A Tunable Dual-Edge Time-to-Digital Converter

Colin Drewes, Steven Harris, Winnie Wang, Richard Appen, Olivia Weng, Ryan Kastner
University of California, San Diego
{cdrewes, s5harris, wbwang, rappen, oweng, kastner}@ucsd.edu

William Hunter, Christopher McCarty
Georgia Tech Research Institute
{bill.hunter, christopher.mccarty}@gtri.gatech.edu

Dustin Richmond
University of Washington
{dustinar}@uw.edu

***Abstract*—Side-channel leakage poses a major security threat in multi-tenant FPGA environments. One tenant can instantiate a voltage fluctuation sensor that measures minute changes in the power distribution network (PDN) and infer information about co-tenant computation and data. This work presents the Tunable Dual-Edged Time-to-Digital Converter (TDC) – a voltage fluctuation sensor with two unique elements: first, it has the ability to tune the sample duration, phase, and frequency to more effectively extract information about the co-located computation; second, it captures both rising and falling transitions which provides unique information about the target computation.**

I. Introduction

As cloud providers deploy FPGAs in data centers, it becomes increasingly clear time-sharing schemes leave large portions of the FPGA under-utilized. Virtualization has been proposed to maximize utilization by supporting multiple concurrent users. This introduces a new class of security attacks that leverage the shared power distribution networks in FPGA systems. These attacks implement some variant of a voltage fluctuation sensor within the programmable logic of the device.

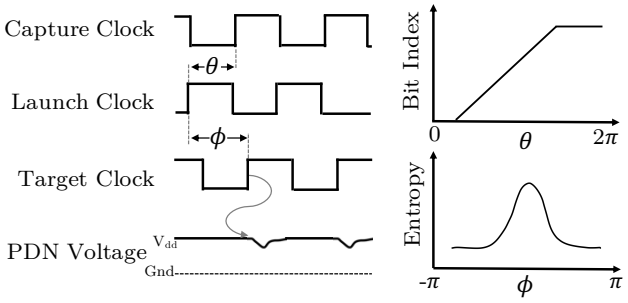

Fig. 1. The effect of tuning θ and ϕ on the output of our Time-To-Digital Converter. θ is the known phase relationship between the Launch and Capture clock and affects the location of the transition bit index within the sensor. ϕ is the unknown phase relationship between the Launch clock and the Target clock. As $\phi \to 0$ the variations caused by the positive edge of the Target clock will be measured by the TDC sensor and maximize the channel capacity as measured by entropy.

II. Dual-Edge Time-to-Digital Converter

Time-to-Digital Converters (TDC) measure the propagation delay of a signal through an array of logic elements with semi-uniform delay. The propagation speed of the delay elements is a function of the PDN voltage. We present the design of a Tunable Dual-Edged Time-to-Digital Converter (TDC) which has the following key features.

1) Dual-Edge: Two types of transitions are captured by the Tunable Dual-Edged TDC: a rising ($0 \to 1$) and a falling ($1 \to 0$) pulse edge. Our experiments show that rising and falling edges contain unique information. We also find that the falling edge more linear propagates within the sensor's logic elements, making it the better choice for side-channel recovery.

2) Sample Window Tuning (θ): The Tunable Dual-Edged TDC is able to dynamically change θ – the time between the launch of a transition and its subsequent capture. θ corresponds to the length of the sample window, which exposes a fundamental tradeoff between capturing the entirety of PDN variations and potentially sampling additional irrelevant PDN behaviors. Second, θ can position the transition's location within the delay line as in Figure 1.

3) Target Computation Tuning (ϕ): Our Tunable Dual-Edged TDC has the ability to dynamically reconfigure the position of its rising and falling transitions with respect to a co-tenant's applications as in Figure 1. Due to the synchronous nature of target computations, positions of zero information recovery exist where the sensor sampling frequency is out of phase of the target. We find that the ability to reconfigure this value has significant impact on the side-channel information recovery of the sensor.

III. Conclusion

As a measure of the effectiveness of optimizing ϕ on information recovery, we examine the ability to extract the type of co-tenant computation from sensor trace output. A set of sensor power-traces are gathered for each of seven applications: AES and PRESENT cipher running on Orca and MicroBlaze soft-processor, an absence of computation, combinatorial loop power-wasters, and HLS AES. A set of power-traces is gathered at an optimized position of ϕ (as measured by maximum variance in sensor output), and a random position of ϕ (to determine performance without our optimization strategies). We find that the ability to classify a power-trace into one of the seven computations is significantly improved within the optimized ϕ data set.