operation. The Trojan is also equipped with an Enable signal, which can be utilized to prevent any transitions caused by varying inputs from the LFSR. The influence of the hardware Trojan on the RO-NAND gate, and RO-NOT gate within an FPGA is evaluated by contrasting it with the corresponding reference RO from the Trojan-free version on the identical FPGA. To decrease measurement noise, the average frequency values were taken for each of the seven ROs for all the 10 Trojan free FPGAs locations. Similar measurements are repeated for all ROs of all Trojan inserted FPGAs. Thus, when positioned near the Trojan, NAND-based Ring Oscillators (ROs) experience a greater degree of variation in their frequency percentages, in contrast to ROs based on NOT gates. Regarding father locations, NAND-based ROs exhibit a pattern akin to NOT-based ROs, showcasing comparatively lesser frequency variation. This discrepancy could be attributed to the heightened susceptibility of NAND-based RO frequencies to nearby logic influences. Consequently, it becomes more challenging for a distant Trojan to impact the frequency of NAND-based ROs.

1.1.4.2 ROs as SCA Countermeasure

Ring Oscillators circuits (ROs) have been utilized as a countermeasure against Side-Channel Attacks (SCA), such as concealing the power consumption patterns of cryptographic operations like the AES algorithm. This approach helps thwart attackers who attempt to exploit power consumption information to gain insights into secret keys or sensitive data.

Masking and hiding are two extensively employed techniques to enhance the security of an

AES chip against Differential Power Analysis (DPA) attacks.

The core idea of masking methods is to disrupt the correlation between power consumption and the theoretical power profiles constructed by potential attackers. Liu et al. [121] by employing digital controlled ring oscillators onto the S-box module, create countermeasures for Differential Power Analysis. The authors activated and deactivated RO circuits, serving to dynamically obscure the power consumption of the AES SBox operation.

Whereas the fundamental concept behind hiding methods is to maintain a constant power consumption for various transitions. Nomikos [81] implemented two distinct hiding-based countermeasures designed to protect the AES SBOX against deep learning-based Side-Channel Analysis (SCA) attacks. These countermeasures combat the attacks by introducing noise through two distinct approaches. The first approach generates correlation noise by concurrently executing a second SBOX transformation using a fake key. And the second approach diminishes the leakage of the secret key by complementary memory writing in parallel. Outcomes indicate that the authors successfully fortified the AES SBOX against deep learning attacks through the combined application of these two countermeasures.

Krautter [68] demonstrates a countermeasure against voltage-based Side-Channel Attacks (SCA) by introducing a hiding technique. This involves inserting a mapped active fence of ring oscillators between the victim and attacker circuits. As a result, the authors effectively amplify the required number of traces by two orders of magnitude for the successful recovery of a key from an AES-128 module implemented on a Lattice ECP5 FPGA. Ziener et al. [78] utilize a series of 16-bit shift registers to manipulate the power consumption profile of the FPGA, thus watermarking an intellectual property (IP) core.

1.1.4.3 Covert Channel Applications

Apart from cryptographic use cases, TDC sensors can also serve as receivers for covert communication from hardware Trojans that surreptitiously leak information within the victim's circuit. [41] Thus, intentionally added covert channel receivers (TDC) and transmitters (RO/SCs or other power waste circuits) can illicitly extract various other confidential data from the FPGA. [41] Also such covert channels can serve as a prevailing communication channel such as computer networks to modulate or conceal information in various media. [138] Furthermore, it can also be employed to clandestinely extract information in more intricate attack scenarios. As an example, in cases where hardware backdoors is inserted into a system they can utilize a covert channel to secretly transmit confidential information to a security level with lower privileges.

Gnad [41] demonstrated a transmission rate of 8 Mbit/s and managed to decrease errors to 0.003%. Incorporating 85% of the entire FPGA area by other co-existing tenants' modules to simulate the presence of noise, it exhibited successful transmissions of word-size messages, after assessing the channel's performance, the error rate escalates to 0.02%. In the recent paper, Link [74] showcased the feasibility of establishing a covert channel connecting the CPU and an FPGA by modulating the utilization of the Power Distribution Network.

Ramesh [102] manually routes a long wire close to the target circuit, using crosstalk to perform a side-channel attack, retrieving the key from the AES module within an Intel FPGA. The study showcases that the presence of a covert channel via long wires is observable across multiple Intel SRAM FPGA families, encompassing the Stratix V family deployed in Microsoft Catapult servers.

1.2 Contribution

This thesis constitutes a comprehensive investigation into TDC delay line-based sensors, encompassing a range of critical aspects. The primary contributions of this research are delineated as follows:

Integration of Carry 4 Delay Line-Based Sensor with Short Circuit Power Consumption module This study delves into the intricacies of integrating a Carry 4 delay line-based sensor in conjunction with a Short Circuit power generation module. The investigation focuses on understanding the working process of these components in tandem, while also establishing a mapping relationship on the FPGA platform. Furthermore, the research addresses the configuration of Short Circuit arrays, enabling precise control over power generation.

Development of an Automated Calibration Module Utilizing MMCM A novel automated calibration module is designed and implemented, leveraging the capabilities of the Dynamic Phase Shift Interface in Mixed-Mode Clock Manager (MMCM) Xilinx Vivado. This module empowers the sensor to undergo calibration under diverse operating conditions, enabling it to be configured to operate within any desired nominal range, thereby ensuring optimal performance and accuracy. The calibration process is streamlined, enhancing the sensor's adaptability and reliability.

Comparative Analysis of Carry 4 Delay Line-Based Sensors This research conducts a comparative analysis between two variants of Carry 4 delay line-based sensors: one with 90 taps and another with 258 taps. The investigation encompasses an assessment of their working

processes and effectiveness in capturing delay measurements, by examining their individual strengths and weaknesses in the context of operating as Side Channel Analysis sensors.

Exploration of RO-Based Power Generation Module with SC-array The thesis investigates a scenario where a Ring Oscillator (RO) based Power Generation Module is employed for generating power noise, complemented by the application of glitches generated by a Short Circuit array. The study offers an understanding of the interplay between these components and their combined effect on power noise generation. These contributions collectively advance our understanding of TDC delay line-based sensors and their integration with power consumption modules. They facilitate more precise control, enhanced reliability, and a deeper comprehension of sensor behavior in various operating conditions. The insights garnered from this researches hold implications for the further research in the field of Hardware Security.

1.3 Outline

Section 1.1 offers an in-depth overview of TDC delay line sensors, highlighting their fundamental traits. Moreover, it delves into RO-based TDC delay sensors, examining their advantages, drawbacks, and essential attributes. The section further explains two particular malicious waster circuit types: RO and FF-based devices. Additionally, it investigates possible applications of ROs in SCA defenses and their role as covert channel transmitters. In Section 2.1, we delve into our 90 tap TDC Voltage sensor design, its operational method, resources, and application techniques. Following Section 2.2 offers an insight into the Glitch Voltage sensor, contrasting its operation with our TDC Voltage sensor. Moving on, Section 3.1 showcases a new calibration method for our Voltage sensor using the Mixed-Mode Clock Manager (MMCM) Module in Xilinx Vivado. Section 3.2 presents two SC and RO power consumption array designs, outlining their configurations and primary features, to emulate Voltage glitches. In the next sections, we detail our experimental findings. Section 3.3 documents experiments conducted with 90 and 258 tap TDC Voltage sensors, highlighting the Peak-to-Peak test outcomes where we identify the potential amplitude of captured Voltage glitches. Section 3.4 focuses on mapping experiments, investigating sensor sensitivity based on its proximity to the attack circuit. Section 3.5 presents the Noise test results, assessing the Voltage sensor's performance within a high-power consumption module. Section 4 offers a concise discussion on the experimental results and suggests directions for design enhancement. Lastly, in Section 5, we summarize the thesis's main points and hint at potential avenues for future research.

Chapter 2: Background

Unlike traditional Application-Specific Integrated Circuits (ASICs), FPGAs are reprogrammable semiconductor devices that allow engineers to configure logic gates and interconnects to create customized digital circuits. This adaptability grants FPGAs a unique edge in prototyping, rapid development, and in applications where flexibility is paramount. Nowadays, FPGAs find extensive use in accelerating tasks that require significant computational power, such as artificial intelligence, digital signal processing, and cryptography. FPGAs can be programmed to efficiently handle complex cryptographic algorithms, such as Advanced Encryption Standard (AES) or Elliptic Curve Cryptography (ECC). This makes them well-suited for securing sensitive data applications in transit or at rest, whether in communications infrastructure, storage systems, or IoT devices. Moreover, the widespread adoption of FPGA technology in cloud environments renders it particularly enticing for malicious actors. By monitoring variations in power consumption during for example cryptographic operations, potential attackers are able to scrutinize power consumption patterns, which can inadvertently leak sensitive information like encryption keys.

For implementation of the sensor this study utilizes the Nexys A7 board of Xilinx Artix®-7 FPGA family. Architecture of the sensor composed of configurable Logic Blocks (CLBs) that are the primary building blocks of the FPGA. Each CLB contains four 6-input, 2-output Look-Up Tables (LUTs) and eight flip-flops (FFs). LUTs are essentially programmable logic gates that allow to implement any combinational logic function. Flip-flops are used for sequential logic elements, like registers and memory elements. Switch Boxes (SBs) manage the routing and interconnections between the CLBs and other functional elements on the FPGA. Each CLB contains two slices. A slice is a subsection of the CLB that houses four 6-input/2-output LUTs, eight flip-flops (FFs), multiplexers, and other components.

2.1 TDC Delay Line based Voltage Sensor

Taking into account the factors mentioned above, analyzing a Time-to-Digital Converter (TDC) sensor as a countermeasure against Side-Channel Attacks (SCAs) on Field-Programmable Gate Arrays (FPGAs) is a strategic endeavor in enhancing security. The delay line of such a sensor consists of the n number of the delay elements. The basic delay elements of the sensor are integral

components that determine the granularity and precision of the temporal measurements achieved by the TDC. Each output from delay elements is connected to the respective data input register on the slice, with a total of m taps.

The sensor's design employs phase-shifted signals, with one signal dedicated to driving the delay line and another serving as the clocking signal for the registers. This configuration allows for precise control and synchronization of the sensor's operations, facilitating accurate time measurements. Thus, the sensor output indicates how far the rising edge of the signal propagated through the delay line at the certain clock cycle. If the propagation delay increases due to a lower supply voltage on the board, the rising edge of the signal will cover a shorter distance along the chain within a single clock cycle. As a consequence, the number of non-zero elements in a sequence (Hamming weight) will decrease. Thus, by observing the Hamming weight value, we are able to consider the fluctuation of the supply voltage for a specific clock cycle.

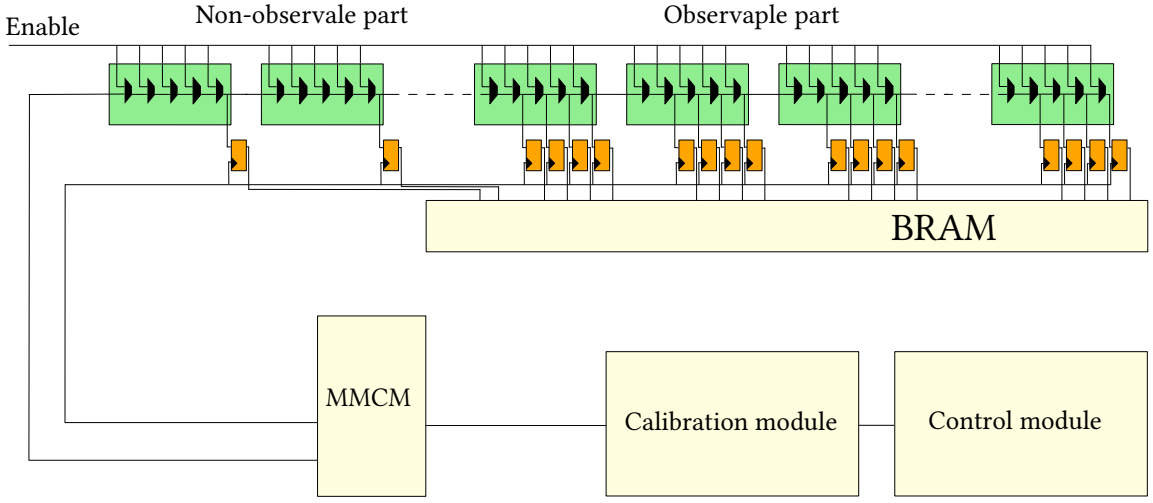

Figure 2.1: TDC Carry 4 delay line Voltage sensor

In this study, we developed a Time-to-Digital Converter (TDC) Voltage sensor, as displayed in Figure 2.1, utilizing Xilinx Vivado design suite technology. The implementation was carried out on an Xilinx Artix 7 series FPGA board.

TDC (Time-to-Digital Converter) sensor uses a configurable delay line with observable and non-observable parts, the register block consisting of the series of FFs (FDCE), calibration and control modules. CARRY4 primitives from Xilinx's 7-series introduce the basic delay element of the design. The choice of Carry 4 line relies on the fact that this is the fastest logic chain on the board, thus the design is able to provide the fastest propagation delays on the FPGA. The introduced

delay line consists of 30 such Carry 4 elements. The first 10 introduces the non-observable portion of the sensor, while the subsequent 20 elements pertain to the observable part. Non-observable section is performed by course delay units, each of which tapped on the 4th output (O) Carry 4 output, and linking to a related flip-flop (FDCE) located on the same slice. This is done to ensure an initial calibration of the sensor. The observable Carry 4 elements are tapped with 4 active outputs (O) of each unit, in the same manner, linked to corresponding flip-flop (FDCE) on the slice. Thus, the design incorporates a total of 90 flip-flops (FDCE) positioned along the delay line. Each of these flip-flop inputs D is connected to its respective segment of the delay line. When the rising edge of the clk signal is detected, the outputs Q of the flip-flops combine to form a 90-bit string, which is then stored in the memory unit of the design. This process ensures that the captured data is accurately recorded and available for further processing and analysis.

The design employs the Mixed-Mode Clock Manager (MMCM) [87] sourced from the Xilinx Vivado design suite to generate clocks with varying phase shifts relative to one another. Thus, the MMCM generates a tdl_in signal at a frequency of $f = 100\,\text{MHz}$, corresponding to a period of $T = 10\,\text{ns}$, which drives the initial element of the delay line. In synchrony, the MMCM generates a phase-shifted *clk* signal which serves as the trigger for the flip-flops, enabling them to sample the values from the delay line. The degree of phase shift can be fine-tuned by considering the propagation delays within the internal structure of the FPGA design. This adjustment allows for precise control over the nominal V_{nom} Hamming weight value required for the certain design and operating conditions.

The Hamming weight of the output is influenced by the number of ones in a bitstring, which in turn correlates with how far the rising edge has propagated along the carry chain during one clock cycle. In our standard operating conditions, under nominal mode settings, the value of V_{nom} is directly correlated to a Hamming weight value of 60 in our setup. Upon receiving an array of bitstrings, these are subsequently processed using a Python script. This processing yields data on the voltage curve's behavior within a specified time frame and at the specific location of the FPGA board. Since, the propagation delay is inversely proportional to the Voltage drop of the sensor, it can be inferred that when the Hamming weight value increases, the circuit exhibits voltage overshoot due to the signal propagating more rapidly through the delay line. Conversely, reducing the Hamming weight value results in a decrease in signal speed, causing an undershoot event.

Apart from driving the flip-flops in the carry delay chain, the clk signal also governs a memory unit, generated by using Xilinx Vivado Block Memory generator LogiCORE™ IP. The selection of the memory type was based on the primary requirements of the design, primarily comparing RAM and BRAM blocks. This module should be responsible for storing and retrieving 90-bit long

strings from each sampled trial. Since, BRAM block is more dense, larger in capacity, providing higher performance memory storage and retrieval, faster access times and higher throughput rates, compared to RAM block, the choice was made in the favor of BRAM block. The depth of the BRAM (Block RAM) module, an adjustable parameter, directly dictates the count of clock cycles that can be recorded from each individual experience. Considering that the design functions at a sampling frequency of 1 sample per cycle, it utilizes 100 cycles for transient experiments and 10,000 cycles for tasks such as Side Channel Analysis, Code Density Testing, and computing mean and standard deviation values. The depth of the BRAM module is a critical factor in accommodating the required number of clock cycles for these different types of analyses. The control of this storage unit is managed by a control module in nominal mode, and by calibration module in the automatic mode, it collects data from the predefined number of trials and sends it to the PC through the UART module.

2.2 TDC Delay Line based Glitch-Voltage Sensor

Voltage glitches on an FPGA refer to a deliberate manipulation of the PDN levels in order to induce faults or disrupt its normal operation. In a voltage glitching attack on an FPGA, the attacker carefully studies the target hardware to identify vulnerable points in the power delivery system. They then apply short-duration voltage spikes or drops at precise moments to disrupt the FPGA's functioning. A voltage glitch detector serves as a pivotal defense mechanism against Voltage Fault Injection Attacks, with its primary function being the continuous monitoring of the voltage supplied to an integrated circuit, detecting and identifying such attacks effectively. In typical scenarios, it is configured with a predetermined threshold, and any deviation beyond this threshold prompts the detector to take immediate action. This may involve triggering protective measures such as temporarily suspending operations, initiating a secure shutdown, or implementing a circuit reset. Moreover, advanced systems may integrate the voltage glitch detector with secure elements or hardware security modules (HSMs) to ensure a swift and coordinated response. Additionally, these detectors are designed with filtering capabilities to distinguish between intentional glitches and normal voltage fluctuations, thereby preventing false alarms. By logging and reporting detected glitches, they facilitate thorough post-incident analysis and forensic investigation. Through meticulous testing, validation, and potentially deploying redundant detectors, this countermeasure substantially bolsters the resilience of integrated circuits against Voltage Fault Injection Attacks, fortifying the security posture of electronic systems.

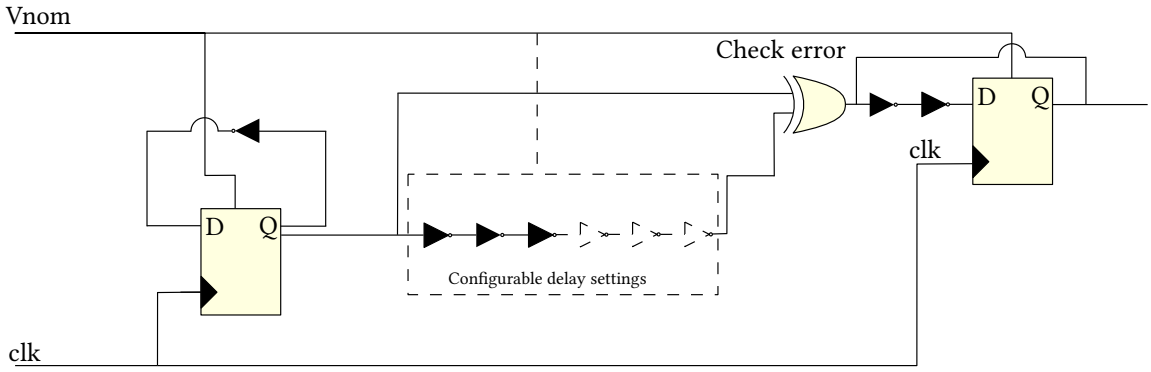

Figure 2.2: Voltage-glitch sensor

The voltage glitch detector is rendered on Figure 2.2 leverages three key elements: a launching flip-flop (FF), a delay chain, and a capture flip-flop. The distinction between TDC voltage sensor and Glitch voltage detector lies in their use of delay lines. In the case of a Voltage sensor, the delay line measures the extent of signal propagation. Conversely, for a glitch sensor, a delay line is employed to calibrate the standard operational delay, enabling the identification of deviations from normal cases. Unlike TDC voltage sensor 2.1 that requires a calibration for the initial setup of the correct voltage range. In the functioning of glitch sensors, it is imperative to meticulously calibrate the sensor to accurately detect the predetermined calibrated values of fault injection drops. Thus, a calibration process of such sensors involves an adjusting the delay chain, enabling the sensor to assess the accuracy of timing in each cycle and detect potential tampering resulting from fault-injection attacks. The authors [93] suggest a configuration of delay buffers in the way of 1:1 relationship of delay chain with the voltage and clock frequency that are used to power the design. Paramount importance in this context is minimizing false negatives, which denote successful fault events going undetected. On the other hand, if the calibration is overly stringent, there's a risk of detecting false positives, regular voltage fluctuations as erroneous alerts. Thus, that can lead to platform instability, potentially necessitating costly recalls.

In the upcoming sections, we are exploring the application of TDC sensor utilizing a Delay Carry 4 line, within RO and SC based power waste circuits. This integration aims to expedite countermeasures against potential malicious exploitation of hardware.

Chapter 3: Implementation and Results

Side Channel Attacks (SCAs) on Field Programmable Gate Arrays (FPGAs) represent a significant concern in the realm of cybersecurity. These attacks exploit information leakage that occurs during the normal operation of an electronic device, often through unintended channels such as power consumption, electromagnetic emissions, or timing variations. For FPGAs, which are widely utilized in critical applications ranging from aerospace to cryptographic systems, vulnerabilities to SCAs can have far-reaching consequences. The ability to glean sensitive information through these covert channels can potentially compromise the confidentiality and integrity of the FPGA-based system.

By integrating the TDC Voltage sensor alongside Ring Oscillators and Short Circuits, it becomes possible to monitor and regulate the power consumption patterns and electromagnetic emissions of the FPGA, thereby thwarting potential side channel attacks. In this context, the integration and meticulously analyzing the working operation of a TDC Voltage sensor within RO and SC arrays provides us essential insights for developing safeguards against Fault Injection attacks. These proactive approaches not only are able to fortify the security of the FPGA but also bolster the overall resilience of the electronic system against sophisticated adversarial threats.

This section delves into examining the functioning of TDC sensor which is introduced in the Section 2.1 alongside with designs of RO and SC power consumption modules, as a robust countermeasure against fault injection attacks.

3.1 TDC Sensor Calibration

To guarantee precise and dependable assessments of propagation delays within the delay line elements, which can be adapted to any design and accounts for an initial unidentified level of noise, we developed a calibration method. Our approach is based on a construction calibration module that adjusts the phase shift between tdl_in input signal to the delay line and clk signal. To achieve the required phase shift, we utilize the Dynamic Phase Shift Interface of the Mixed-Mode Clock Manager (MMCM) Module [87]. The interface has four control signals PSEN, PSINCDEC, PSCLK, and PSDONE.The phase of the MMCM output clock(s) changes either upwards or downwards based on the interplay between PSEN, PSINCDEC, PSCLK, and PSDONE, considering the initial or

previously executed dynamic phase shift. PSEN, PSINCDEC, and PSDONE operate in synchronization with PSCLK. When PSEN is activated for a single clock period of PSCLK, it triggers an increment or decrement in phase shift. A high state of PSINCDEC initiates an increment, while a low state initiates a decrement. Phase shift completion is marked by PSDONE being set high for a single clock period. Each increment or decrement takes deterministic 12 PSCLK cycles to complete. With each increment, the phase shift of the MMCM clock outputs is augmented by $\delta = 1/56nd$ of the VCO period. In our setup we have $T = 10\,\text{ns}$, that equals to the period of PSCLK; Thus, by multiplying the period T by δ we get t - phase shift after each increment for the given setup: $t = T * \delta;\ t = 10.000\,\text{ps} * 1/56 = 17\,\text{ps}$.

In order to precisely control the phase shift within our setup, we designed and implemented a calibration module. This module allows before implementing Side Channel Analysis to set an adjustable parameter Q_{nom} that is equal to the nominal value of Hamming weight with the given operating conditions and noise level. Working process of the module based on the FSM (Finite State Machine) that retrieves values from the delay line and calculates the Hamming weight for each clock cycle. Thus, after applying the Start signal, the module determines the current state of the voltage noise level on the board. Depending on the initial value of the noise, FSM sends control signals to MMCM to adjust phase shift between clk and tdl_in signals. For instance, the initial Hamming weight value is 30 for the given operating conditions, while we set parameter $V_{nom} = 70$; FSM increments a delay of the *clk* signal relative to the *tdl_in* signal, and sends DONE signal when increment is completed. This method allows us to set our Voltage sensor in the cloud environment, where the initial ratio between propagation delay of the delay line and current voltage level is unknown.

3.1.1 Calibration Test

To assess the performance of our sensor under various operational conditions (including temperature changes, power usage, noise levels, and manufacturing characteristics), we conduct a test calibration experiment. The layout of experiment, illustrated in Figure 3.1, involves a TDC Voltage sensor, an RO power consumption module, and an RO power glitch circuit. Ring Oscillator power consumption block can be configured with anywhere from 1 to 20,000 RO modules, enabled by the *enable_w* signal through the selection port of enable MUXs. To induce power fluctuations during the experiment, we employ a power consumption module consisting of 10,000 RO circuits, and apply glitches using a glitch module comprising 3,000 ROs.

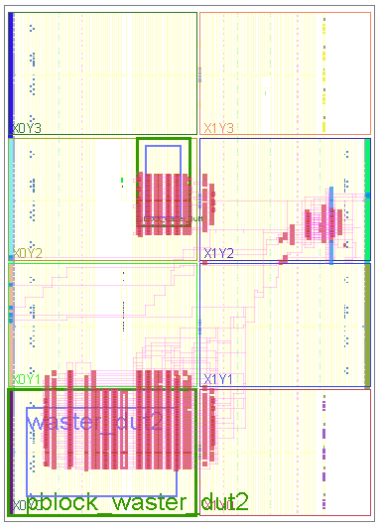

Figure 3.1: The layout of Calibration Test

To verify the reliability of the calibrated setup, we initially set several values of $Q_{nom}\{40, 60, 80\}$.

Subsequently, we introduce sequential glitches by activating the RO glitch module to observe the calibration module's operation. As anticipated, the calibration module exhibits a linear response, demonstrating predefined values of Hamming weight Q_{nom} in three cases $\{40, 60, 80\}$. The figure 3.2 indicates that the glitch curve is independent of the nominal Hamming weight value, confirming the proper functioning of the Voltage sensor across the entire range. To analyze the stabilization process of the calibration module, we introduce two consistent glitches at intervals of 40 cycles, occurring on the 30th and 70th cycles. It is evident that after the first glitch, all three cases display linear stabilization. Therefore, we can conclude that the Voltage sensor automatically stabilizes and operates effectively.

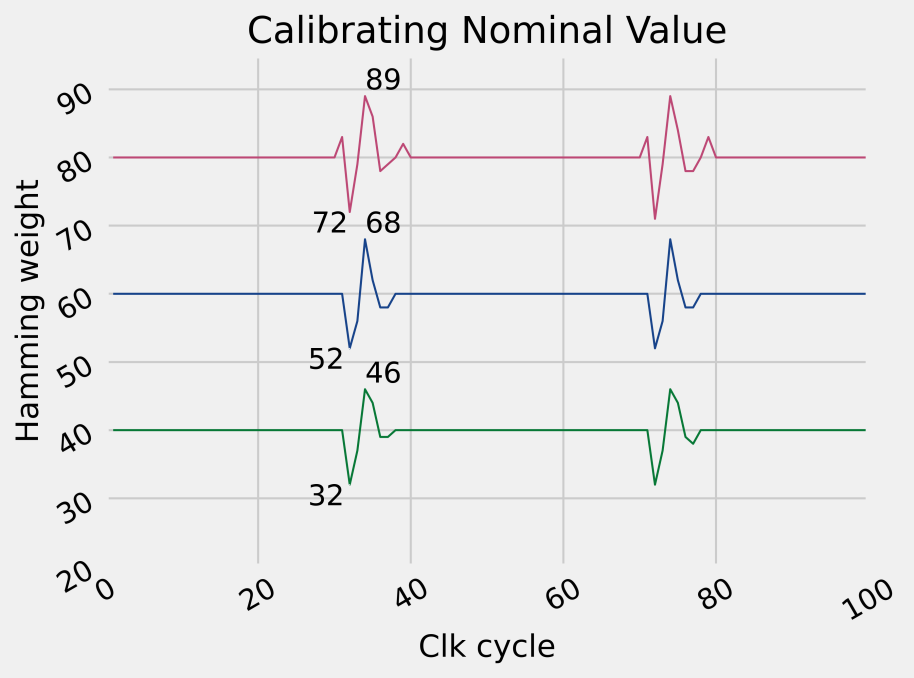

Figure 3.2: Calibration test

3.2 Power Waste Circuit Designs

In the context of the Hardware security Short Circuit and Ring Oscillator arrays serve as tools of power dissipation with multiple functions. Our designs are demonstrated on Figure 3.3. These include acting as safeguards against Fault Injection attacks, functioning as covert channel transmitters, generating noise to simulate power consumption, and calibrating voltage sensors. In this segment, we will delve into the approach for integrating Short Circuits (SCs) and Ring Oscillators (ROs) into our setup.

3.2.1 RO Circuits

Implementing Ring Oscillator-based arrays as power consumption modules on FPGA (Field-Programmable Gate Array) systems represents a proactive approach to analyze the operation of a Time-to-Digital Converter (TDC) delay line-based sensor as a countermeasure against Fault Injection attacks, thus enhancing security of the system.

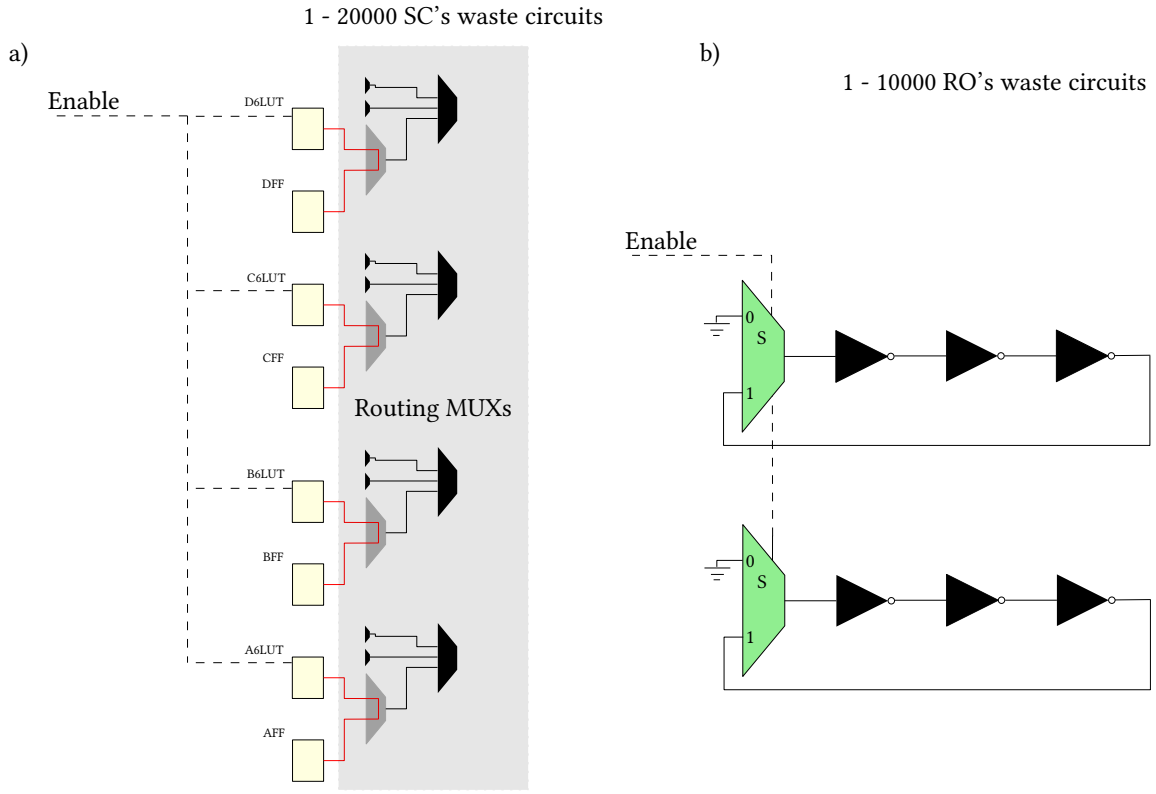

Figure 3.3: SC's and RO's waste circuit designs

Ring oscillators consume power in FPGA systems due to the continuous switching of transistors within the oscillator circuit. In a Ring Oscillator, a chain of inverters is connected in a loop. In our setup we implement 3 inverters in the chain shown on figure 3.3, which are enabled by the enable signal connected to the multiplexer. When the input signal to the first inverter changes, it propagates through the loop, causing each subsequent inverter to switch states, creating an oscillating waveform. This continuous switching action results in dynamic power consumption. Each time an inverter switches, it charges and discharges the capacitive loads associated with the transistors, consuming energy. Additionally, there are resistive losses in the transistors themselves, which contribute to power dissipation. Thus, we establish an array comprising a variable quantity of waste power modules, ranging from 1 to 10000. By overseeing this array through a control module, we simulate the voltage fluctuations within the system. Thus, through monitoring the power consumption of these oscillators, it becomes possible to gain valuable information into the behavior and functioning of the TDC delay line sensor.

3.2.2 SC Circuits

Short-circuit scenarios can be caused by driving two different logic values to the bus at the same time. This situation leads to a direct electrical path between a high and low logic level, potentially causing voltage drop due to the increased current flow through the affected nodes. This leads to by several orders of magnitude higher current draw from the power supply.

In FPGA designs, a short circuit occurs when one of the outputs of an FPGA primitives, such as a Look-Up Table (LUT) and Flip-Flop (FF), drives a logic-1 that is directly connected to the output of another primitive that is driving a logic-0.

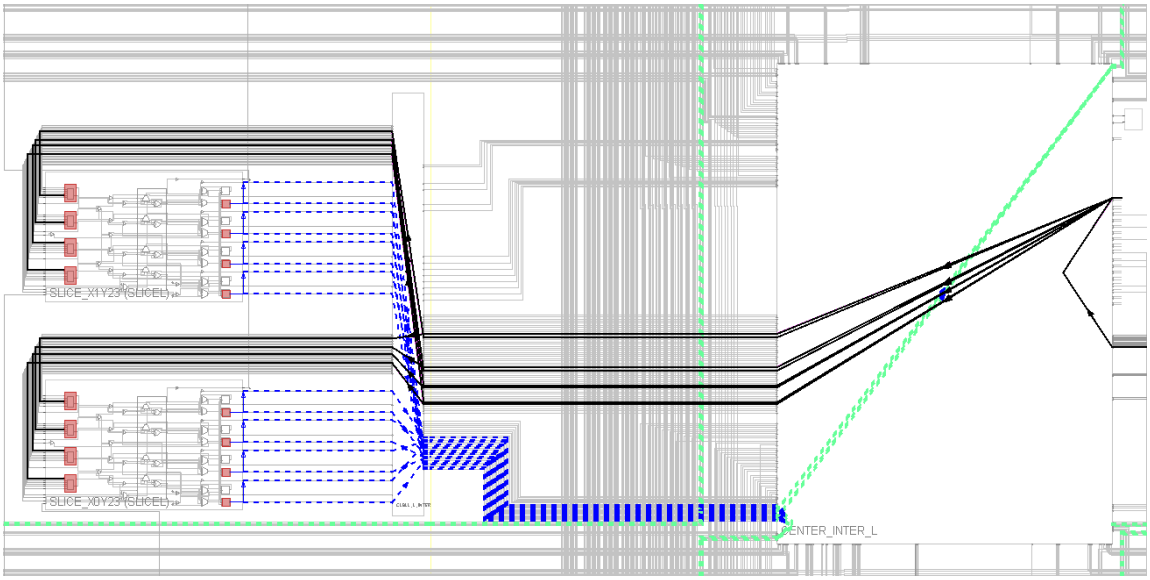

Figure 3.4: Short circuits layout schematic

This case can be possible by connecting two primitives through switching matrices of the routing multiplexer, where each input of the multiplexer is activated. Thus, we connect four of corresponding pairs LUT - FF: A6LUT - AFF, B6LUT - BFF, C6LUT - CFF, D6LUT - DFF, layout of the schematic is shown on Figure 3.4. Through a configured routing multiplexer, it creates a low-resistance path for current flow in the circuit, enabling a voltage drop. In this way, we covered the whole area of each slice implementing four short circuits per one slice, with the possibility of creating any size array of these short circuits.

In practice, generating controlled Short Circuits (SCs) within FPGAs is a challenging endeavor due to the presence of advanced design rule checkers in design tools such as the Xilinx Vivado

design suite. These checkers are designed to prevent any such misconfigurations during design flow. As a result, the creation of SC elements necessitates manual intervention and cannot be streamlined through the use of Hardware Description Language (HDL) tools. To overcome the challenge, we generated short circuit bitstreams by using RapidWrite [103], an open source platform from AMD AECG (Previously Xilinx Research Labs) with a gateway to backend tools in Vivado®. The tool enables customization of the implementations that would not be possible in the standard Xilinx design flow. Firstly we created a static region of the design with *sc_enable* wire as an output of one of the buffers, that is left unconnected. Input of the buffer is driven by the control module, by means of that we specify the time frame and logic of the circuit.

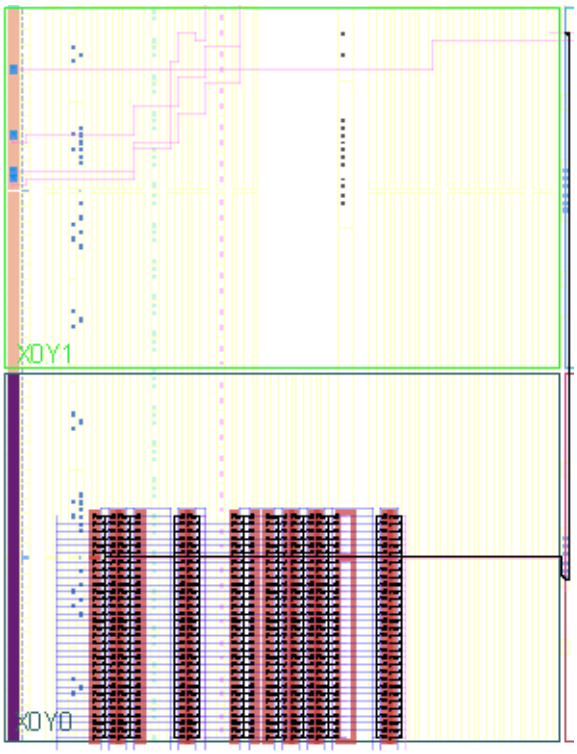

Figure 3.5: Short circuit array is driven by enable signal

Thus, by creating a checkpoint in Vivado, we loaded .dcp in RapidWrite tool, where we manipuled a netlist of the design by initialised LUTs and FFs with inverse values, and connecting them to switching multiplexer. We incorporate a short circuit array into our design by linking it with the *sc_enable* driver, as illustrated in Figure 3.5. Upon loading the final checkpoint in Vivado for bitstream generation, we came across an anticipated issue: [DRC MDRV-1] Multiple Driver

Nets: Net CLBLM_R_X3Y0_NE2BEG2_net has multiple drivers: SLICE_X2Y0_C6LUT_inst/O, and SLICE_X2Y0_CFF_inst/Q. The nets for the connecting short circuits have multiple drivers. To resolve this, we addressed the problem by reducing the severity of all DRC checks using the following TCL command: set_property SEVERITY {Warning}. Subsequently, the design was uploaded successfully and executed on the board. Thus, we implement an array with a configurable number of short circuits modules, ranging from 1 to 20000. Supervising this array via a control module enables us to replicate voltage fluctuations within the system. By observing the power consumption patterns of the specific type of power waste modules, we are able to get an understanding of the benefits of such wasters, as well as compare the efficiency with more common RO based power consumption circuits, acquiring valuable information about performance of the TDC delay line sensor.

3.3 Peak-to-Peak Test

The following test has several purposes:

1. Examine how the amplitude of the detected Voltage glitch is influenced by the Q_{nom} value of the Voltage sensor.

2. Compare the sensitivity and result behavior of the two types of the Voltage sensors with 90 and 258 taps.

In the following experiment we make an evaluation of how the Q_{nom} value of the sensor impacts the time quantization level of the measurements. Previously the question was discussed in the paper [107]. The authors of this paper suggested a sensor consisting of LUT delay elements for initial delay and Carry 4 delay elements for observable parts. Their device has no run-time calibration, implementing calibration by adjusting an initial delay of the sensor. The authors introduced direct dependency of the initial delay of the sensor and observed peak to peak fluctuation of the measurements. In our paper we suggest using a self-calibration module that was discussed in the section 3.1, employing Carry 4 as a delay element for the whole length of the delay line. Thus, in the given experiment, we explore the sensitivity of the two sensors with 90 and 258 tap lengths, by comparing the results of the series of experiments. We conduct multiple tests using different initial Hamming weight values, Q_{nom}, by introducing a voltage glitch to gauge the sensor's sensitivity. The voltage glitch circuit consists of 1000 ROs, having the same setup parameters, and locations relative to the Voltage sensors. For the first experiment we evaluated the sensor that has 90 tap delay line, and for the second that has 258 taps. The layout of the experiments are depicted on

the Figure 3.6 and Figure 3.7 We gradually increased Q_{nom} values from 30 to 80 Hamming weight values for the first sensor, and from 30 to 240 for the longest one, by adjusting Q_{nom} value and capturing peak to peak value for each trial.

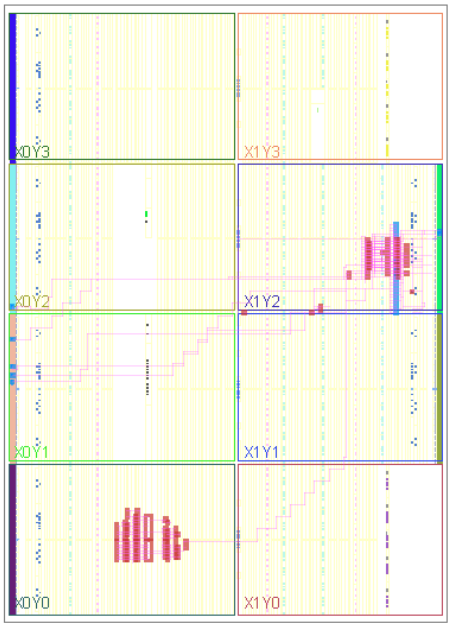

Figure 3.6: Peak-to-Peak Test of 90 tap Voltage Sensor

Q_{nom}*	Type of the sensor	
	90 tap	258 tap
30	5	4
40	6	4
50	6	7
60	6	6
70	6	7
80	9	9
100	.	11
150	.	13
200	.	16
230	.	17
240	.	17

Table 3.1: Dependancy Peak-to-Peak value of the capturing signal from Nominal value of the Sensor

The voltage glitch circuit is made up of 1000 ROs, all with consistent setup parameters and positions in relation to the Voltage sensors. In our first experiment, we assessed a sensor with a 90 tap delay line, and in the second, one with 258 taps. The experimental layouts of both tests can be seen in Figure 3.6 and Figure 3.7. For the first sensor, we incrementally raised the Q_{nom} values from 30 to 80 Hamming weight values. For the longer sensor, we adjusted the Q_{nom} values from 30 up to 240, recording the peak-to-peak value for each test.

* Nominal value of the sensor for given Peak-to-Peak value

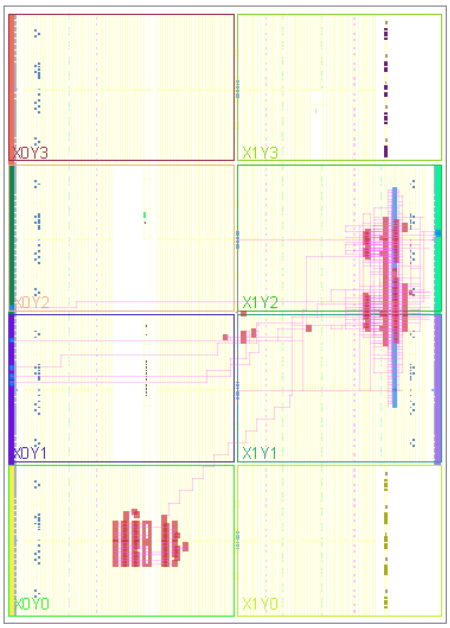

Figure 3.7: Peak-to-Peak Test of 258 tap Voltage Sensor

Table 3.1 highlights the findings from our experiments. In the experiment with a minimum Q_{nom} value of 30, the glitch amplitude matches 4 units of the Hamming weight. Conversely, with the Q_{nom} value at its maximum of 240, the amplitude is 17. It's evident from the data that as Q_{nom} values rise, there's a corresponding increase in the amplitude of the captured signal. The two tests, conducted under the same conditions of noise, power consumption, and operation, exhibit a difference of 13 values of the Hamming weight.

These results confirm that the higher we set the Q_{nom} value, the longer initial delay of the propagating signal before the capturing range of the glitch, the more fluctuation of the signal is zoomed to the observable range. Thus, it leads to higher quantization levels of the measurements. Given that our sensor is designed to detect voltage drops, signifying reductions in propagation delays and Hamming weight values, there's no requirement for an extended range for value increments. As such, it's practical to equip the sensor with an elevated Q_{nom} value, allowing for more precise data capture with a larger quantization interval. From the outcomes of both experiments, it's evident that the sensor equipped with a longer delay line of 258 taps can detect finer levels of voltage fluctuations. This leads to more precise results, especially at elevated Q_{nom} levels.

3.4 Mapping Test

The test is multifaceted in its objectives:

1. Discern how the placement of attack circuits affects the mapping of the sensor onto the FPGA.

2. Evaluate the efficacy of various attack circuit configurations in the different setups, specifically comparing Ring Oscillator arrays with Short Circuit arrays.

3. Juxtapose the functionalities of the two types of the sensors. The first possesses 90 taps, while the latter has 258 taps, determining the superior performer.

The specified test investigates 8 different positions of the attack circuit on the board, which is divided into two primary sections. In the initial set of experiments, we delve into the mapping of the 90 tap Voltage glitch sensor in relation to the RO and SC arrays. These arrays span 15x15 slices within their respective CLK regions. The configurations for the RO and SC experiments are portrayed in Figure 3.8 and Figure 3.12 respectively.

As detailed in section 2.1, our RO power consumption module is composed of a chain of inverters, each with an enable signal connected to each segment. In contrast, the SC module is built by initializing varying voltage levels that are interconnected. The design of each RO and SC power consumption unit is depicted in Figure 3.10 and Figure 3.11, respectively. Both RO and SC modules primarily employ LUT and Routing MUX as core elements in their architectures.

The Voltage sensor is positioned on the board's right side. This specific location was selected for all experiments to place the device near the MMCM and the clock enable pin E3 of Nexys A7-100T. The aim was to minimize the impact of voltage fluctuations on the clock network during voltage glitch experiments.

The attack circuit is situated within the initial 15x15 slices of every clock region on the FPGA. Each position corresponds to a specific clock region on the FPGA, ranging from X0Y0 to X1Y3. In varying experiments, individual circuit module are activated by the *enable_w* signal, while the others remain inactive. To ensure the precise placement of each circuit on the board, we designed 8 pblocks during the synthesis phase of the Xilinx Design flow. Within the pblock properties, we deactivated the IS_SOFT option. This ensures that the tool cannot place any cells outside of the designated pblock.

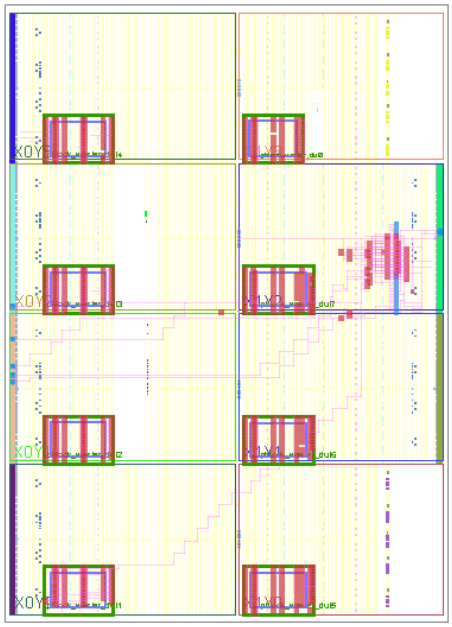

Figure 3.8: Mapping Test of 90 tap Voltage Sensor within RO arrays

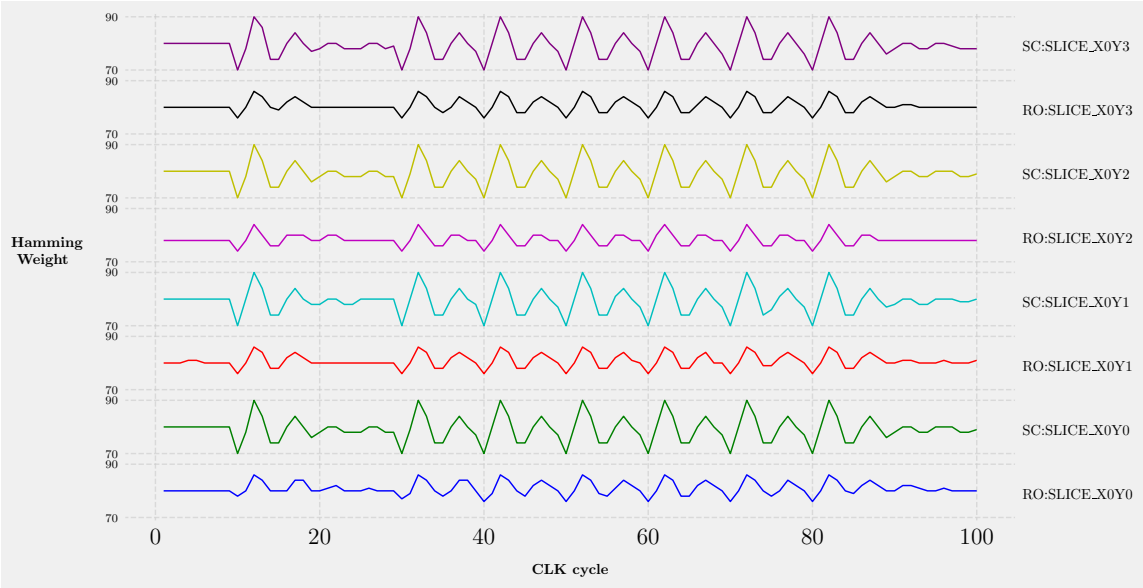

Figure 3.9: Mapping test of 90 tap Voltage Sensor in CLK regions X0Y0:X0Y3

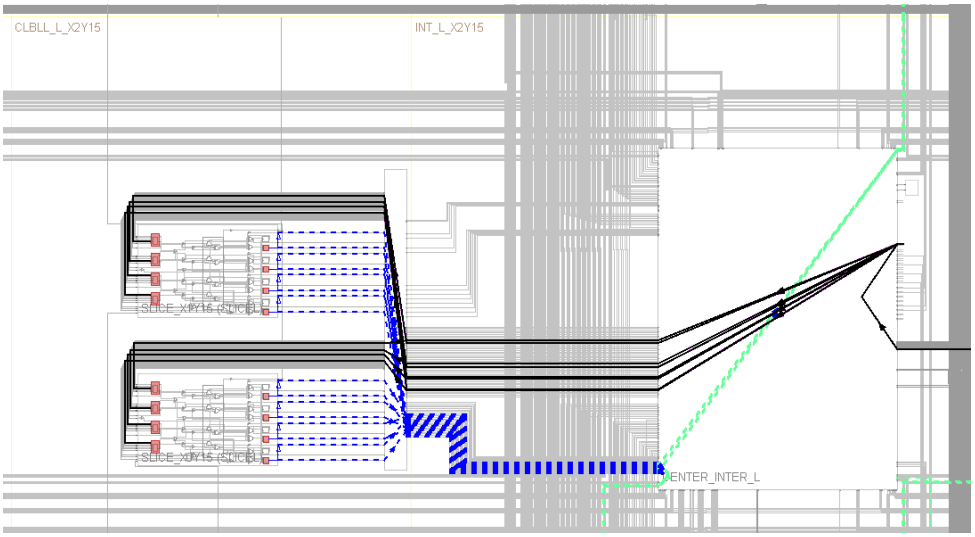

Figure 3.10: Layout of RO array Slice

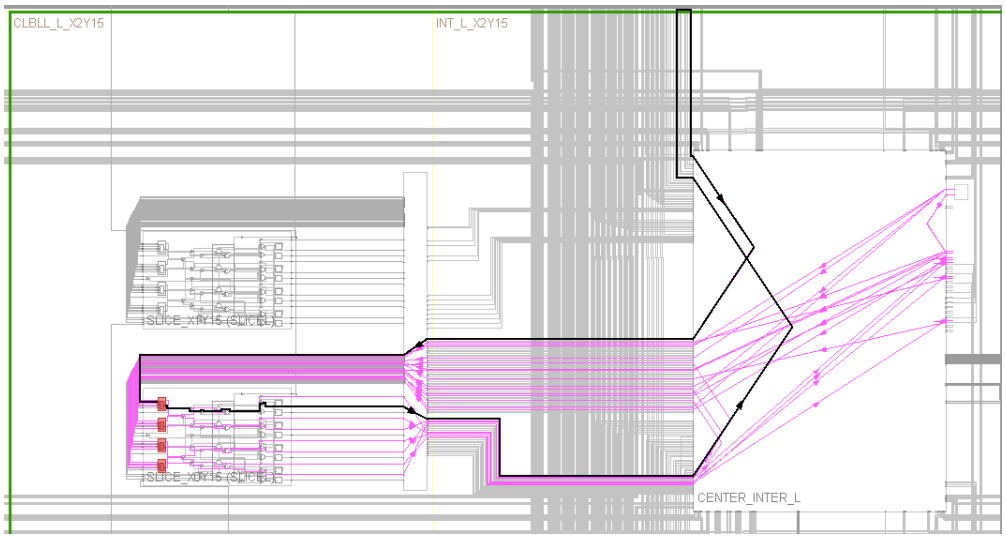

Figure 3.11: Layout of SC array Slice

Hence, each circuit is positioned equidistantly in relation to the others. We applied similar constraints to the Voltage glitch sensor. Notably, the IS_SOFT property proves beneficial when positioning the attack circuit near the sensor's clock region, given that the locations of the attack circuit and certain components of the sensor setup might intersect.

To grasp the distinctions between the two types of attack circuits, RO-based and SC-based,

we presented the aggregated results of both experiments on a single graph, highlighting various FPGA locations. The chart 3.9 depicts the outcomes of the SC and RO experiments, showcasing four clock regions distanced from the voltage sensor, specifically within the range of X0Y0 to X0Y3. Examining the graph, it becomes evident that, regardless of the specific location on the board, the RO power consumption module has a lesser impact on the Voltage sensor. It registers a Hamming weight value that peaks at 86 and goes as low as 76. In contrast, the SC array exhibits a Hamming weight value amplitude ranging from 70 to 90, consistent across all locations along the X0 coordinates.

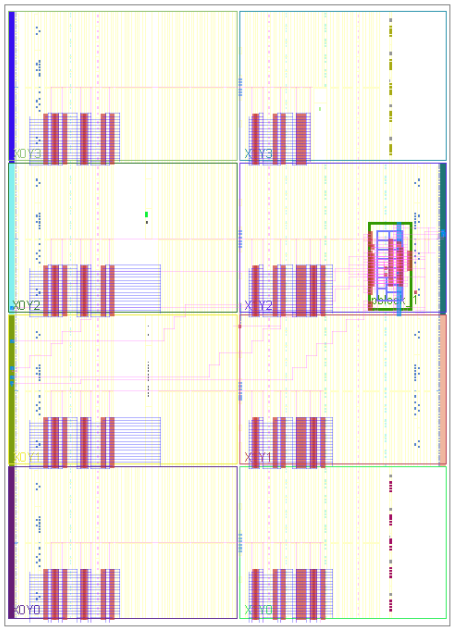

Figure 3.12: Mapping Test of 90 tap Voltage Sensor within SC arrays

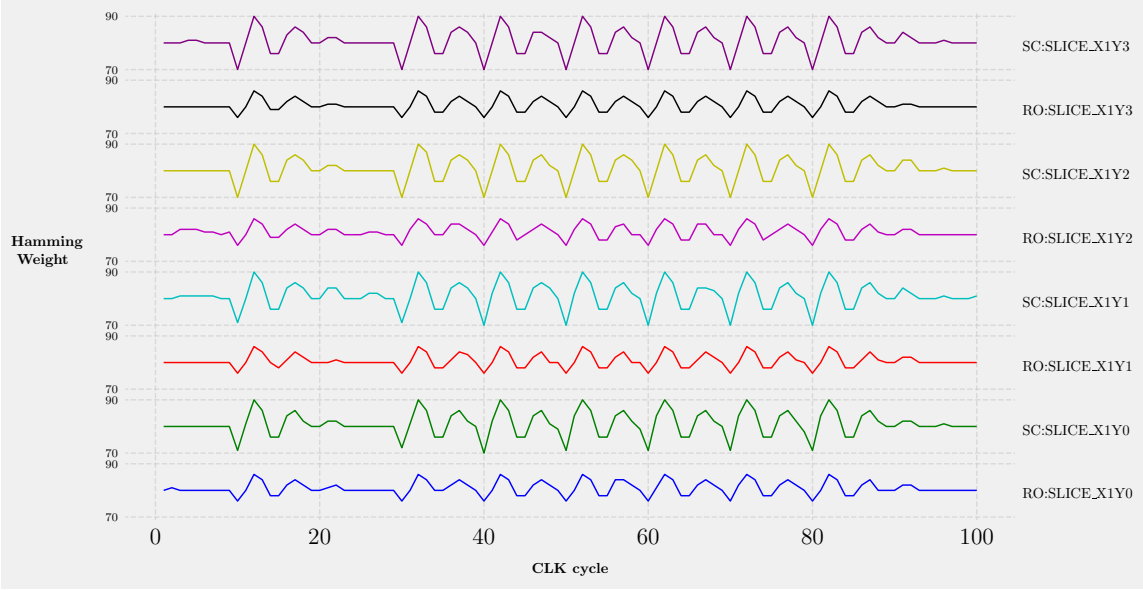

Figure 3.13: Mapping test of 90 tap Voltage Sensor in CLK regions X1Y0:X1Y3

The graph 3.13 presents results from the latter half of the FPGA, encompassing the clock regions from X1Y0 to X1Y3, proximal to the sensor. While there are slight variations, the general pattern of these curves aligns closely with the prior test findings. This indicates that the positioning of the power consumption modules has a minimal impact on the Voltage drop levels for this particular FPGA board.

In the subsequent set of experiments, we examined the configuration of the 258 tap Voltage glitch sensor in relation to both the RO and SC arrays. The layout of the SC array inside the sensor is illustrated in Figure 3.15, which portrays the test results from the more distant sections of the FPGA, within the clock regions X0Y0:X0Y3. These results exhibit behavior similar to the 90-tap sensor. However, this round of testing revealed the sensor's capacity to detect finer Voltage fluctuations. Notably, the outcome shows an amplitude of about 40 values of Hamming weight, doubling the previous experiment's results. This indicates that while a sensor with a broader range necessitates more extensive area coverage, its efficacy is considerably heightened. The graph 3.17 presents the findings of the experiment where the attack circuits are positioned on the nearer half of the FPGA, spanning clock regions X1Y0 to X1Y3. Contrasting with the previous test, where discernable differences between proximate and distant locations of the attack circuit and Voltage sensor were absent, this setup, with its extended tap range and elongated delay line, highlighted discrepancies in glitch capturing based on distance. Specifically, when the attack circuit was

located in closer proximity to the sensor, an average amplitude value increase of 2-4 was observed. This observation supports the idea of using a Voltage sensor with an extended delay line, as it enhances the capability to detect minor fluctuations potentially induced by stealthy glitch devices.

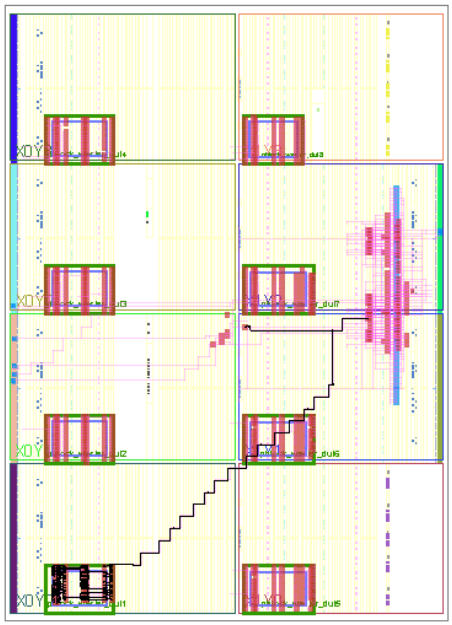

Figure 3.14: Mapping Test of 258 tap Voltage Sensor within RO arrays

The data from both experiments highlight that both RO and SC attack circuits are effective across various locations on the FPGA. This offers expansive possibilities for malicious actors to employ such setups. The introduced sensor can consistently detect Voltage fluctuations, irrespective of its proximity to the target circuit. This emphasizes the potential of such sensors in the context of Fault Injection Attacks, allowing for flexibility in sensor placement, even at distances from the target. Furthermore, given that these two sensor types can uniformly detect Voltage glitches at both proximate and distant locations from the target, they can also be employed as glitch detection devices, serving as protective measures against hardware security threats.

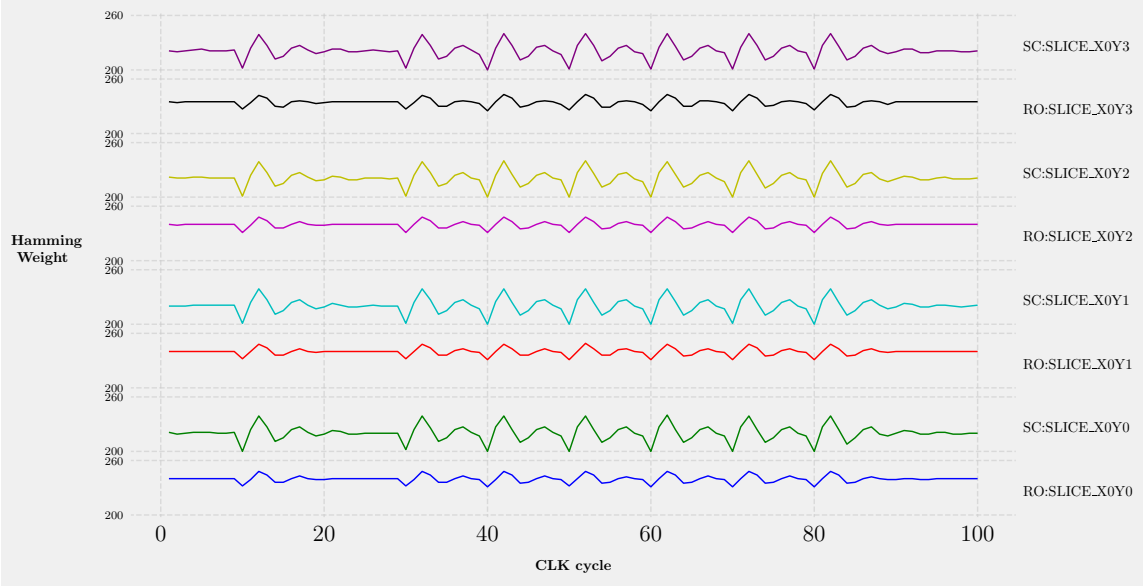

Figure 3.15: Mapping test of 258 tap Voltage Sensor in CLK regions X0Y0:X0Y3

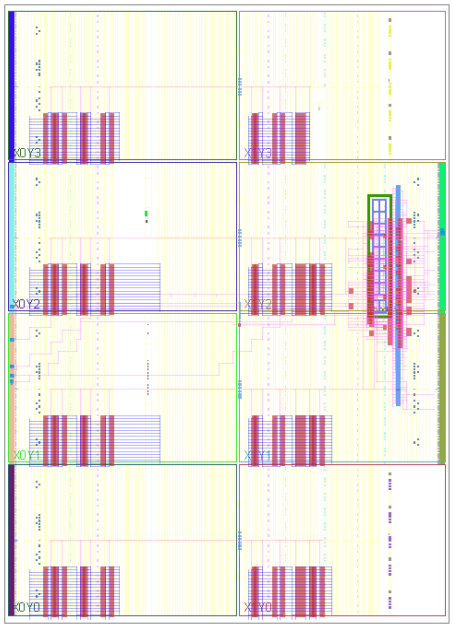

Figure 3.16: Mapping Test of 258 tap Voltage Sensor within SC arrays

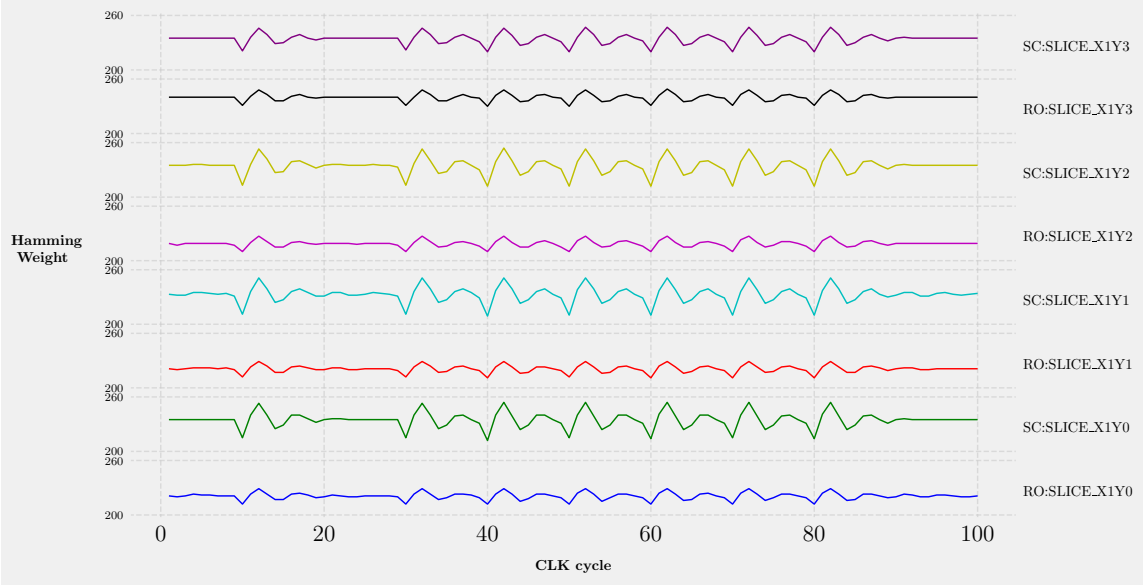

Figure 3.17: Mapping test of 258 tap Voltage Sensor in CLK regions X1Y0:X1Y3

3.5 Noise Test

In the following series of experiments we have the following several purposes:

1. Analyze the working process of the Voltage sensors, within a high Noise Power consumption Level on the board.

2. Find out the working process and effectiveness of two types of attack circuits RO and SC, working simultaneously and their overall effect on the Voltage sensors.

3. Compare the effectiveness of two types of Voltage sensors with 90 and 258 tap delay lines, within a high and low Noise Power consumption Level on the board in the given setup.

The following test consists of the two main sections. The first section introduces the results of the test of 90 tap Voltage Glitch sensor in the given setup that is depicted on the Figure 3.18. On the given figure we can observe the layout of the sensor on the right hand side of the FPGA board. The sensor was located using pblock constraints with switched off option of IS_SOFT placing, in order to avoid overlapping with the power generating module. The Power consumption module consists of 15,000 ROs and is strategically positioned directly in front of the sensor.

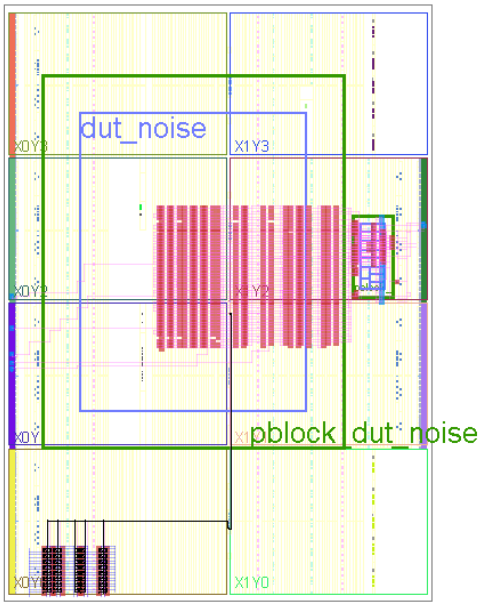

Figure 3.18: Layout of 90 tap Voltage Sensor with Power Generation module

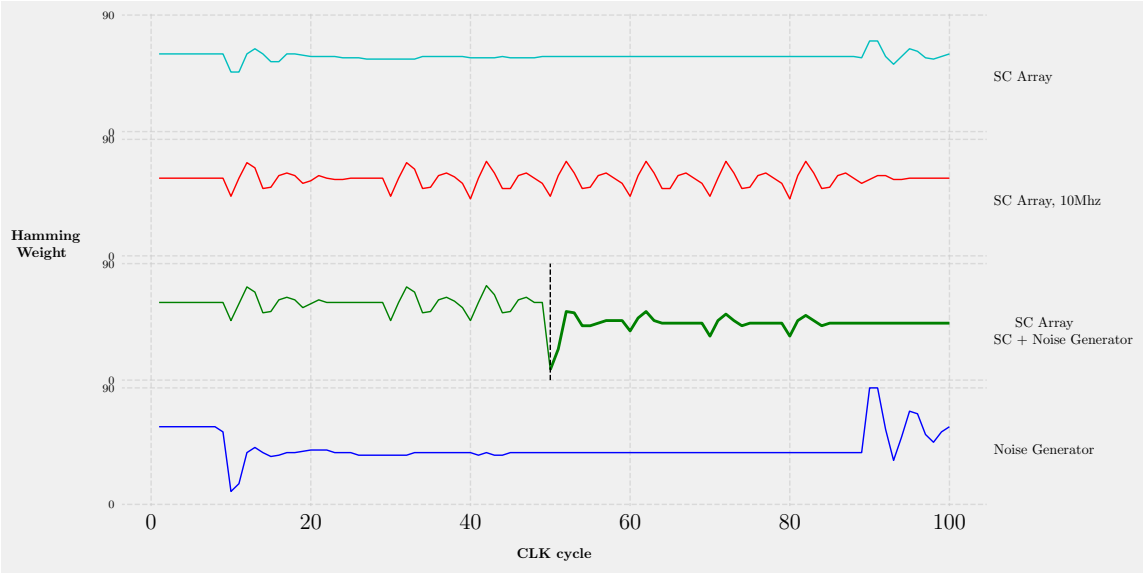

Figure 3.19: Noise Test of 90 tap Voltage Sensor within High Power Consumption Level

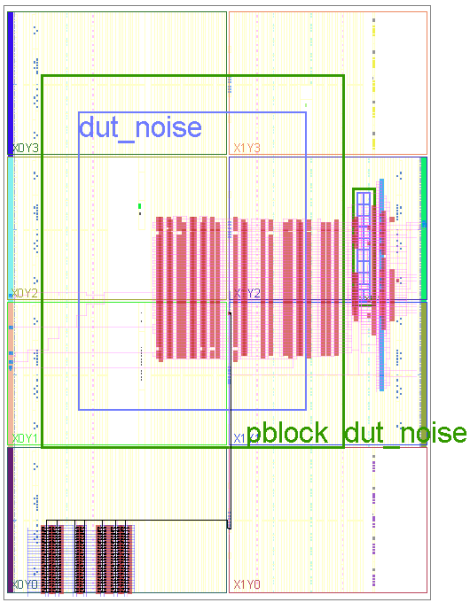

Figure 3.20: Layout of 258 tap Voltage Sensor with Power Generation module

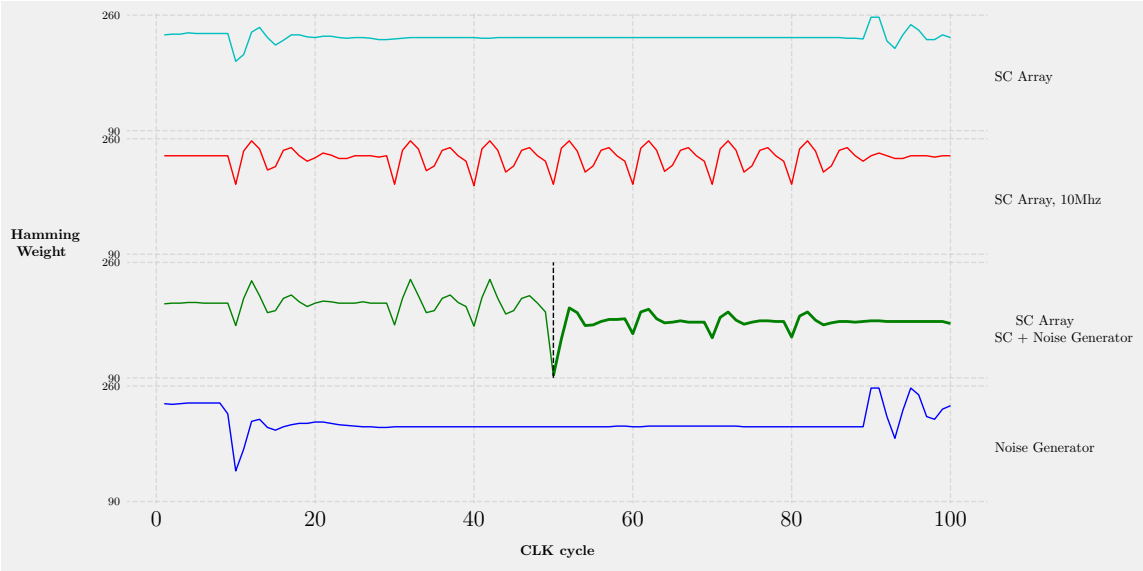

Figure 3.21: Noise Test of 258 tap Voltage Sensor within High Power Consumption Level

The circuit placement was precisely determined by using pblock constraints to ensure its

accurate position on the board. The attack mechanism consists of an SC array situated in the X0Y0:X20Y20 area of the board. To create the SC array, we employed the RapidWrite tool, configuring the LUT and Routing MUX components as detailed in Section 3.2. The findings from the experiment are depicted in Figure 3.19. Observing the top portion of the plot, one can discern the response behavior of the SC array when the power consumption module is deactivated. The SC module gets activated at the 10th clock cycle and is turned off by the 90th clock cycle. The graph indicates that the response amplitude is approximately 22 Hamming weight values. This is a higher amplitude compared to the Mapping test mentioned in Section 3.4. The difference is attributed to the use of a 20x20 array in this experiment as opposed to the 15x15 array utilized in the prior test.

The response behavior of the Noise Generator is showcased in the bottom section of the graph. As anticipated, the amplitude of its signal significantly exceeds that of the SC array. The signal peaks at a Hamming weight of 90 and dips to a minimum of 10 when the Power generation module is deactivated. Both plots display a fairly consistent behavior during the active phases of the generation modules. The red graph depicts how the SC array performs when triggered at a 10 Mhz frequency. The green graph represents the intertwined behavior of both the SC array and the Noise generation module. We set out to examine the Voltage sensor's proficiency in identifying glitches, especially in conditions saturated with Voltage noise. To do this, we switched on the SC array at the 8th clock cycle and the Noise generator module at the 50th clock cycle. At the latter mark, the Voltage dips to its nadir, showing a minimum value of Hamming weight 8, indicating the combined power drop of the two modules. In the second half of the graph, which represents cumulative data, we notice a behavior reminiscent of the SC array. However, due to elevated power consumption, the nominal level of fluctuations isn't as high. It's evident that the circuit displays similar response patterns but at a reduced power consumption level. The design for the 258 tap Voltage Sensor experiment is depicted in Figure 3.20 and the results of the experiment are introduced in Figure 3.21. As anticipated, we note a considerably greater amplitude range in this experiment compared to the one using the 90 tap Voltage sensor. An interesting observation is that the spike in voltage after triggering the Noise Generator is noticeably less compared to the spike after activating the SC array, a variance stemming from the differing behaviors of RO and SC arrays. From the two experiments, several key insights emerge. Foremost, even within a high power consumption environment, the sensor effectively captures the glitch behavior, which can be especially advantageous when deploying in cloud environments. Moreover, we observe that the alternate RO array setups can effectively employ power consumption hiding modules to disguise the activities of a potential target circuit.

Chapter 4: Discussion

In the subsequent section, we outline the key findings from our experiments. We highlight which designs prove most advantageous under specific circumstances, provide recommendations for implementing the TDC Voltage Sensor to counteract malicious usage, and suggest potential directions for future studies on this particular subject.

After initially building the TDC Voltage Glitch sensor with its self-calibrating module, we found that such sensors can greatly benefit hardware security developers. The preliminary calibration test, as referenced in Test 3.1.1, demonstrates the efficiency of our proposed calibration method. Our innovative technique utilizes the phase shift clock functionality of the Mixed-Mode Clock Manager (MMCM) Module in Xilinx Vivado [87]. The calibration module oversees the MMCM, adjusting phase shift based on the delay line outputs. Consequently, MMCM can dynamically alter the clock phase between the tdl_in input signal to the delay line and the system clock, establishing the necessary delay to effectively detect voltage glitches. This allows us to establish any specified Q_{nom} values for the Hamming weight, based on the desired range and precision needed for evaluation.

The subsequent Peak-to-Peak test 3.3 validates the effectiveness of our novel calibration technique, further underscoring its significance. In this test, we evaluated two variations of our Voltage sensors with 90 and 258 taps. The outcomes, presented in Table 3.1, highlight the direct relationship between Q_{nom} value and its sensitivity, depicted through the amplitude value of the Voltage glitch. From these results, it's evident that it's practical to design sensors with a larger initial delay relative to the observable portion, or in our instance, by setting a higher Q_{nom} value for the Hamming weight. This approach is especially suited for detecting decreases in voltage, as it doesn't require monitoring large voltage spikes. Consequently, this technique ensures the optimal quantization level for detection, yielding precise and trustworthy readings. Moreover, when contrasting sensors with different delay line lengths of 90 and 258 taps, we discern the strengths and weaknesses of each. The clear advantage of the sensor with a shorter delay line lies in its spatial efficiency. Specifically, our 90 tap Voltage sensor uses only about a third of the space needed for the 258 tap Voltage sensor, which can be an asset in cloud settings. Conversely, when space isn't a primary concern, the 258 tap sensor excels in sensitivity and the range of glitches it

can detect. Therefore, when determining the optimal delay length for a sensor, designers should weigh three primary factors: the desired quantization level for detecting variations, available space, and the necessary detection range for glitches.

In the subsequent mapping test 3.4, we examine the correlation between the positions of RO and SC arrays on the board for the two TDC Voltage sensors with 90 and 258 taps. Both series of experiments showcase the effectiveness of both RO and SC arrays as power consumption devices independently on their location on the board. Furthermore, the collective findings from our tests support the notion that our sensors perform effectively regardless their mapping relative to the target circuits. This implies that malicious actors could use them efficiently. Conversely, it offers greater flexibility in positioning when implementing effective voltage sensors to detect Voltage glitch attacks, thus bolstering hardware security. Both the RO and SC arrays have distinct advantages, as evidenced by our comprehensive testing. RO devices shine in terms of a smaller footprint and ease of implementation. While conventional hardware tools typically discourage combinational loops, workarounds exist such as enabling permissions constraints in Vivado Xilinx or adapting RO circuits using latches or FFs. Conversely, SC arrays demand more intricate implementation, frequently necessitating the use of external tools because of standard design flows prohibit the configuration of Routing MUXs. Our method employed the RapidWrite tool for internal modifications, subsequently producing SC checkpoints. SC arrays excel in their performance, capturing significantly higher Hamming weight amplitude values in our tests. Both arrays, with their unique efficiencies, prove essential in countering Voltage glitch attacks, a claim corroborated by our subsequent Noise experiment.

The noise test 3.5 highlights the pronounced efficacy of the SC array when used in Fault Injection attacks. In our tests, we situated a substantial RO array, comprising 15,000 RO circuits, in proximity to the sensor. Despite this heightened consumption level, upon activating the 15,000 RO power consumption noise generator, our 90-tap TDC sensor detected Voltage glitches with a 17 Hamming weight amplitude value. In comparison, the 258-tap Voltage sensor recorded a 38 amplitude value. These findings indicate that the SC array can be exploited by malicious users in various capacities, notably as efficient power consumption units, while maintaining a comparatively smaller spatial footprint. Thus, it's imperative for hardware security developers to be cognizant of these findings and devise countermeasures to prevent its malicious utilization in remote power analysis attacks. Conversely, the noise test 3.5 reveals that the power consumption module placed ahead of the voltage sensors is able to reduce the voltage glitch introduced by the 20x20 SC array. This unequivocally indicates a vast array of possibilities in employing these power consumption modules as a shielding device to obscure critical side-channel information that could

be exploited by malevolent actors in cloud settings.

The intrinsic advantages of TDC delay line-based sensors, combined with the capabilities of RO and SC power consumption arrays, underscore the imperative of thorough assessment of these tools. Subsequent strategic incorporation in hardware architecture is crucial to preemptively guard against potential Voltage glitch vulnerabilities.

Chapter 5: Conclusion

In the evolving landscape of FPGA hardware security, the pivotal role of TDC Voltage sensors emerges as both a beacon of promise and a subject demanding meticulous scrutiny. This research journey into understanding TDCs, specifically the TDC Voltage delay line base sensors, provides a blueprint for unlocking their potential in fortifying FPGA-based systems against malicious activities.

Our study revealed a high potential of the TDC voltage sensor, especially with the innovative self-calibrating unit, as well as the opportunities presented by RO and SC arrays. The ingenuity of our calibration approach, leveraging the Mixed-Mode Clock Manager (MMCM) in Xilinx Vivado, lays down a marker for future endeavors in the domain. Not only does it streamline the detection of voltage glitches, but it also fine-tunes the process to a high degree of precision and controllability.

Subsequent examinations, spanning from the Peak-to-Peak to the Mapping tests, emphasized the flexibility and dynamism these sensors bring to the table. They revealed a harmonious balance between spatial efficiency and detection sensitivity, a duality pivotal for any hardware security tool. Our findings elucidate a clear roadmap for sensor design, underpinned by the trinity of considerations: quantization, spatial constraints, and glitch detection range. Furthermore, our deep dives into RO and SC array performances highlighted their dual potential. While they can be instrumental in safeguarding against voltage glitch attacks, they also hold a high potential for malicious usage. This dual-edge nature underscores the need for hardware security professionals to always be several steps ahead, preempting possible malevolent exploitation.

The noise test draws attention to the risks and rewards embedded within the SC array. Its prowess as an efficient power consumption unit presents a robust shield against potential vulnerabilities. While its ability to be an efficient power consumption unit stands out, the potential for its exploitation in remote power analysis attacks serves as a warning story.

Building on these findings, the next frontier in FPGA hardware security will involve a more integrated approach, weaving together the strengths of TDC voltage sensors, RO, and SC arrays, and new protective modules. It's clear that while using TDC Voltage sensors for detecting glitches offer much promise, it's not a panacea. There will be a need for continued research, development, and testing. The dynamic nature of digital threats means that tools and methodologies will need

to evolve in tandem. Moreover, as FPGA architectures become more complex and integrated into a wider array of applications that require constant security control, from cloud computing to edge devices, the inherent challenges tied to hardware security intensify. Potential vulnerabilities could emerge from unexpected quarters, making the task of securing systems even more intricate. However, with the foundational knowledge this research provides, future endeavors can be approached with a mix of caution and optimism. Integration of AI-driven threat detection alongside TDC Voltage sensors, for instance, could be the next step to bolster security measures. These intelligent systems can analyze patterns, predict potential vulnerabilities, and provide real-time feedback to hardware components, ensuring that FPGA systems are constantly adapting and improving their defense mechanisms. Thus, collaboration between FPGA designers, software developers, and hardware security experts is paramount. As FPGA components get embedded in more varied environments, understanding the specific security challenges of each use-case becomes essential. Such collaboration would result in design methodologies that inherently prioritize security from the ground up, rather than treating it as an afterthought. The escalating reliance on FPGAs for critical system functions underscores the need for enhanced security measures. Harnessing the newest breakthroughs in sensor technology combined with AI-driven insights propels us towards a more robust hardware landscape. Merging time-tested techniques with cutting-edge innovations heralds a bright horizon for FPGA security.

In conclusion, this detailed study of TDC voltage sensors within RO and SC arrays signifies an important milestone in the continuing journey of enhancing FPGA security. As we traverse the constantly changing digital environment, the techniques, knowledge, and approaches highlighted in this study will surely act as beacons, guaranteeing that FPGA frameworks stand robust against the continually emerging challenges.

Bibliography

[1] Alberto Aloisio, Paolo Branchini, Roberta Cicalese, Raffaele Giordano, Vincenzo Izzo, and Salvatore Loffredo. "FPGA Implementation of a High-Resolution Time-to-Digital Converter." In: *2007 IEEE Nuclear Science Symposium Conference Record*. Vol. 1. Oct. 2007, pp. 504–507.

[2] Md Toufiq Hasan Anik, Jean-Luc Danger, Sylvain Guilley, and Naghmeh Karimi. "Detecting Failures and Attacks via Digital Sensors." In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 40.7 (July 2021), pp. 1315–1326.

[3] Antonio Aprile, Elisabetta Moisello, Edoardo Bonizzoni, and Piero Malcovati. "An Extensive Investigation and Analysis of Temperature-to-Digital Converter FoMs." In: *2021 28th IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*. Nov. 2021, pp. 1–4.

[4] Mario Barbareschi, Giorgio Di Natale, and Lionel Torres. "Implementation and Analysis of Ring Oscillator Circuits on Xilinx FPGAs." In: *Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment*. Jan. 14, 2017, pp. 237–251.

[5] Eugen Bayer and Michael Traxler. "A High-Resolution (< 10 \rm Ps RMS) 48-Channel Time-to-Digital Converter (TDC) Implemented in a Field Programmable Gate Array (FPGA)." In: *IEEE Transactions on Nuclear Science* 58.4 (Aug. 2011), pp. 1547–1552.

[6] Eugen Bayer, Peter Zipf, and Michael Traxler. "A Multichannel High-Resolution (<5 Ps RMS between Two Channels) Time-to-Digital Converter (TDC) Implemented in a Field Programmable Gate Array (FPGA)." In: *2011 IEEE Nuclear Science Symposium Conference Record*. Oct. 2011, pp. 876–879.

[7] Eduardo Boemo and Sergio López-Buedo. "Thermal Monitoring on FPGAs Using Ring-Oscillators." In: *Field-Programmable Logic and Applications*. Ed. by Wayne Luk, Peter Y. K. Cheung, and Manfred Glesner. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1997, pp. 69–78.

[8] Keith A. Bowman, Carlos Tokunaga, Tanay Karnik, Vivek K. De, and Jim W. Tschanz. "A 22nm Dynamically Adaptive Clock Distribution for Voltage Droop Tolerance." In: *2012 Symposium on VLSI Circuits (VLSIC)*. June 2012, pp. 94–95.

[9] Jakub Breier, Shivam Bhasin, and Wei He. “An Electromagnetic Fault Injection Sensor Using Hogge Phase-Detector.” In: *2017 18th International Symposium on Quality Electronic Design (ISQED)*. Mar. 2017, pp. 307–312.

[10] Julien Brouchier, Tom Kean, Carol Marsh, and David Naccache. “Temperature Attacks.” In: *IEEE Security & Privacy* 7.2 (Mar. 2009), pp. 79–82.

[11] D. Brown et al. “Design and Implementation of a Low-Resource 64-Tap FPGA-Based Time-to-Digital Converter.” In: *IEEE Transactions on Instrumentation and Measurement* 67.11 (2018), pp. 2709–2717.

[12] Juan Pablo Caram, Jeff Galloway, and J. Stevenson Kenney. “Time-to-Digital Converter With Sample-and-Hold and Quantization Noise Scrambling Using Harmonics in Ring Oscillators.” In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 65.1 (Jan. 2018), pp. 74–83.

[13] Juan Pablo Caram, Jeff Galloway, and J. Stevenson Kenney. “Time-to-Digital Converter With Sample-and-Hold and Quantization Noise Scrambling Using Harmonics in Ring Oscillators.” In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 65.1 (Jan. 2018), pp. 74–83.

[14] Chun-Chi Chen, Chao-Lieh Chen, Wei Fang, and Yen-Chan Chu. “All-Digital CMOS Time-to-Digital Converter With Temperature-Measuring Capability.” In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 28.9 (Sept. 2020), pp. 2079–2083.

[15] Chun-Chi Chen, Poki Chen, Chorng-Sii Hwang, and Wei Chang. “A Precise Cyclic CMOS Time-to-Digital Converter with Low Thermal Sensitivity.” In: *IEEE Transactions on Nuclear Science* 52.4 (Aug. 2005), pp. 834–838.

[16] Chun-Chi Chen, Shih-Hao Lin, and Chorng-Sii Hwang. “An Area-Efficient CMOS Time-to-Digital Converter Based on a Pulse-Shrinking Scheme.” In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 61.3 (Mar. 2014), pp. 163–167.

[17] Chun-Chi Chen, An-Wei Liu, Yu-Chi Chang, and Poki Chen. “An Accurate CMOS Time-to-Digital-Converter-Based Smart Temperature Sensor with Negative Thermal Coefficient.” In: *2005 IEEE SENSORS*. Oct. 2005, 4 pp.-.

[18] Poki Chen, Chun-Chi Chen, Chin-Chung Tsai, and Wen-Fu Lu. “A Time-to-Digital-Converter-Based CMOS Smart Temperature Sensor.” In: *IEEE Journal of Solid-State Circuits* 40.8 (Aug. 2005), pp. 1642–1648.

[19] Poki Chen, Mon-Chau Shie, Zhi-Yuan Zheng, Zi-Fan Zheng, and Chun-Yan Chu. "A Fully Digital Time-Domain Smart Temperature Sensor Realized With 140 FPGA Logic Elements." In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 54.12 (Dec. 2007), pp. 2661–2668.

[20] Z. Chen, S. Liu, and L. Cao. "A New Design of High-Resolution TDC for High-Energy Physics Experiments." In: *IEEE Transactions on Nuclear Science* 50.5 (2003), pp. 1557–1562.

[21] Nakjun Choi, Jeeun Lee, and Kwangjo Kim. "Fault Injection, Simple Power Analysis, and Power Glitch Attacks against FPGA-implemented Xoroshiro128+." In: (Jan. 23, 2019).

[22] Hayden Cook, Jacob Arscott, Brent George, Tanner Gaskin, Jeffrey Goeders, and Brad Hutchings. "Inducing Non-uniform FPGA Aging Using Configuration-based Short Circuits." In: *ACM Transactions on Reconfigurable Technology and Systems* 15.4 (Dec. 31, 2022), pp. 1–33.

[23] Ke Cui, Zhongjie Ren, Xiangyu Li, Zongkai Liu, and Rihong Zhu. "A High-Linearity, Ring-Oscillator-Based, Vernier Time-to-Digital Converter Utilizing Carry Chains in FPGAs." In: *IEEE Transactions on Nuclear Science* 64.1 (Jan. 2017), pp. 697–704.

[24] Ke Cui, Jintao Yu, Jiaxuan Zou, and Xiangyu Li. "A High-Resolution TDC Design Based on Multistep Fine Time Measurement by Utilizing Delay-Adjustable Looped Carry Chains on FPGAs." In: *IEEE Transactions on Instrumentation and Measurement* 72 (2023), pp. 1–10.

[25] Chinmay Deshpande, Bilgiday Yuce, Leyla Nazhandali, and Patrick Schaumont. "Employing Dual-Complementary Flip-Flops to Detect EMFI Attacks." In: *2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. Oct. 2017, pp. 109–114.

[26] Christos Diktopoulos, Konstantinos Georgopoulos, Andreas Brokalakis, Georgios Christou, Grigorios Chrysos, Ioannis Morianos, and Sotiris Ioannidis. "Assessing the Effectiveness of Active Fences Against SCAs for Multi-Tenant FPGAs." In: *2022 32nd International Conference on Field-Programmable Logic and Applications (FPL)*. Aug. 2022, pp. 391–396.

[27] Shijin Duan, Wenhao Wang, Yukui Luo, and Xiaolin Xu. "A Survey of Recent Attacks and Mitigation on FPGA Systems." In: *2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. July 2021, pp. 284–289.

[28] Mohammad Ebrahimabadi, Suhee Sanjana Mehjabin, Raphael Viera, Sylvain Guilley, Jean-Luc Danger, Jean-Max Dutertre, and Naghmeh Karimi. "Detecting Laser Fault Injection Attacks via Time-to-Digital Converter Sensors." In: *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. June 2022, pp. 97–100.

[29] Anis Fellah-Touta, Lilian Bossuet, and Carlos Andres Lara-Nino. “Combined Internal Attacks on SoC-FPGAs: Breaking AES with Remote Power Analysis and Frequency-based Covert Channels.” In: *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. July 2023, pp. 281–286.

[30] John J. Leon Franco, Eduardo Boemo, Encarnacion Castillo, and Luis Parrilla. “Ring oscillators as thermal sensors in FPGAs: Experiments in low voltage.” In: *2010 VI Southern Programmable Logic Conference (SPL)*. IEEE, Mar. 2010. URL: https://doi.org/10.1109%2Fspl.2010.5483027.

[31] Daisuke Fujimoto, Yu-ichi Hayashi, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede. “Detection of IEMI Fault Injection Using Voltage Monitor Constructed with Fully Digital Circuit.” In: *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*. May 2018, pp. 753–755.

[32] Navyata Gattu, Mohammad Nasim Imtiaz Khan, Asmit De, and Swaroop Ghosh. “Power Side Channel Attack Analysis and Detection.” In: *Proceedings of the 39th International Conference on Computer-Aided Design*. ICCAD ’20. New York, NY, USA: Association for Computing Machinery, Dec. 17, 2020, pp. 1–7.

[33] Ilias Giechaskiel, Kasper Rasmussen, and Jakub Szefer. “Reading Between the Dies: Cross-SLR Covert Channels on Multi-Tenant Cloud FPGAs.” In: *2019 IEEE 37th International Conference on Computer Design (ICCD)*. Nov. 2019, pp. 1–10.

[34] Ilias Giechaskiel, Kasper Rasmussen, and Jakub Szefer. “Reading Between the Dies: Cross-SLR Covert Channels on Multi-Tenant Cloud FPGAs.” In: *2019 IEEE 37th International Conference on Computer Design (ICCD)*. Nov. 2019, pp. 1–10.

[35] Ilias Giechaskiel, Kasper Rasmussen, and Jakub Szefer. “Reading Between the Dies: Cross-SLR Covert Channels on Multi-Tenant Cloud FPGAs.” In: *2019 IEEE 37th International Conference on Computer Design (ICCD)*. Nov. 2019, pp. 1–10.

[36] Ilias Giechaskiel, Kasper Bonne Rasmussen, and Jakub Szefer. “Measuring Long Wire Leakage with Ring Oscillators in Cloud FPGAs.” In: *2019 29th International Conference on Field Programmable Logic and Applications (FPL)*. Sept. 2019, pp. 45–50.

[37] Ilias Giechaskiel, Kasper Bonne Rasmussen, and Jakub Szefer. “C3APSULe: Cross-FPGA Covert-Channel Attacks through Power Supply Unit Leakage.” In: *2020 IEEE Symposium on Security and Privacy (SP)*. May 2020, pp. 1728–1741.

[38] Ognjen Glamocanin. “Evaluating, Exploiting, and Hiding Power Side-Channel Leakage of Remote FPGAs.” Lausanne: EPFL, 2023. 249 pp.

[39] Ognjen Glamočanin, Hajira Bazaz, Mathias Payer, and Mirjana Stojilović. “Temperature Impact on Remote Power Side-Channel Attacks on Shared FPGAs.” In: *2023 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. Apr. 2023, pp. 1–6.

[40] Ognjen Glamočanin, Anđela Kostić, Staša Kostić, and Mirjana Stojilović. “Active Wire Fences for Multitenant FPGAs.” In: *2023 26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*. May 2023, pp. 13–20.

[41] Dennis R. E. Gnad, Cong Dang Khoa Nguyen, Syed Hashim Gillani, and Mehdi B. Tahoori. “Voltage-Based Covert Channels Using FPGAs.” In: *ACM Transactions on Design Automation of Electronic Systems* 26.6 (June 28, 2021), 43:1–43:25.

[42] Dennis R. E. Gnad, Fabian Oboril, Saman Kiamehr, and Mehdi B. Tahoori. “An Experimental Evaluation and Analysis of Transient Voltage Fluctuations in FPGAs.” In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 26.10 (Oct. 2018), pp. 1817–1830.

[43] Dennis R. E. Gnad, Fabian Oboril, and Mehdi B. Tahoori. “Voltage Drop-Based Fault Attacks on FPGAs Using Valid Bitstreams.” In: *2017 27th International Conference on Field Programmable Logic and Applications (FPL)*. 2017, pp. 1–7.

[44] Joseph Gravellier, Jean-Max Dutertre, Yannick Teglia, and Philippe Loubet-Moundi. “High-Speed Ring Oscillator Based Sensors for Remote Side-Channel Attacks on FPGAs.” In: *2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*. Dec. 2019, pp. 1–8.

[45] Joseph Gravellier, Jean-Max Dutertre, Yannick Teglia, and Philippe Loubet Moundi. “Side-Line: How Delay-Lines (May) Leak Secrets from Your SoC.” In: *Constructive Side-Channel Analysis and Secure Design*. Springer International Publishing, 2021, pp. 3–30. URL: https://doi.org/10.1007%2F978-3-030-89915-8_1.

[46] Werner Grollitsch, Roberto Nonis, and Nicola Da Dalt. “A 1.4psrms-Period-Jitter TDC-less Fractional-N Digital PLL with Digitally Controlled Ring Oscillator in 65nm CMOS.” In: *2010 IEEE International Solid-State Circuits Conference - (ISSCC)*. Feb. 2010, pp. 478–479.

[47] Mathieu Gross, Jonas Krautter, Dennis Gnad, Michael Gruber, Georg Sigl, and Mehdi Tahoori. “FPGANeedle: Precise Remote Fault Attacks from FPGA to CPU.” In: *Proceedings of the 28th Asia and South Pacific Design Automation Conference*. ASPDAC ’23. New York, NY, USA: Association for Computing Machinery, Jan. 31, 2023, pp. 358–364.

[48] Mathieu Gross, Robert Kunzelmann, and Georg Sigl. *CPU to FPGA Power Covert Channel in FPGA-SoCs*. 2023. preprint.

[49] Lipika Gupta, Tripti Sharma, and Bhavani Saranga. "Ring Oscillators Based All Digital Phase Locked Loop: A Comparative Study." In: *2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT)*. Mar. 2023, pp. 238–242.

[50] Mordechai Guri, Matan Monitz, Yisroel Mirski, and Yuval Elovici. "BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations." In: *2015 IEEE 28th Computer Security Foundations Symposium*. IEEE, July 2015. URL: https://doi.org/10.1109%2Fcsf.2015.26.

[51] Ali Hasnain, Yame Asfia, and Sajid Gul Khawaja. "Power Profiling-Based Side-Channel Attacks on FPGA and Countermeasures: A Survey." In: *2022 2nd International Conference on Digital Futures and Transformative Technologies (ICoDT2)* (May 24, 2022), pp. 1–8.

[52] Wei He, Jakub Breier, Shivam Bhasin, Noriyuki Miura, and Makoto Nagata. "Ring Oscillator under Laser: Potential of PLL-based Countermeasure against Laser Fault Injection." In: *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. Aug. 2016, pp. 102–113.

[53] Tamzidul Hoque. "Ring Oscillator Based Hardware Trojan Detection." University of Toledo, 2015.

[54] Jiajian Huang, Shengyao Ran, Wei Wei, and Qun Yu. "Digital Integration of LiDAR System Implemented in a Low-Cost FPGA." In: *Symmetry* 14.6 (6 June 2022), p. 1256.

[55] Qiwei Huang, Hyobin Joo, Jinwoo Kim, Chenchang Zhan, and Jinwook Burm. "An Energy-Efficient Frequency-Domain CMOS Temperature Sensor With Switched Vernier Time-to-Digital Conversion." In: *IEEE Sensors Journal* 17.10 (May 2017), pp. 3001–3011.

[56] Taras Iakymchuk, Maciej Nikodem, and Krzysztof Kępa. "Temperature-Based Covert Channel in FPGA Systems." In: *6th International Workshop on Reconfigurable Communication-Centric Systems-on-Chip (ReCoSoC)*. June 2011, pp. 1–7.

[57] Tetsuya Iizuka, Teruki Someya, Toru Nakura, and Kunihiro Asada. "An All-Digital Time Difference Hold-and-Replication Circuit Utilizing a Dual Pulse Ring Oscillator." In: *Proceedings of the IEEE 2013 Custom Integrated Circuits Conference*. Sept. 2013, pp. 1–4.

[58] Mohammad A. Islam, Shaolei Ren, and Adam Wierman. “Exploiting a Thermal Side Channel for Power Attacks in Multi-Tenant Data Centers.” In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Oct. 2017. URL: https://doi.org/10.1145%2F3133956.3133994.

[59] Darshana Jayasinghe, Brian Udugama, and Sri Parameswaran. “FPGA Based Countermeasures against Side Channel Attacks on Block Ciphers.” In: *Proceedings of the 28th Asia and South Pacific Design Automation Conference*. ASPDAC ’23. New York, NY, USA: Association for Computing Machinery, Jan. 31, 2023, pp. 365–371.

[60] Kentaroh Katoh and Kazuteru Namba. “Time-to-Digital Converter-Based Maximum Delay Sensor for On-Line Timing Error Detection in Logic Block of Very Large Scale Integration Circuits.” In: *Sensors and Materials* 27 (Jan. 1, 2015).

[61] Shane Kelly, Xuehui Zhang, Mohammed Tehranipoor, and Andrew Ferraiuolo. In: *J Electron Test* 31.1 (Feb. 2015), pp. 11–26. URL: https://doi.org/10.1007%2Fs10836-015-5504-x.

[62] F. Kiamilev, R. Hoover, R. Delvecchio, N. Waite, S. Janansky, R. McGee, C. Lange, and M. Stamat. “Demonstration of Hardware Trojans.” In: *DEFCON* (2008).

[63] Paul Kocher, Joshua Jaffe, and Benjamin Jun. “Differential Power Analysis.” In: *Advances in Cryptology — CRYPTO’ 99*. Ed. by Michael Wiener. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1999, pp. 388–397.

[64] Jun Yu Koh and T. Nandha Kumar. “Review of Side Channel Attacks and Countermeasures of FPGA Based Systems.” In: *2021 IEEE 19th Student Conference on Research and Development (SCOReD)*. Nov. 2021, pp. 102–107.

[65] Jun Yu Koh and T. Nandha Kumar. “Review of Side Channel Attacks and Countermeasures of FPGA Based Systems.” In: *2021 IEEE 19th Student Conference on Research and Development (SCOReD)*. Nov. 2021, pp. 102–107.

[66] Jonas Krautter, Dennis Gnad, and Mehdi Tahoori. “CPAmap: On the Complexity of Secure FPGA Virtualization, Multi-Tenancy, and Physical Design.” In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (June 19, 2020), pp. 121–146.

[67] Jonas Krautter, Dennis R. E. Gnad, and Mehdi B. Tahoori. “Mitigating Electrical-level Attacks towards Secure Multi-Tenant FPGAs in the Cloud.” In: *ACM Transactions on Reconfigurable Technology and Systems* 12.3 (Aug. 13, 2019), 12:1–12:26.

[68] Jonas Krautter, Dennis R.E. Gnad, Falk Schellenberg, Amir Moradi, and Mehdi B. Tahoori. "Active Fences against Voltage-based Side Channels in Multi-Tenant FPGAs." In: *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. Nov. 2019, pp. 1–8.

[69] R. S. S. M. R. Krishna, Ashis Kumar Mal, and Rajat Mahapatra. "Time-Domain Smart Temperature Sensor Using Current Starved Inverters and Switched Ring Oscillator-Based Time-to-Digital Converter." In: *Circuits, Systems, and Signal Processing* 39.4 (Apr. 1, 2020), pp. 1751–1769.

[70] R. S. S. M. R. Krishna, Ashis Kumar Mal, and Rajat Mahapatra. "CMOS Time-Mode Smart Temperature Sensor Using Programmable Temperature Compensation Devices and $$\Delta \Sigma$$ Time-to-Digital Converter." In: *Analog Integrated Circuits and Signal Processing* 102.1 (Jan. 1, 2020), pp. 97–109.

[71] P. Kwiatkowski and R. Szplet. "Time-to-Digital Converter with Pseudo-Segmented Delay Line." In: *2019 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*. May 2019, pp. 1–6.

[72] Yuan Liang, Xing Gao, Kun Sun, Wenjie Xiong, and Haining Wang. "An Investigation on Data Center Cooling Systems Using FPGA-based Temperature Side Channels." In: *2022 41st International Symposium on Reliable Distributed Systems (SRDS)*. Sept. 2022, pp. 46–57.

[73] Lang Lin, Markus Kasper, Tim Güneysu, Christof Paar, and Wayne Burleson. "Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering." In: *Cryptographic Hardware and Embedded Systems - CHES 2009*. Ed. by Christophe Clavier and Kris Gaj. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009, pp. 382–395.

[74] Technical Paper Link. *Covert Channel Between the CPU and An FPGA By Modulating The Usage of the Power Distribution Network*. Mar. 30, 2023.

[75] Chong Liu and Yonggang Wang. "A 128-Channel, 710 M Samples/Second, and Less Than 10 Ps RMS Resolution Time-to-Digital Converter Implemented in a Kintex-7 FPGA." In: *IEEE Transactions on Nuclear Science* 62.3 (June 2015), pp. 773–783.

[76] R. Liu, Y. Yan, and S. Han. "A 10ps Resolution Time-to-Digital Converter with Power-Efficient Coarse-Fine Time-Interval Histogramming." In: *IEEE International Solid-State Circuits Conference (ISSCC)*. 2015, pp. 1–3.

[77] S. Lopez-Buedo, J. Garrido, and E. Boemo. “Thermal testing on reconfigurable computers.” In: *IEEE Des. Test. Comput. Design & Test of Computers* 17.1 (2000), pp. 84–91. URL: https://doi.org/10.1109%2F54.825679.

[78] S. Lopez-Buedo, J. Garrido, and E.I. Boemo. “Dynamically Inserting, Operating, and Eliminating Thermal Sensors of FPGA-based Systems.” In: *IEEE Transactions on Components and Packaging Technologies* 25.4 (Dec. 2002), pp. 561–566.

[79] Ping Lu, Ying Wu, and Pietro Andreani. “A 90nm CMOS Digital PLL Based on Vernier-Gated-Ring-Oscillator Time-to-Digital Converter.” In: *2012 IEEE International Symposium on Circuits and Systems (ISCAS)*. May 2012, pp. 2593–2596.

[80] Yukui Luo and Xiaolin Xu. “A Quantitative Defense Framework against Power Attacks on Multi-tenant FPGA.” In: *2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*. Nov. 2020, pp. 1–4.

[81] Dina Mahmoud and Mirjana Stojilović. “Timing Violation Induced Faults in Multi-Tenant FPGAs.” In: *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. Mar. 2019, pp. 1745–1750.

[82] Adrien Le Masle and Wayne Luk. “Detecting Power Attacks on Reconfigurable Hardware.” In: *22nd International Conference on Field Programmable Logic and Applications (FPL)*. Aug. 2012, pp. 14–19.

[83] Mahantesh P Mattad, Hansraj Guhilot, and Rajanish K Kamat. “Area Efficient Time to Digital Converter (TDC) Architecture with Double Ring-Oscillator Technique on FPGA for Fluorescence Measurement Application.” In: *2011 IEEE Recent Advances in Intelligent Computational Systems*. Sept. 2011, pp. 260–263.

[84] Ivan Miketic, Krithika Dhananjay, and Emre Salman. “Covert Channel Communication as an Emerging Security Threat in 2.5D/3D Integrated Systems.” In: *Sensors* 23.4 (4 Jan. 2023), p. 2081.

[85] Seyedeh Sharareh Mirzargar and Mirjana Stojilović. “Physical Side-Channel Attacks and Covert Communication on FPGAs: A Survey.” In: *2019 29th International Conference on Field Programmable Logic and Applications (FPL)*. Sept. 2019, pp. 202–210.

[86] Noriyuki Miura, Zakaria Najm, Wei He, Shivam Bhasin, Xuan Thuy Ngo, Makoto Nagata, and Jean-Luc Danger. “PLL to the Rescue: A Novel EM Fault Countermeasure.” In: *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. June 2016, pp. 1–6.

[87] *Mixed-Mode Clock Manager (MMCM) Module*. URL: https://www.xilinx.com/products/intellectual-property/mmcm_module.html.

[88] Shayan Moini, Aleksa Deric, Xiang Li, George Provelengios, Wayne Burleson, Russell Tessier, and Daniel Holcomb. "Voltage Sensor Implementations for Remote Power Attacks on FPGAs." In: *ACM Transactions on Reconfigurable Technology and Systems* 16.1 (Dec. 22, 2022), 11:1–11:21.

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

[90] Md Rafid Muttaki, Tao Zhang, Mark Tehranipoor, and Farimah Farahmandi. "FTC: A Universal Sensor for Fault Injection Attack Detection." In: *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. June 2022, pp. 117–120.

[91] Md Rafid Muttaki, Tao Zhang, Mark Tehranipoor, and Farimah Farahmandi. "FTC: A Universal Sensor for Fault Injection Attack Detection." In: *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. June 2022, pp. 117–120.

[92] Daniel Nemiroff. "Fault-Injection Countermeasures, Deployed at Scale." In: (2022).

[93] Daniel Nemiroff and Carlos Tokunaga. "Tunable Replica Circuit for Fault- Injection Detection." In: (2022).

[94] Cong Dang Khoa Nguyen. "Voltage-Based Covert Channel Communication between Logically Separated IP Cores in FPGAs." In: (2018).

[95] Ilkka Nissinen and Juha Kostamovaara. "On-Chip Voltage Reference-Based Time-to-Digital Converter for Pulsed Time-of-Flight Laser Radar Measurements." In: *IEEE Transactions on Instrumentation and Measurement* 58.6 (June 2009), pp. 1938–1948.

[96] H. Niu et al. "A High-Linearity FPGA-Based Time-to-Digital Converter Using a Delay LUT." In: *IEEE Transactions on Instrumentation and Measurement* 67.8 (2018), pp. 1879–1887.

[97] Colin O'Flynn. *PicoEMP: A Low-Cost EMFI Platform Compared to BBI and Voltage Fault Injection Using TDC and External VCC Measurements*. 2023. preprint.

[98] Weibin Pan, Guanghua Gong, Hongming Li, and Jianmin Li. "A 20-Ps Temperature Compensated Time-to-Digital Converter (TDC) Implemented in FPGA." In: *2013 IEEE Nuclear Science Symposium and Medical Imaging Conference (2013 NSS/MIC)*. Oct. 2013, pp. 1–6.

[99] Michael Paquette, Brian Marquis, Rachel Bainbridge, and Joe Chapman. "Visualizing Electromagnetic Fault Injection With Timing Sensors." In: *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*. Nov. 2021, pp. 1–8.

[100] Matthias Probst, Lars Tebelmann, Moritz Wettermann, and Michael Pehl. *Remote Side-Channel Analysis of the Loop PUF Using a TDC-Based Voltage Sensor*. preprint. In Review, June 19, 2023.

[101] George Provelengios, Daniel Holcomb, and Russell Tessier. "Mitigating Voltage Attacks in Multi-Tenant FPGAs." In: *ACM Transactions on Reconfigurable Technology and Systems* 14.2 (June 30, 2021), pp. 1–24.

[102] Chethan Ramesh, Shivukumar B. Patil, Siva Nishok Dhanuskodi, George Provelengios, Sebastien Pillement, Daniel Holcomb, and Russell Tessier. "FPGA Side Channel Attacks without Physical Access." In: *2018 IEEE 26th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*. Apr. 2018, pp. 45–52.

[103] *RapidWright*.

[104] Francesco Regazzoni, Yi (Estelle) Wang, and François-Xavier Standaert. "FPGA Implementations of the AES Masked Against Power Analysis Attacks." In: 2011.

[105] Christoph Ruething, Andreas Agne, Markus Happe, and Christian Plessl. "Exploration of Ring Oscillator Design Space for Temperature Measurements on FPGAs." In: *22nd International Conference on Field Programmable Logic and Applications (FPL)*. Aug. 2012, pp. 559–562.

[106] Amer Samarah and Anthony Chan Carusone. "A Digital Phase-Locked Loop With Calibrated Coarse and Stochastic Fine TDC." In: *IEEE Journal of Solid-State Circuits* 48.8 (Aug. 2013), pp. 1829–1841.

[107] Falk Schellenberg, Dennis R. E. Gnad, Amir Moradi, and Mehdi B. Tahoori. "An Inside Job: Remote Power Analysis Attacks on FPGAs." In: *IEEE Design & Test* 38.3 (June 2021), pp. 58–66.

[108] Falk Schellenberg, Dennis R.E. Gnad, Amir Moradi, and Mehdi B. Tahoori. "Remote Inter-Chip Power Analysis Side-Channel Attacks at Board-Level." In: *2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. Nov. 2018, pp. 1–7.

[109] Zhihui Shao, Mohammad A. Islam, and Shaolei Ren. "A First Look at Thermal Attacks in Multi-Tenant Data Centers." In: *SIGMETRICS Perform. Eval. Rev. SIGMETRICS Performance Evaluation Review* 46.2 (Jan. 2019), pp. 93–94. URL: https://doi.org/10.1145%2F3305218.3305254.

[110] T. Shima, S. Kozuki, T. Otsuka, and N. Retdian. "Multi-Phase Ring-Coupled Oscillator for TDC Using a Differential Inverter with an Oscillation Frequency Booster Circuit." In: *2019 IEEE 31st International Conference on Microelectronics (MIEL)*. Sept. 2019, pp. 273–276.

[111] Arvind Singh, Monodeep Kar, Sanu Mathew, Anand Rajan, Vivek De, and Saibal Mukhopadhyay. "Reducing Side-Channel Leakage of Encryption Engines Using Integrated Low-Dropout Voltage Regulators." In: *Journal of Hardware and Systems Security* 1.4 (Dec. 1, 2017), pp. 340–355.

[112] Teruki Someya, A. K. M. Mahfuzul Islam, Takayasu Sakurai, and Makoto Takamiya. "An 11-nW CMOS Temperature-to-Digital Converter Utilizing Sub-Threshold Current at Sub-Thermal Drain Voltage." In: *IEEE Journal of Solid-State Circuits* 54.3 (Mar. 2019), pp. 613–622.

[113] Zhipeng Song, Zhixiang Zhao, Hongsen Yu, Jingwu Yang, Xi Zhang, Tengjie Sui, Jianfeng Xu, Siwei Xie, Qiu Huang, and Qiyu Peng. "An 8.8 Ps RMS Resolution Time-To-Digital Converter Implemented in a 60 Nm FPGA with Real-Time Temperature Correction." In: *Sensors* 20.8 (8 Jan. 2020), p. 2172.

[114] David Spielmann, Ognjen Glamočanin, and Mirjana Stojilović. "RDS: FPGA Routing Delay Sensors for Effective Remote Power Analysis Attacks." In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (Mar. 6, 2023), pp. 543–567.

[115] T. Sugawara, K. Sakiyama, S. Nashimoto, D. Suzuki, and T. Nagatsuka. "Oscillator without a Combinatorial Loop and Its Threat to FPGA in Data Centre." In: *Electronics Letters* 55.11 (2019), pp. 640–642.

[116] Takeshi Sugawara, Tatsuya Onuma, and Yang Li. "(Short Paper) Signal Injection Attack on Time-to-Digital Converter and Its Application to Physically Unclonable Function." In: *Advances in Information and Computer Security*. Ed. by Kazumaro Aoki and Akira Kanaoka. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 117–127.

[117] Ji Sun, Ray Bittner, and Ken Eguro. "FPGA Side-Channel Receivers." In: *Proceedings of the 19th ACM/SIGDA International Symposium on Field Programmable Gate Arrays*. FPGA '11. New York, NY, USA: Association for Computing Machinery, Feb. 27, 2011, pp. 267–276.

[118] Mark Tehranipoor, N. Nalla Anandakumar, and Farimah Farahmandi. "Universal Fault Sensor." In: *Hardware Security Training, Hands-on!* Ed. by Mark Tehranipoor, N. Nalla Anandakumar, and Farimah Farahmandi. Cham: Springer International Publishing, 2023, pp. 273–292.

[119] Shanquan Tian, Shayan Moini, Adam Wolnikowski, Daniel Holcomb, Russell Tessier, and Jakub Szefer. "Remote Power Attacks on the Versatile Tensor Accelerator in Multi-Tenant FPGAs." In: *2021 IEEE 29th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*. May 2021, pp. 242–246.

[120] Shanquan Tian and Jakub Szefer. "Temporal Thermal Covert Channels in Cloud FPGAs." In: *Proceedings of the 2019 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*. FPGA '19. New York, NY, USA: Association for Computing Machinery, Feb. 20, 2019, pp. 298–303.

[121] K. Tiri and I. Verbauwhede. "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation." In: *Automation and Test in Europe Conference and Exhibition Proceedings Design*. Vol. 1. Feb. 2004, 246–251 Vol.1.

[122] Theodoros Trochatos, Anthony Etim, and Jakub Szefer. *Security Evaluation of Thermal Covert-channels on SmartSSDs*. 2023.

[123] Brian Udugama, Darshana Jayasinghe, Hassaan Saadat, Aleksandar Ignjatovic, and Sri Parameswaran. "VITI: A Tiny Self-Calibrating Sensor for Power-Variation Measurement in FPGAs." In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022), pp. 657–678.

[124] Boyan Valtchanov, Alain Aubert, Florent Bernard, and Viktor Fischer. "Modeling and observing the jitter in ring oscillators implemented in FPGAs." In: *2008 11th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems*. IEEE, Apr. 2008. URL: https://doi.org/10.1109%2Fddecs.2008.4538777.

[125] David Vyhlidal and Miroslav Cech. "Time-to-Digital Converter With 2.1-Ps RMS Single-Shot Precision and Subpicosecond Long-Term and Temperature Stability." In: *IEEE Transactions on Instrumentation and Measurement* 65.2 (Feb. 2016), pp. 328–335.

[126] Jinhong Wang, Shubin Liu, Qi Shen, Hao Li, and Qi An. "A Fully Fledged TDC Implemented in Field-Programmable Gate Arrays." In: *IEEE Transactions on Nuclear Science* 57.2 (Apr. 2010), pp. 446–450.

[127] S. Wang et al. "A 64-Tap Time-to-Digital Converter for Space Applications." In: *IEEE International Symposium on Circuits and Systems (ISCAS)*. 2016, pp. 2827–2830.

[128] Kyoungho Woo, Scott Meninger, Thucydides Xanthopoulos, Ethan Crain, Dongwan Ha, and Donhee Ham. "Dual-DLL-based CMOS All-Digital Temperature Sensor for Microprocessor Thermal Monitoring." In: *2009 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*. Feb. 2009, 68–69, 69a.

[129] Xuehui Zhang and M Tehranipoor. "RON: An on-Chip Ring Oscillator Network for Hardware Trojan Detection." In: *2011 Design, Automation & Test in Europe*. Grenoble: IEEE, Mar. 2011, pp. 1–6.

[130] Yuan Yao, Pantea Kiaei, Richa Singh, Shahin Tajik, and Patrick Schaumont. *Programmable RO (PRO): A Multipurpose Countermeasure against Side-channel and Fault Injection Attack*. June 25, 2021. preprint.

[131] Yuan Yao, Pantea Kiaei, Richa Singh, Shahin Tajik, and Patrick Schaumont. *Programmable RO (PRO): A Multipurpose Countermeasure against Side-channel and Fault Injection Attack*. June 25, 2021. preprint.

[132] Chi-En Yin and Gang Qu. "Temperature-aware cooperative ring oscillator PUF." In: *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, 2009. URL: https://doi.org/10.1109%2Fhst.2009.5225055.

[133] Haile Yu, Qiang Xu, and Philip H.W. Leong. "Fine-Grained Characterization of Process Variation in FPGAs." In: *2010 International Conference on Field-Programmable Technology* (Dec. 2010), pp. 138–145.

[134] C. Zhang et al. "Nonlinearity Analysis and Compensation for a Carry 4 Delay Line-Based Time-to-Digital Converter." In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 66.1 (2019), pp. 280–291.

[135] MengDi Zhang, HuaChuang Wang, and Bo Liu. "A High Precision TDC Design Based on FPGA+ARM." In: *Journal of Physics: Conference Series* 1486.7 (Apr. 2020), p. 072054.

[136] Tao Zhang, Md Latifur Rahman, Hadi Mardani Kamali, Kimia Zamiri Azar, Mark Tehranipoor, and Farimah Farahmandi. "FISHI: Fault Injection Detection in Secure Heterogeneous Integration via Power Noise Variation." In: *2023 IEEE 73rd Electronic Components and Technology Conference (ECTC)*. May 2023, pp. 2188–2195.

[137] Tao Zhang, Md Latifur Rahman, Hadi Mardani Kamali, Kimia Zamiri Azar, Mark Tehranipoor, and Farimah Farahmandi. "FISHI: Fault Injection Detection in Secure Heterogeneous Integration via Power Noise Variation." In: *2023 IEEE 73rd Electronic Components and Technology Conference (ECTC)*. May 2023, pp. 2188–2195.

[138] Mark Zhao and G. Edward Suh. "FPGA-Based Remote Power Side-Channel Attacks." In: *2018 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA: IEEE, May 2018, pp. 229–244.

[139] Shuze Zhao, Ibrahim Ahmed, Vaughn Betz, Ashraf Lotfi, and Olivier Trescases. "Frequency-Domain Power Delivery Network Self-Characterization in FPGAs for Improved System Reliability." In: *IEEE Transactions on Industrial Electronics* 65.11 (Nov. 2018), pp. 8915–8924.

[140] Jiajun Zheng, Ping Cao, Di Jiang, and Qi An. "Low-Cost FPGA TDC With High Resolution and Density." In: *IEEE Transactions on Nuclear Science* 64.6 (June 2017), pp. 1401–1408.

[141] Kenneth M. Zick and John P. Hayes. "Low-Cost Sensing with Ring Oscillator Arrays for Healthier Reconfigurable Systems." In: *ACM Transactions on Reconfigurable Technology and Systems* 5.1 (Mar. 23, 2012), 1:1–1:26.

[142] Kenneth M. Zick, Meeta Srivastav, Wei Zhang, and Matthew French. "Sensing Nanosecond-Scale Voltage Attacks and Natural Transients in FPGAs." In: *Proceedings of the ACM/SIGDA International Symposium on Field Programmable Gate Arrays*. Monterey California USA: ACM, Feb. 11, 2013, pp. 101–104.

[143] Daniel Ziener, Florian Baueregger, and Jürgen Teich. "Using the Power Side Channel of FPGAs for Communication." In: *2010 18th IEEE Annual International Symposium on Field-Programmable Custom Computing Machines*. May 2010, pp. 237–244.

[144] Loic Zussa, Jean-Max Dutertre, Jessy Clediere, and Bruno Robisson. "Analysis of the Fault Injection Mechanism Related to Negative and Positive Power Supply Glitches Using an On-Chip Voltmeter." In: *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. May 2014, pp. 130–135.

[145] Loic Zussa, Jean-Max Dutertre, Jessy Clediere, and Bruno Robisson. “Analysis of the Fault Injection Mechanism Related to Negative and Positive Power Supply Glitches Using an On-Chip Voltmeter.” In: *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. May 2014, pp. 130–135.

[146] Loïc Zussa, Jean-Max Dutertre, Jessy Clédière, and Assia Tria. “Power Supply Glitch Induced Faults on FPGA: An in-Depth Analysis of the Injection Mechanism.” In: *2013 IEEE 19th International On-Line Testing Symposium (IOLTS)*. July 2013, pp. 110–115.