A Bus Authentication and Anti-Probing Architecture Extending Hardware Trusted Computing Base Off CPU Chips and Beyond

Zhenyu Xu, Thomas Mauldin, Zheyi Yao, Shuyi Pei, Tao Wei, and Qing Yang
Department of Electrical, Computer and Biomedical Engineering
University of Rhode Island
Kingston, Rhode Island, USA 02881
{zhenyu_xu, thomas_mauldin, zheyi_yao, shuyi_pei, tao_wei, qyang}@uri.edu

***Abstract*—Tamper-proof hardware designs present a great challenge to computer architects. Most existing research limits hardware trusted computing base (TCB) to a CPU chip and anything off the CPU chip is vulnerable to probing and tampering. This paper introduces a new hardware design that provides strong defenses against physical attacks on interconnecting buses between chips in a computer system thereby extending the hardware TCB beyond CPU chips. The new approach is referred to as DIVOT: Detecting Impedance Variations Of Transmission-lines (Tx-lines). Every Tx-line in a computer system, such as a bus and interconnection wire has a unique, intrinsic, and fingerprint-like property: Impedance Inhomogeneity Pattern (IIP), i.e. the impedance distribution over distance. Such unpredictable, uncontrollable, and non-reproducible IIP fingerprints can be used to authenticate a Tx-line to ensure the confidentiality and integrity of data being transmitted. In addition, physical probes perturb the electromagnetic (EM) field around a Tx-line, leading to an altered IIP. As a result, runtime monitoring of IIPs can also be used to actively detect physical probing, snooping, and wire-tapping on buses. While the physics behind the IIP is known, the major technical breakthrough of DIVOT is the new integrated time domain reflectometer, iTDR, that is capable of carrying out in-situ and runtime monitoring of a Tx-line without interfering with normal data transfers. The iTDR is based on two innovations: analog-to-probability conversion (APC) and probability density modulation (PDM). The iTDR performs runtime IIP measurements non-invasively and is CMOS-compatible allowing it to be integrated with any interface logic connected to a bus. DIVOT is a generic, scalable, cost-effective, and low-overhead security solution for any computer system from servers to embedded computers in smart mobile devices and IoTs. To demonstrate the proposed architecture, a working prototype of DIVOT has been built on an FPGA as a proof of concept. Experimental results clearly showed the feasibility and performance of DIVOT for both hardware authentication and tamperproof applications. More specifically, the probability of correctly identifying a bus is close to 1 with an equal error rate (EER) of less than 0.06% at room temperature. We present an example design that incorporates DIVOT into an off-chip memory bus to protect against physical attacks including probing/snooping, tampering, and cold boot attacks.**

***Index Terms*—Secure Computer Architecture, Authentication, PUF, Physical Attacks, Probing, Tampering**

I. Introduction

Security in computer design is of paramount importance in today's digital era when financial, health-care, governmental, and all other business applications rely on computers. No matter whether it is a high-performance server or an embedded computer in a smart phone, they all face great security challenges. A high-performance server at a data center providing cloud services may be vulnerable to physical attacks, such as probing the memory bus [31], [71] or a cold boot attack [26], [76], by powerful adversaries who happen to be malicious insiders [12], [56]. This has been the major factor limiting the wide adoption of cloud computing services. Physical attacks on mobile computing devices and IoTs are even easier than servers because adversaries can easily gain physical access to private and secure information stored in edge devices' memory and storage [38], [49], [53]. Therefore, designing a secure computer architecture is a fundamental requirement for correct execution, probably more so than high performance, because "no amount of performance gains can compensate for incorrect execution" [27] or loss of data confidentiality and integrity.

Because of its importance, there has been extensive research reported in the literature on secure computing architectures [3], [15], [18], [36], [39], [42], [50], [63], [64], [70], [72], [73]. While these secure architectures provide adequate solutions to software attacks such as malicious OS [4], out-of-order execution [34], [37], cache timing side channels [22], [33], [68], and so forth, they have limitations on protecting physical attacks such as probing and tampering on memory buses and memory modules. Memory encryption [7], [28], [72] and Oblivious RAM (ORAM) [23], [60], [67] protect data stored in off-chip DRAM from physical attacks. These approaches generally incur substantial performance overheads that can be reduced to some extent by many interesting techniques [1], [55], [72], [77]. However, any encryption requires a secure key that itself is subject to attacks [43], [65]. As new techniques are being proposed, designs for security get better but so do adversary's skills. Although extensively studied, no provably tamper-proof system exists. The IBM 4765 Secure Coprocessor [5], [59] shields an entire computer in a tamper-resistant enclosure that includes hardware that deters attacks, such as a Faraday cage and an array of sensors. Although having good security properties against physical attacks, it is prohibitively expensive.

This paper introduces a completely new hardware approach to protecting against physical attacks on external memory buses and memory modules. It is based on two-way physical authentication of a memory bus interconnecting a CPU and a memory module (DRAM or NVRAM). The authentication is done by examining the fingerprint of the bus concurrently with data transfers. The fingerprint is the unique, intrinsic, unpredictable, uncontrollable, and non-reproducible physical property of the bus: Impedance Inhomogeneity Pattern (IIP), i.e. the impedance distribution over distance. Electromagnetic (EM) principles teach that any Tx-line has a fundamental property called characteristic impedance that is determined by the geometry and materials of the Tx-line. The non-uniformity of both material and geometry of a Tx-line makes impedance change with distance, providing a unique IIP qualified as a physical unclonable function [29], [32], [62], [69], [75]. What makes it possible to have high-speed and concurrent authentication of buses is our new design of an integrated time domain reflectometer, iTDR for short, that is capable of carrying out in-situ and runtime monitoring of an IIP without interfering with normal data transfers. As a signal (address, data, control, or clock) propagates along a Tx-line, the non-uniform impedance causes small back-reflections, governed by the EM principles. The backward propagating wave contains all the information of the IIP that is collected by our iTDR. By incorporating the iTDR circuit at the interface logic of a chip connected to a bus, the concurrent two-way authentication is possible while data transfer is in progress.

In addition to authentication, the iTDR can also instantly detect Trojan chip, wire-tapping, and hardware probing. Hardware tampering physically causes a change in the IIP because methods such as inserting Trojan chips, soldering wires, and probing the EM fields all disturb the original IIP. By monitoring IIPs, hardware attacks can be detected using the same iTDR circuit. Once such hardware attacks are detected, a system warning is generated to trigger appropriate actions. Since both authentication and probe warnings are done by **D**etecting **I**mpedance **V**ariations **O**f **T**x-lines using the iTDR, we referred to our new architecture as DIVOT. Interestingly enough, any unauthorized data access or hardware tampering will create a signal dent, similar to a divot, observable by the iTDR as evidenced later in the paper.

For DIVOT to be a practical and scalable technology, low overhead in terms of footprint, logic resources, power consumption, and latency is required. To meet this critical requirement, we propose two new concepts: analog-to-probability conversion (APC) and probability density modulation (PDM). The APC together with the PDM scheme, which can be simply built around a 1-bit comparator (i.e. digital input), successfully avoids using a conventional high-resolution analog-to-digital converter (ADC). Meanwhile, equivalent time sampling (ETS) is used to remove the need for a high real-time sampling rate, which significantly simplifies hardware design and minimizes overhead without compromising the performance in comparison with a high-end TDR. The iTDR performs runtime IIP measurements non-invasively, and is CMOS-compatible allowing it to be integrated with any interface logic connected to a bus. It is interesting to note that the way DIVOT works is surprisingly similar to traditional Error Correcting Code (ECC) in memory designs. ECC detects and corrects bits errors in memory using redundant bits with encoder and decoder circuits that work in parallel with normal data accesses. DIVOT uses redundant circuits, iTDRs, for security purpose, which also works in parallel with normal data accesses. We expect the significance of DIVOT in future computer designs to be in par with ECC, if not more. We believe that DIVOT represents a paradigm shift in hardware security designs.

In order to demonstrate the feasibility of the DIVOT architecture, a working prototype has been built on a 6-layer custom PCB and an FPGA evaluation board, where the digital interfaces and logic resources are provided by a Xilinx ZYNQ Ultrascale+ FPGA chip. The prototyped DIVOT contains a single lane communication link, emulating a bus, as well as the proposed iTDR. The clock speed was set to $156.25MHz$ only for the sake of timing stability. Extensive experiments have been carried out for both authentication and tramper detection. Experiments showed that both authentication and tamper detection can be completed within $50\mu s$. With GHz clock speed in modern computers, DIVOT is able to alert any unauthorized data access or physical tampering within memory operation time frame. An equal error rate (EER) of less than 0.06% was achieved at room temperature. That is, the probability of correctly identifying a Tx-Line is close to 1 with a false positive rate of less than 0.06%. When the ambient temperature swung from 23^oC to 75^oC, the false positive rate increased to 0.14%. Tests also showed other environmental factors such as vibration and acoustic waves can increase the EER up to 0.27%. However,we believe the EER can be substantially reduced if we monitor multiple wires as opposed to just one as done in this experiment. Our prototype design consumes only 71 registers and 124 LUTs, indicating low hardware overhead. Most of these logic resources can be shared by different iTDRs, protecting multiple buses in a parallel fashion. This further reduces the overhead per iTDR, making DIVOT easily scalable to large and complex systems. Therefore, DIVOT holds the potential to be incorporated into any I/O interface logic with very little additional hardware cost.

This paper makes the following contributions:

1) We present a completely new way of protecting against physical attacks in computer systems. For the purpose of authentication and tamper prevention, we developed a hardware design that detects impedance variations of Tx-lines (DIVOT). A simple CMOS logic can be integrated into an interface of any chip connected to a bus to form a much larger hardware TCB than traditionally possible.
2) Two new concepts have been proposed, analog-to-probability conversion (APC) and probability density modulation (PDM). An equivalent time sampling (ETS) scheme provides IIP measurements with sub-millimeter level spatial resolution. Together, these new concepts make our new iTDR design capable of concurrent au-

thentication/tamper detection with normal data transfers. Meanwhile, the new concepts enable the new iTDR to meet the low-overhead and high-performance requirements.

3) While DIVOT holds the promise to work on any communication link, we present an example memory bus design that connects a CPU chip and an off-chip SDRAM module. The new design provides runtime two-way authentication and tamper prevention.
4) A working DIVOT prototype has been built on a custom PCB and a commercial FPGA evaluation board to demonstrate the feasibility and performance of DIVOT. Extensive experiments have been carried out, and experimental results have successfully showed that the DIVOT functions as promised.

The paper is organized as follows. The next section gives DIVOT's working principles. Section III presents an example design of a CPU connecting an off-chip SDRAM through a memory bus. A prototype design, implementation, and experimental evaluation will be presented in Section IV. Section V discusses existing works closely related to our work. We conclude our paper in Section VI.

II. DIVOT Architecture

The major challenge of the DIVOT architecture is to extract the IIP on a Tx-line while data transfer is in progress. Such IIPs are represented by back-reflection waveforms that are generally very weak and mixed with noises. In this section, we present the iTDR design that is both low latency and low overhead in terms of footprint, logic resources, and power consumption. Its high performance is achieved through several technical innovations as described below.

A. iTDR overview

Fig. 1 illustrates how a typical TDR (time domain reflectometer) machine works. A probe signal is launched by a transmitter (Tx), and propagates down the line. Any impedance discontinuity on the Tx-line produces a back-reflection, which can be collected by a detector (Det) through a coupler (CPL). A reflection can be considered as a scaled and phase shifted version of the probe signal. Therefore, as shown in Fig. 1, the total voltage received at the Det is a linear combination of many reflections, contributed by discontinuities along the Tx-line. Consequently, each Tx-line system can be abstracted as a linear time-invariant (LTI) system whose impulse response or transfer function, is determined by its IIP [17]. Theoretically, by sending an ideal impulse signal into a Tx-line, one can resolve the transfer function and the IIP of the Tx-line. This concept is widely used in industry to characterize high-speed electronic components. Conventional TDR machines provide high spatial and voltage resolution, by means of high-end ADCs. Such high-end ADCs are very bulky, and infeasible for our DIVOT architecture.

Our objective here is to design a CMOS-compatible, high performance, and low overhead iTDR that can be integrated into any bus interface logic. To accomplish this objective,

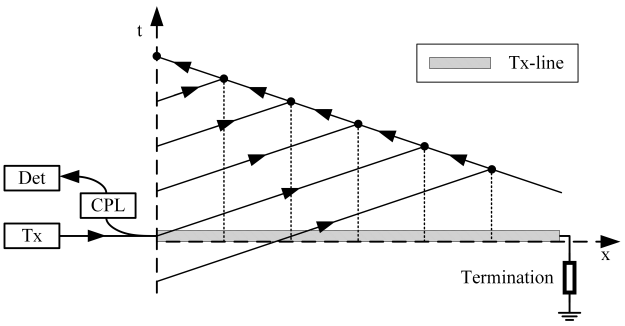


Fig. 1. Schematic of a generic TDR.

several new concepts and techniques are introduced as detailed in the following subsections.

B. Analog-to-probability converter

The IIP is a result of non-uniformity of a Tx-line, and it is typically small. In fact, the collected reflection signal is so weak that SNR (signal to noise ratio) is possibly smaller than 1, meaning that the signal is below noise floor. However, in order to measure the IIP with sufficient accuracy, both high voltage resolution and high SNR are required. An ideal ADC with infinitely high resolution cannot perform the measurement even not considering its complexity and bulky footprint. Therefore, we propose a new technique in place of ADC: analog-to-probability conversion (APC). Instead of using a conventional ADC, a comparator and a counter are utilized to perform IIP measurements with high voltage resolution and equivalently high SNR.

A comparator has a non-inverted/positive input and an inverted/negative input, also referred to as the reference input. The output is a Boolean variable, Y, that shows to be 1 if the voltage on the positive input V_{sig} is higher than the incident on the reference input, V_{ref}. Assuming an ideal constant V_{ref} and a constant input V_{sig}, the output Y is always a constant (0 or 1). However, in reality, electronics are noisy, making Y a random variable rather than a constant. The probability of $Y = 1$ is expressed in Eq. (1):

$$p\{Y = 1\} = p\{V_{sig} - V_{ref} > V_{noise}\}, \tag{1}$$

where V_{noise} represents the total amount of noises that propagate and contribute to the comparator's reference input. In electronics, thermal noise dominates at higher frequencies, thus, V_{noise} presented on the comparator's reference input follows a Gaussian distribution. Fig. 2 plots the Gaussian noise distribution around $V_{ref} = 0$. Essentially, this distribution is a probability density function (PDF). The corresponding cumulative distribution function (CDF) is also plotted in Fig. 2. This clearly shows that a 1-to-1 relation between analog voltage V_{sig} and probability $p\{Y = 1\}$ exists, making APC possible. We can write:

$$V_{sig} = V_{ref} + CDF^{-1}(p\{Y = 1\}), \tag{2}$$

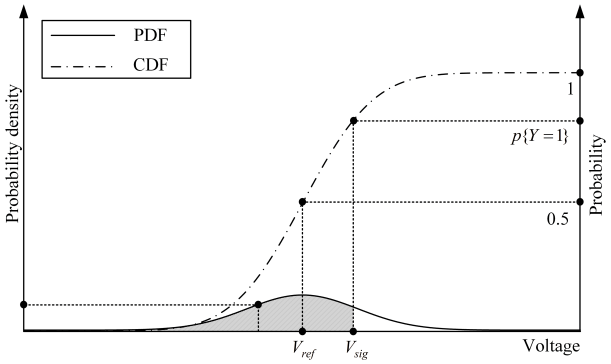


Fig. 2. White Gaussian noise distribution in typical electronic systems.

where $CDF^{-1}()$ is the inverse CDF. In an iTDR, the back-reflection signal is fed to the comparator's positive input. Let the input voltage waveform be $V_{sig}(t)$, which in essence is the IIP of a Tx-line. Let the corresponding probability of $Y = 1$ as a function of time over this waveform be $P\{Y = 1\}(t)$. By repeatedly probing the Tx-line over a large number of times, $P\{Y = 1\}(t)$ over the waveform is measured. $V_{sig}(t)$ can be calculated using Eq. (2), and the IIP of this Tx-line is obtained.

Fig. 2 also infers that the APC's sensitivity, defined as

$$\frac{\mathrm{d}}{\mathrm{d}V_{sig}} p\{Y = 1\}, \tag{3}$$

is determined by the slope of the CDF, which is nothing but the PDF. According to the probability theory, for a Gaussian variable, the PDF within 2 standard deviations (2σ) range is high, indicating that a high APC sensitivity can be achieved within this region. Also, in this region, its linearity holds significantly better than other regions. Therefore, APC is most effective within 2σ, implying that our iTDR should use this range. Considering that the variance of Gaussian noise is also the energy of the noise, APC works well with high sensitivity in a linear region when signal-to-noise ratio (SNR) is equal to or smaller than 1. In other words, the energy of V_{sig} should not exceed σ^2 to achieve a linear mapping between probability and voltage. This leads to a dynamic range of 2σ. In order to increase the measurement dynamic range, we propose probability density modulation (PDM) that will be articulated in the following subsection.

The fundamental difference between the APC and other oversampling-based and/or dithering-based super-resolution ADCs, such as sigma-delta ADC [8], is that APC compares the instant input voltage with a varying reference voltage at each trigger repetitively, avoiding the very high sampling rate required by real-time super-resolution ADC. Therefore, APC doesn't require any sample and hold circuit, which minimizes the input capacitance and maintaining a high input bandwidth. It is worth noting that comparators, used as digital inputs, have much larger analog bandwidth than typical super-resolution ADCs, making APC supreme for today's high-speed buses.

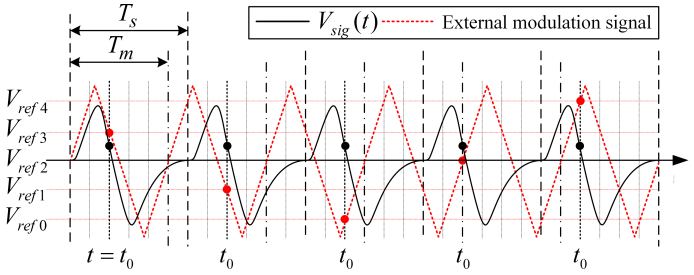


Fig. 3. Illustration of PDM scheme.

C. Probability density modulation (PDM)

Although APC method is theoretically effective, there remains practical challenges for APC to be used for DIVOT. The intensity of intrinsic noise of an IC is typically unpredictable, and it varies from chip to chip. When the SNR is larger than 1, the APC falls into the non-linear region. To solve this problem, an external modulation signal is connected to the reference input to rebuild the PDF in a controlled fashion. This approach, namely probability density modulation (PDM), successfully resolves the remaining issues, making APC a practically valid and versatile technique for our iTDR.

In a PDM scheme, the external modulation signal and intrinsic noise work together for APC to provide high-quality IIP measurements. Although the external modulation signal in a PDM scheme can use many different waveforms, and they can be generated by a wide variety of circuits, we showcase the PDM scheme using a simple triangle wave. A quasi-triangle waveform can be easily achieved using a digital output circuit and a simple resistor-capacitor (RC) charge-discharge circuit. The frequency of the triangle wave f_m, determined by the frequency of the digital output, and the frequency of the data/sampling clock f_s must satisfy certain requirements to work properly. If $f_m = f_s$, the reflection signal will be compared with same voltage in all measurements, completely removing the effectiveness of an external modulation signal. In order to compare a reflection signal with different reference voltages, f_m and f_s must be relatively prime, which provides Vernier time delay between the reflection signal and modulation signal. Fig. 3 demonstrates this concept, assuming $5f_m = 6f_s$. The reflection waveform is repeated for 5 times. At a fixed time point $(t = t_0)$ with respect to the starting point of a period, five discrete reference voltages (V_{ref0} to V_{ref4}) are created over 5 waveform periods. Vernier oscillator theory has also been employed in time-to-digital converters (TDC) in prior arts to achieve high temporal resolution [35].

Fig. 4 plots the associated PDF and CDF of this example. Five reference voltages are introduced by the triangle wave. Each reference voltage appears evenly over time with a probability of 0.2. Therefore, the equivalent PDF is the normalized superposition of each PDF associated with each reference voltage level. The working mechanism is shown in Fig. 4. It clearly shows that the proposed PDM scheme effectively increases the linear region, leading to a much-

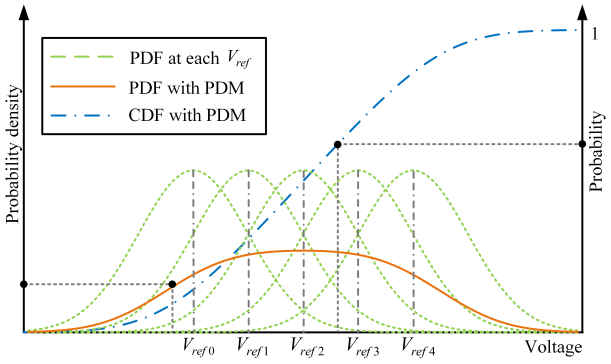


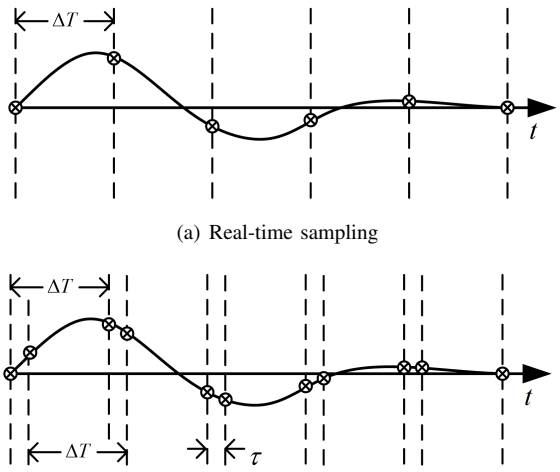
Fig. 4. PDF and CDF with multiple reference voltages.

widened measurement dynamic range in comparison with a single V_{ref}. Thus, by introducing an external modulation signal into APC, one can modify and better balance the CDF in terms of sensitivity, linearity, and dynamic range as necessary. It is worth noting that the external modulation signal in a PDM scheme can be shared with all iTDRs inside a chip, significantly lowering overhead per iTDR.

D. Equivalent time sampling

In a TDR system, high sampling rate is critical, since it determines the spatial resolution, or the smallest resolvable distance in an IIP. However, although possible, real-time sampling at extremely high sampling rate ($> 10GSa/sec$) requires a very complex hardware design. The proven LTI property of this system indicates that the response for a given input produces the same output, regardless of measurement time. Generally, digital signals have several states, represented by different voltage levels. For example, an NRZ communication protocol has two voltage levels representing a 1-bit value at a time; a PAM4 protocol has four voltage levels, representing a 2-bit value at a time. Fundamentally, any data waveform on a Tx-line is formed by switching between different voltage levels, thus, producing rising and falling edges correspondingly. Considering that the interface circuits inside a digital chip is fixed, voltage switching remains consistent over time, i.e. the shapes of rising and falling edges are highly repeatable. Consequently, the back-reflections caused by these rising and falling edges are also consistent, allowing the use of equivalent time sampling (ETS) in our DIVOT architecture.

The DIVOT architecture utilizes the rising or falling edges of data waveforms as the probe signal. ETS has been used to equivalently boost the sampling rate in high resolution TDRs [47]. In this paper, ETS is achieved by changing the phase relationship between the data transmission clock and the iTDR's sampling clock. This is achieved via a phase lock loop (PLL) with phase stepping function, where the output clock's phase can be stepped with respect to the input clock as requested. Fig. 5 compares real-time sampling and ETS. Fig. 5(a) shows that a typical real-time sampling scheme performs measurements at discrete time points with a time interval of ΔT, corresponding to a sampling rate of $1/\Delta T$. Assuming



(a) Real-time sampling

(b) ETS enabled by phase stepping function

Fig. 5. Illustration of ETS.

that total number of points in this measurement is N, the total length of the measurement is $N\Delta T$. In our system, the iTDR steps the phase of the sampling clock by a small increment, τ, with respect to the transmission data clock after each measurement. Thus, after repeating the process over M times, where $M\tau = \Delta T$, shown in Fig. 5(b), a total of $M \times N$ sampling points are achieved over the same data length $N\Delta T$. Thus, without increasing the real-time sampling rate $1/\Delta T$, the iTDR provides an equivalent sampling rate of $M/\Delta T$ or $1/\tau$. In this case, the sampling rate is determined by the smallest phase shift interval ($1/\tau$) rather than the period of the ADC's sampling clock (ΔT).

The PLL in Xilinx Ultrascale+ series FPGA provides a dynamic phase shift of $11.16ps$, corresponding to an equivalent sampling rate greater than $80GHz$. The propagation velocity of an EM wave on PCB Tx-line is about $15cm/ns$. Therefore, the spatial resolution is about $0.837mm$, which is sufficient for the proposed applications.

Usually, all bus interfaces in a computer chip share the same data transmission clock. Thus, one PLL with phase stepping function is sufficient to drive all iTDRs corresponding to different buses, regardless of the number of ports under protection.

E. Runtime measurement support

When the system is running, the data launched into a Tx-line is random. In this case, the probe signals do not happen at a fixed time point. In particular, most high-speed interfaces apply channel encoding to ensure that different symbols occur evenly. Therefore, in a serial communication channel, the number of rising edges approximately equals the number of falling edges and the waveforms of rising and falling edges are highly symmetric. As a result, the reflections of the rising and falling edges cancel each other, making DIVOT unusable. This problem can be addressed by generating a sampling trigger signal from the data buffer, such as a FIFO. For example, in a binary communication protocol, once a value 1 preceding

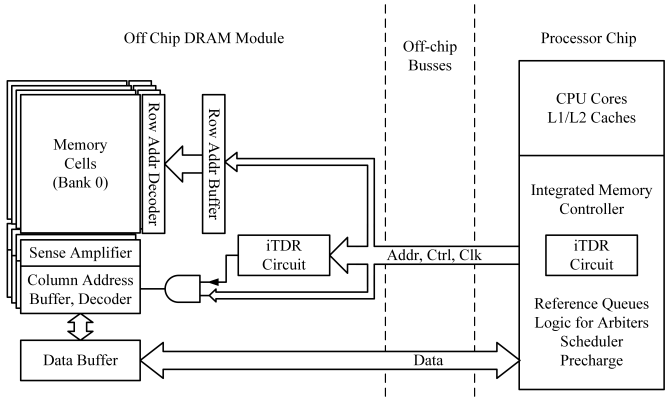


Fig. 6. An example design of incorporating our DIVOT architecture on a memory bus.

a value 0 is ready to be launched into the Tx-line, the iTDR generates a sampling trigger and passes it to the APC to take measurements. Fortunately, the sampling trigger signal is not needed for the clock lane, since the clock waveform is highly consistent and predictable.

III. Memory Bus Protection

Fig. 6 shows an example design of incorporating our DIVOT architecture into a CPU chip and an off-chip SDRAM module. On the processor side, our iTDR circuit is added to the integrated memory controller on the CPU chip, such as a DDR controller, as an integral part of DRAM control logic working together with reference queue, arbiter, scheduler, refresh, and precharge logic [51]. It is directly connected to the external memory bus to receive and collect reflection waveforms while the CPU is accessing SDRAM. Specifically, we use the clock lane on the bus as the Tx-line for collecting IIPs. The iTDR works on all rising edges of the clock that happens highly regularly. The major function of iTDR is continuously monitoring bus activities to (1) authenticate the SDRAM module (e.g. DIMM cards) and the memory bus that are indeed the hardware that CPU recognizes and (2) detect possible bus snooping or probing by any foreign hardware.

On the SDRAM module side, the same iTDR circuit is incorporated into the control logic of the memory module sitting aside the normal address decoding, sense amplifier, and buffering logic [20]. It starts sensing impedance signals on the bus as soon as the system is powered up. Since the clock starts as soon as the system is on irrespective of whether there is a memory operation or not, our iTDR started working to collect reflection waveforms on the clock lane. The output values of the iTDR are stored in a FIFO buffer. When a memory operation starts, the iTDR continues collecting IIPs and updates the previously stored IIP values in the FIFO buffer during precharge cycles (if a new row is accessed), activation cycles, and the row access cycles. The newly collected IIP fingerprint is compared with the stored fingerprint (in a ROM as explained shortly) for authentication purpose to make sure the memory access request is indeed coming from the CPU and the memory bus that was initialized. At the column access time, the column address is gated by the authentication result so that only the authorized CPU chip and memory bus can access, read or write, the SDRAM. Tamper detection and blocking are also done at the same time.

The operation of the new computer systems equipped with the new DIVOT involves three major steps: calibration, monitoring, and reaction to counter attacks.

Calibration process initializes the pairing of communicating chips connected to a bus such as a CPU chip and memory modules that the CPU accesses. This step is done at the manufacturing time or user installation time. During the calibration process, the iTDR on the processor chip will establish the fingerprint (IIP) of the memory bus connected to the memory module that the processor will access. The fingerprint is the IIP of the bus, which is obtained by collecting and calculating back reflections using the iTDR. At the same time, the iTDR on the memory side will also collect the fingerprint of the bus connected to the processor. The fingerprint covers the entire Tx-line from the output of the iTDR on the CPU chip until the input of the iTDR on the memory side. After the fingerprint is collected, both the CPU and the memory module store the fingerprint in their respective EPROM. Note that the security of these ROMs storing the fingerprint is not critical to this architecture because even if attackers gained access to the IIP, they would not be able to use it once an IIP leaves the exact Tx-line.

Monitoring starts once the system is in operation. Both iTDR circuits keep receiving and collecting reflection signals to derive a fingerprint (IIP) of the transmission bus and compare it with the stored fingerprint in the ROM. If the newly collected fingerprint matches the one stored in the ROM, authentication is successful and normal computation proceeds. From the processors point of view, it wants to make sure that the memory module that it intends to read data from, or write data to, is indeed the memory module it recognizes. In this way, correctness, integrity, and confidentiality of the data are maintained. Detecting hardware probing and snooping is carried out at the same time. From the memory modules perspective, it compares the newly collected fingerprint with the one stored in its ROM in real time to ensure all data accesses, read or write, are indeed from the authorized processor chip. Any unauthorized attempt will be instantly blocked. This can effectively protect memory data from physical attacks, such as cold boot attacks [26], [76], because any unauthorized data requests will be rejected no matter whether an attacker swaps the memory module to another computer or uses another Tx-line other than the bus connected to the authorized processor chip.

Reaction to counter attacks kicks in as soon as an abnormal IIP signal is detected whether it is an unauthorized communicating device, such as a different Tx-line or hardware module, or a physical tampering attempt. When the CPU finds a non-matching fingerprint, it indicates that the memory module might have been swapped. In this case, the CPU will respond by stopping the normal memory operation until

the newly collected fingerprint matches the one stored in the ROM again. In this way, it avoids reading incorrect, or replay, data and writing sensitive information to a wrong device. If abnormal IIPs were detected, indicating a possible bus tampering attempt, the CPU would perform necessary actions to protect sensitive information from leaking. Existing protection techniques can be applied here [5], [59]. On the memory side, the reaction is simply blocking or disabling data operations in the memory once abnormal signals are detected. We omit the hardware and software designs for reactions after authentication fails or tamper attempts are detected. We leave this as our future work.

IV. Experimental Evaluation

A. Prototype

In order to demonstrate the feasibility of the DIVOT architecture, we designed and implemented a working prototype. The prototype is built on a 6-layer custom PCB and a Xilinx ZYNQ Ultrascale+ series FPGA evaluation board (ZCU104). The custom PCB contains a comparator, a coupler, and a terminated Tx-line, while FPGA board contains all of the logic components necessary to build a single-lane bus equipped with the DIVOT architecture. The custom PCB and evaluation board are connected via FPGA Mezzanine Card (FMC). The simplified schematic is shown in Fig. 9(a). The data launched into the Tx-line from the FPGA is completely random to demonstrate the feasibility of runtime IIP monitoring on data buses. Six $25cm$ PCB Tx-lines are used as devices under test to carry out the experiments. Considering the hardware limit, the data rate and APC clock rate are set to $156.25MHz$ for stability and simplicity. According to Xilinx Vivado Utilization Report, hardware resources used by the DIVOT circuit include 71 registers and 124 LUTs (approximately 0.8% of available resources on xczu7ev-ffvc1156-2-e), where 80% are used to generate counters.

B. Similarity and Error functions

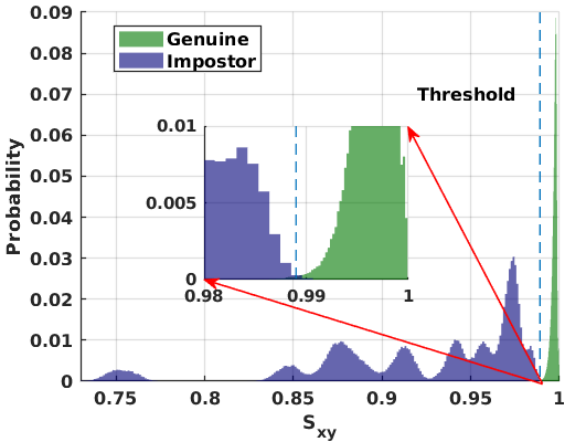
Similarity (S_{xy}) is defined as the inner product between two IIP waveforms:

$$S_{xy} = \sum_{n=0}^{N-1} x(n)y(n), \tag{4}$$

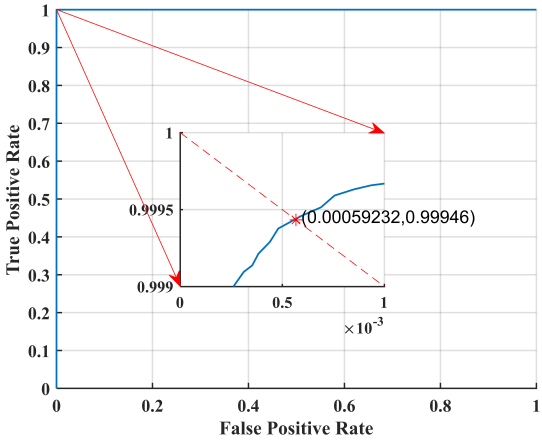
where x and y are two different IIP waveforms, and n is the index in time/distance domain. Time and distance are linearly related by the propagation velocity divided by 2, where 2 accounts for round trip. S_{xy} is normalized to have a value ranging from 0 to 1. Similarity can be readily used for authentication. For runtime tamper detection applications, the IIP error function (E_{xy}) is defined to quantify the difference between the normal IIP $x(n)$ and tamper waveform $y(n)$. The error function, $E_{xy}(n)$, is given by:

$$E_{xy}(n) = [x(n) - y(n)]^2 \tag{5}$$

A large error at a certain index, n_0, indicates that a tamper attack is present at the corresponding location.



(a) Measured distribution of normalized S_{xy} of same Tx-lines (Genuine) and different Tx-lines (Impostor). The magnified figure shows the clear separation of the two results.



(b) Measured receiver operating characteristics (ROC) of iTDR. The magnified box shows that false positive rates is below 0.0006, indicating high authentication accuracy.

Fig. 7. Measured IIP results over six Tx-lines using the DIVOT prototype. (a) results of similarity function; (b) results of receiver operating characteristics. All results were obtained over 8,192 measurements.

C. Authentication

Our first experiment is to demonstrate that the IIPs, measured by the iTDR, from the same Tx-line (Genuine) remain the same over time and the IIPs from different Tx-lines (Impostor) differ greatly. For this purpose, we measured six Tx-lines on the customized PCB for 8192 times, giving rise to six groups of IIP data. Normalized similarity is calculated within each group and between different groups. Genuine and impostor distributions are plotted in Fig. 7(a), and the corresponding receiver operating characteristic curve (ROC) is shown in Fig. 7(b).

As shown in Fig. 7(a), the distribution of a genuine IIP is clearly separated from that of an impostor IIP. If a proper threshold value is chosen, we can clearly differentiate two Tx-lines. In other words, our iTDR can effectively authenticate a Tx-line. As shown in Fig. 7(b), among the six Tx-lines

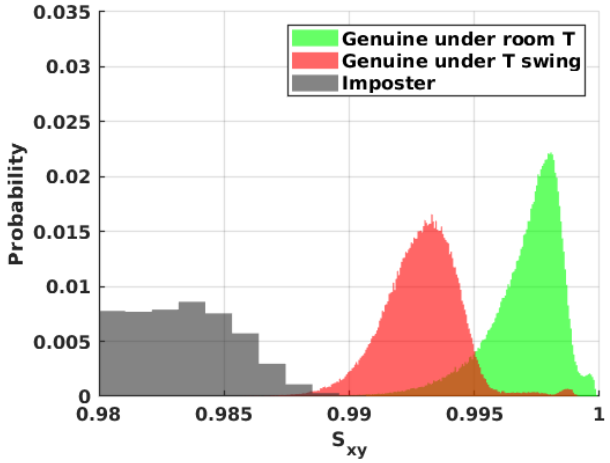


Fig. 8. Measured distribution of normalized S_{xy} with a temperature (T) swing from 23^oC to 75^oC.

measured over 8192 times, an EER of less than 0.06% was observed in this experiment. During authentication process, we can set a threshold value to correctly identify a Tx-line with certainty. For example, if the newly measured IIP is equal to the IIP value stored in the ROM within $\pm 0.1\%$, then it is authenticated. Otherwise, authentication fails.

It is known that an increased temperature leads to an increased dielectric constant (Dk), or permittivity, in todays PCB laminates [30]. An escalated Dk leads to a rise in line capacitance associated with a high-speed bus resulting in a decreased local impedance. However, due to the fact that the impedance at any point along a bus changes in the same fashion as ambient temperature varies, the impedance contrast (IIP) is not expected to change significantly. To evaluate the temperature influence, we conducted the tests in an electric oven and swung the temperature from 23^oC to 75^oC. The genuine distribution moved towards left, while the impostor distribution didn't change noticeably. This resulted in an increased EER of 0.14%. The comparison between genuine distribution at room temperature and genuine distribution at a swinging temperature is shown in Fig. 8.

Vibration and acoustic waves may reduce the performance of bus authentication by affecting its IIP given that they compress or stretch a bus. To evaluate the system under such conditions, a piezo-electric driver was attached to the board and a continuously chirped knocking frequency, ranging from 1 Hz to 50 Hz, was applied. Under this condition, the EER increased to 0.27%. Although DIVOT can still be used for Tx-line authentication with higher threshold values, further reducing the EER under this condition remains an open question for future research. Theoretical analysis suggests that monitoring multiple wires on a bus can exponentially increase authentication accuracy. Further investigations are needed to prove this initial analysis and assess its performance and cost trade-offs.

Cross-talk or EM radiation from chips in close proximity to a bus may couple into the proposed DIVOT receiver and contribute to noise. However, since the IIP measurement is synchronized with waveforms flowing on the bus, the DIVOT receiver effectively removes the asynchronized EMI noises. Thus, we do not expect a significant performance reduction. To test this hypothesis, a high-speed digital circuit was put close to a bus, and the evaluation test showed that the EER stayed at 0.06%.

D. Countermeasure for Trojan and cold boot attack

This experiment is to show how Trojan and cold boot attacks can be detected using DIVOT. Load modification happens when an adversary replaces an original chip with Trojan chips, or tries to carry out a cold boot attack. Whenever such an attack happens, the interface of the chip at the end of a bus on a PCB shows in an abrupt impedance change, leading to a large reflection peak at the load. No matter if it is modifying or replacing the load, a change of IIP at the termination occurs resulting in a large reflection peak, which can be easily detected by our iTDR.

We carried out our experiment by replacing the receiver chip with a different chip (same model number), and checked the IIP waveform error function, E_{xy}. The result is shown in Fig. 9(b) and 9(c). Fig. 9(b) plots IIP distribution as a function of signal propagation time over the Tx-line measured. The time range spans between $0ns$ and $3.8ns$ representing the total time for the signal to propagate over the Tx-line from one end to the other and back. The dotted line in this figure shows the IIPs measured with no attacks whereas the solid line represents the IIPs after the receiver chip is replaced. It is clearly shown in this figure that the IIP differs greatly when the chip is replaced at the other end (around time point of $3.5ns$, see the magnified box in the figure). Fig. 9(c) shows the error function, E_{xy}, over the same time range. The dotted line in this figure represents the error function of IIPs with no attack, represented by ambient noise, while the solid line represents the error function when the attack happens. As shown in Fig. 9(c), the IIP waveform changes dramatically at the termination point where the chip is replaced. A very large peak of E_{xy} was observed by the iTDR indicating that an attack is present. These results demonstrated the feasibility of using DIVOT to protect against Trojan and cold boot attacks.

E. Countermeasure for Wire-tapping

From DIVOT's perspective, wire-tapping is one of the most invasive tampers because it dramatically changes the impedance of a Tx-line. In our experiment, we scratched the solder mask of a PCB Tx-line, soldered a tapping-wire on it, and connected it to an oscilloscope to emulate a wire-tapping attack. The result is shown in Fig. 9(d)-9(f), where (d) shows a photo of wire-tapping; (e) shows the IIP waveforms before and after applying wire-tapping; and (f) shows the E_{xy} of two IIPs before and after applying wire-tapping. Similar to Fig. 9(c), E_{xy} between the IIP taken at two different time points is plotted in dotted line in Fig. 9(f). The solid line shows that the IIP change is very significant, and easy to be

detected using the proposed DIVOT architecture. Experiments also showed that wire-tapping is so invasive that even when the wire was removed, the remaining changes on IIP was still large, indicating that, in this case, the original IIP was permanently destroyed and non-reversible.

F. Countermeasure for magnetic probing/snooping

Magnetic probing is typically considered as a non-invasive side channel attack, as the magnetic probe gathers data without the need to touch the Tx-line. However, the existence of a magnetic probe in proximity with a Tx-line perturbs the magnetic field. EM theory indicates that the magnetic field associated with the PCB Tx-line, i.e. microstrip, induces Eddy currents in the magnetic probe, which in turn generates a magnetic field to oppose the original. Thus, equivalently, it introduces a mutual inductance to the PCB Tx-line, modifying the line inductance locally. Overall, theory suggests that the IIP is capable of not just detecting magnetic probing, but also locating it along a Tx-line.

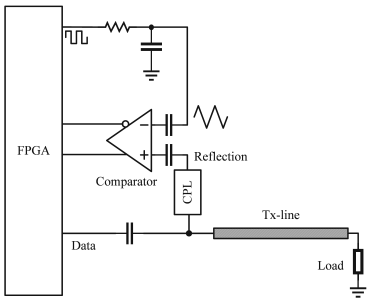
The experimental results are shown in Fig. 9(g)-9(i), where (g) shows a photo of magnetic probing; (h) shows the IIP before and after the magnetic probe was applied; and (i) shows the E_{xy} of two IIPs before and after applying magnetic probe on the Tx-line. For better comparison, E_{xy} between the intact IIP taken at two different time points, is plotted in dotted line in Fig. 9(i). Although the difference between IIPs before and after applying the magnetic probe is relatively small, the large peaks (contrast) in the error function graph clearly demonstrated DIVOT's capability of detecting magnetic probes by setting the threshold at 5×10^{-7}. Since the magnetic probing gives the smallest error increase, this threshold also works in detecting other tampers previously mentioned. Interestingly, DIVOT is also capable of revealing the location of magnetic probing along a bus.

V. Related Works

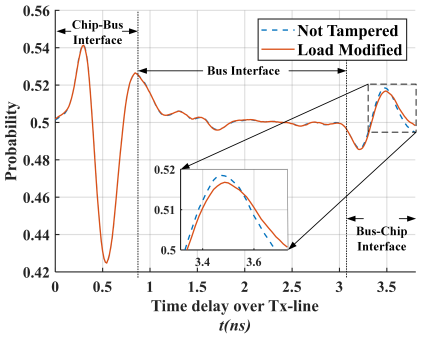
Physical attacks in the context of secure computer architectures have been extensively studied and received increasing interests recently. Unlike software attacks such as stack buffer overflows [2], [19], cross-site scripting [25], [66] and software-initiated side-channel analysis (e.g., row hammer [24], [57] and cache timing attacks [22], [33], [68]), hardware attacks require physical access to the computer or being in a nearby environment, and thus is capable of observing and manipulating target devices. Physical attacks are usually done by exploiting side-channel leakage including power [16], [44], electromagnetic radiation [48], cold boot attacks [26], [76], or intentional fault injection [9], [11], and hardware back door [74], etc.

To mitigate the known hardware attacks, significant amount of research (e.g., [3], [15], [18], [36], [39], [42], [50], [63], [64], [70], [72], [73]) seeks to provide effective isolation between applications and the underlying software (OS, hypervisor and etc.). TPM [64] is a microcontroller that can securely store the attestation key and perform software attestation, which is widely used in commodity computers today. Arm TrustZone [3] provides hardware-enforced isolation for cortex-based processors. Bastion architecture [15] uses a trusted hypervisor to provide secure containers to applications. XOM [36] also includes a trusted hypervisor but provides isolated containers that are managed by untrusted OS. Aegis [61] requires a trusted security kernel but offers stronger memory integrity guarantees than XOM. Another version of Aegis [63] leverages PUFs [29], [62] to endow a private key that are used for software attestations. Intel's SGX [42] allows users to create isolated memory regions of code and data called enclaves, that are effectively isolated from other applications or higher privileged softwares. Sanctum [18] is a secure processor that isolates cache sets and page tables associated with enclave, and microarchitectural state updated by enclave execution. Ascend [50] and Phantom [39] adopt Oblivious RAM [60] techniques in the memory controller to conceal the access pattern of memory. The above-mentioned architectures provide isolation and attestations for software at hardware level and is able to defend against some types of physical attacks depending on different threat models. However, due to the limited in-processor resources, memory encryption [7], [28], [72] and techniques such as Merkle trees [52], MACs [13] and etc. are necessary to avoid data outside of protection boundary from unauthorized accesses to ensure data confidentiality, integrity and freshness. Our solution protects against physical attacks such as bus probing, memory cell readings and snooping on Tx-lines off CPU chips, without interfering with data transfers. DIVOT provides a strong defense against physical attacks using very simple CMOS-compatible logic with little overhead in terms of performance penalty and hardware cost.

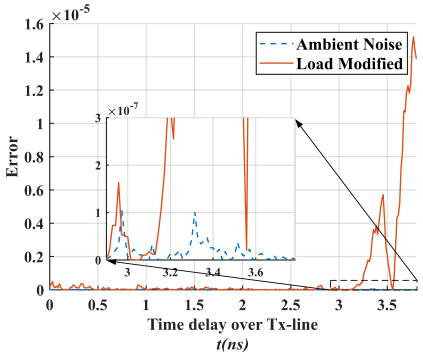
There have been existing research works on countermeasures to physical attacks reported in the literature [21], [40], [41], [45], [46], [69], [78]. Probe attempt detector (PAD) [40] proposes the use of ring oscillator circuits to capture the variation in the load capacitance induced by a probe on a victim wire. The PAD can be easily integrated in the address decoder of a bus, and it can switch between decoding mode and surveillance mode. However, the decoding and surveillance of a PAD cannot operate concurrently and hence is not suitable for noninterrupted runtime tamper detection. Paley et al. [45] present a countermeasure for physical tampering of PCBs, leveraging the resistance of PCB copper traces. However, measuring DC resistance prevents data transfer over the monitored traces because it requires the voltage over these traces remain stable during measurements. Also, it cannot work for ac-coupled high-speed buses. Furthermore, the resistance is not sensitive to the EM based probe. Park et al. [46] utilize the parasitic resistance induced by interconnection mismatch between metal layers on a chip to create a PUF, but it cannot be used to countermeasure PCB modification nor physical probing. Zhang et al. [78] show that input impedance variance between different traces can work as a PUF to protect a PCB board from being modified in the supply chain. However, this technique cannot provide runtime protection due to the necessity of using a bulky impedance analyzer; besides its low identification performance compared to RO-



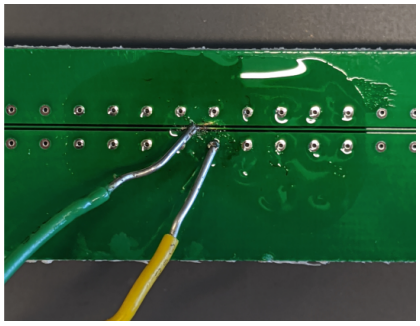
(a) Experiment setup



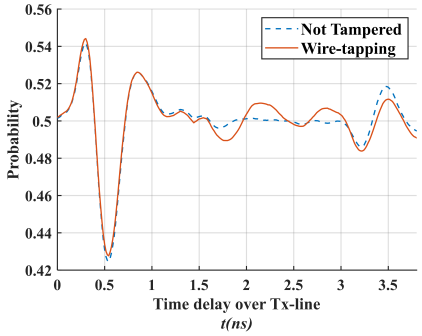
(b) Comparison of IIPs with and without load modification



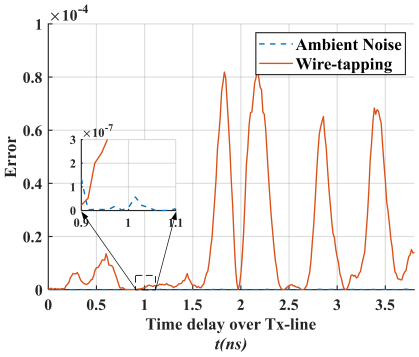
(c) Comparison of $E_{xy}(t)$ with and without load modification



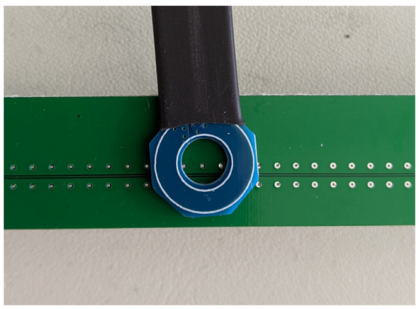
(d) Experiment setup of wire-tapping



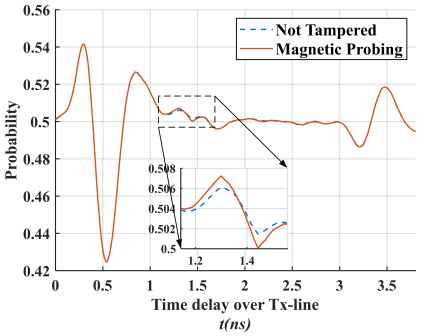
(e) Comparison of IIPs with and without wire-tapping



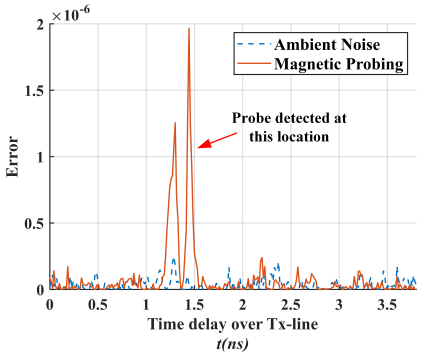
(f) Comparison of $E_{xy}(t)$ with and without wire-tapping



(g) Experiment setup of magnetic probing



(h) Comparison of IIPs with and without magnetic probing



(i) Comparison of $E_{xy}(t)$ with and without magnetic probing

Fig. 9. Experiment setups and results for detecting hardware physical attacks including cold boot attacks, wire-tapping, and probing on buses. (a,b, and c) show detection of cold boot attacks and Trojan chips; (d, e, and f) show detection of wire-tapping; (g, h, and i) show detection of magnetic probing attacks.

PUF, Arbiter-PUF, or Tx-line PUF presented here. Wei et al. [69] report a new PUF technology based on IIP. A vector network analyzer (VNA) was used to extract the IIP from a bus/cable. However, VNA is an expensive testing equipment, and it was not a practically feasible technology to be integrated into a computer system for runtime hardware security.

The major difference between DIVOT and the abovementioned approaches is that DIVOT uses the backscatters from already-existing digital waveforms flowing on a bus, and extracts the IIP without affecting normal data transfers. In other words, DIVOT is transparent to normal operations. Furthermore, DIVOT can fight against EM-based non-contact probes using a simple integrated circuit at a bus interface, which none of above mentioned existing works can do. Besides, DIVOT shows its huge advantage in terms of size and cost, making it practically feasible to protect a wide variety of buses and interfaces. In addition, since over 90% of the hardware in a DIVOT detector can be shared/multiplexed by many detectors on a chip, it can scale cost-effectively to multiple buses in a complex SoC or CPU.

Another group of related works (e.g., [7], [14], [28], [54], [55], [72], [77]) discuss challenges in the state-of-the-art memory encryption and integrity verification as well as corresponding solutions. Counter-based encryption [14] is

demonstrated useful to ensure data confidentiality. Yan et al. [72] make counter-based encryption practical for memory encryption. They eliminate the counter overflow problems, reduce counter size, and improve authentication performance by splitting the counter simultaneously and overlapping the authentication latency with memory accesses. DEUCE [77] proposes a write efficient scheme for encrypted PCM that re-encrypts only the words that have changed when a writeback incurs. SYNERGY [55] combines security and reliability by re-purposing ECC-chip to store security metadata (i.e., MACs), thus obtaining data and security metadata can be fulfilled in a single memory access. Their successive work, Morphable Counters [54], further reduces the performance overhead incurred in integrity-tree traversal. Triad-NVM [7] discusses persisting security metadata in NVMM and proposes an efficient recovery mechanism in a hybrid main memory system. DIVOT takes a completely different approach from the above existing works. Our iTDR logic authenticates both master and slave of a bus for all memory access operations. At the same time, physical tampering can be detected instantly using the same iTDR logic.

Besides hardware attacks, researchers have been exploring side channel attacks and countermeasures in computer systems (e.g., [6], [10], [22], [23], [33], [34], [37], [60], [67], [68], [70]). Cache timing attacks [22], [33], [68] leverage cache access patterns and timing to recover confidential information. Meltdown [37] exploits out-of-order execution of user instructions to read sensitive information from kernel memory. Spectre [34] leverages branch prediction and tricks speculatively executed instructions into leaking information. Interestingly, side channel information such as EM emanation can also be leveraged to protect against attacks as evidenced by a recent work EMMA [58]. Awad et al. [6] propose ObfusMem that hides memory traits leveraging smart memory to avoid leakage of secret information. InvisiMem [1] uses smart memory to mitigate side channel leakage by having the processor and the memory send packets at a constant rate and applying randomized encryption to the whole packet, including data, address and access type. NDA [70] and SpecShield [10] prevent speculative execution attacks by restricting propagation of potential secrets to covert channels. We note that the above prior works are orthogonal to our work and these techniques can be integrated in our design to add another layer of protection against software attacks.

VI. Conlusion

This paper presented a new hardware design for secure computer architectures, namely DIVOT, **D**etecting **I**mpedance **V**ariations **O**f **T**ransmission-lines. In order to detect small and weak impedance inhomogeneity patterns, an integrated time domain reflectometer (iTDR) circuit has been designed and implemented to provide strong defenses against physical attacks, such as cold boot attacks, bus snooping, wiretapping, and probing memory buses and modules. With the newly introduced concepts such as analog-to-probability conversion and probability density modulation, the iTDR is capable of authenticating memory buses, memory modules, and processor chips without negatively impacting normal processing. Furthermore, the new DIVOT architecture can be implemented with very little additional hardware, high energy efficiency, and no performance overhead. DIVOT cost-effectively extends the hardware TCB beyond the CPU chip that has been assumed vulnerable in most existing research on secured computer architectures to date. The new iTDR can be incorporated in any bus interface of a computer system, including high performance servers and embedded computers in smart mobile devices or IoTs, to offer low cost and strong hardware security. A working prototype has been built using a commercial off the shelf FPGA and a custom PCB. Experimental results demonstrated its feasibility, high performance, and low hardware overhead that includes only 71 registers and 124 LUTs. Our future work includes extending the DIVOT design to I/O buses, network interfaces, and data storage systems, as well as increasing detection accuracy by monitoring multiple wires on a bus.

Acknowledgements

This research is supported in part by National Science Foundation under grants #CCF-1439011 and CCF-1421823. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF. It is also partly supported by a research contract between URI and Shenzhen Dapu Microelectronics Co., Ltd. The authors are very grateful to the anonymous reviewers for their detailed comments and suggestions. These comments and suggestions helped us to improve the quality of the paper greatly.

References

[1] S. Aga and S. Narayanasamy, "Invisimem: Smart memory defenses for memory bus side channel," in *ACM SIGARCH Computer Architecture News*, vol. 45, no. 2. ACM, 2017, pp. 94–106.

[2] O. Aleph, "Smashing the stack for fun and profit," *http://www. shmoo. com/phrack/Phrack49/p49-14*, 1996.

[3] ARM Architecure, "Security technology building a secure system using trustzone technology (white paper)," 2009.

[4] S. Arnautov, B. Trach, F. Gregor, T. Knauth, A. Martin, C. Priebe, J. Lind, D. Muthukumaran, D. O'Keeffe, M. L. Stillwell, and Others, "{SCONE}: Secure linux containers with intel {SGX}," in *12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16)*, 2016, pp. 689–703.

[5] T. W. Arnold, C. Buscaglia, F. Chan, V. Condorelli, J. Dayka, W. Santiago-Fernandez, N. Hadzic, M. D. Hocker, M. Jordan, T. E. Morris, and Others, "IBM 4765 cryptographic coprocessor," *IBM Journal of Research and Development*, vol. 56, no. 1.2, pp. 10–11, 2012.

[6] A. Awad, Y. Wang, D. Shands, and Y. Solihin, "Obfusmem: A low-overhead access obfuscation for trusted memories," in *ACM SIGARCH Computer Architecture News*, vol. 45, no. 2. ACM, 2017, pp. 107–119.

[7] A. Awad, M. Ye, Y. Solihin, L. Njilla, and K. A. Zubair, "Triad-nvm: Persistency for integrity-protected and encrypted non-volatile memories," in *Proceedings of the 46th International Symposium on Computer Architecture*. ACM, 2019, pp. 104–115.

[8] P. M. Aziz, H. V. Sorensen, and J. Vn der Spiegel, "An overview of sigma-delta converters," *IEEE signal processing magazine*, vol. 13, no. 1, pp. 61–84, 1996.

[9] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The sorcerer's apprentice guide to fault attacks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 370–382, 2006.

[10] K. Barber, A. Bacha, L. Zhou, Y. Zhang, and R. Teodorescu, "Specshield: Shielding speculative data from microarchitectural covert channels," in *2019 28th International Conference on Parallel Architectures and Compilation Techniques (PACT)*. IEEE, 2019, pp. 151–164.

[11] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012.

[12] A. Baumann, M. Peinado, and G. Hunt, "Shielding applications from an untrusted cloud with haven," *ACM Transactions on Computer Systems (TOCS)*, vol. 33, no. 3, p. 8, 2015.

[13] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in *Annual international cryptology conference*. Springer, 1996, pp. 1–15.

[14] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," in *Proceedings 38th Annual Symposium on Foundations of Computer Science*. IEEE, 1997, pp. 394–403.

[15] D. Champagne and R. B. Lee, "Scalable architectural support for trusted software," in *HPCA-16 2010 The Sixteenth International Symposium on High-Performance Computer Architecture*. IEEE, 2010, pp. 1–12.

[16] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Annual International Cryptology Conference*. Springer, 1999, pp. 398–412.

[17] S. D. Corey and A. T. Yang, "Interconnect characterization using time-domain reflectometry," *IEEE transactions on microwave theory and techniques*, vol. 43, no. 9, pp. 2151–2156, 1995.

[18] V. Costan, I. Lebedev, and S. Devadas, "Sanctum: Minimal hardware extensions for strong software isolation," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016, pp. 857–874.

[19] C. Cowan, F. Wagle, C. Pu, S. Beattie, and J. Walpole, "Buffer overflows: Attacks and defenses for the vulnerability of the decade," in *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, vol. 2. IEEE, 2000, pp. 119–129.

[20] V. Cuppu, B. Jacob, B. Davis, and T. Mudge, "A performance comparison of contemporary DRAM architectures," in *ACM SIGARCH Computer Architecture News*, vol. 27, no. 2. IEEE Computer Society, 1999, pp. 222–233.

[21] EETimes. (2009) Maxim : Secure supervisor ic has active tamper detection. [Online]. Available: https://www.eetimes.com/maxim-secure-supervisor-ic-has-active-tamper-detection

[22] H. Fang, S. S. Dayapule, F. Yao, M. Doroslovački, and G. Venkataramani, "Prefetch-guard: Leveraging hardware prefetches to defend against cache timing channels," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2018, pp. 187–190.

[23] C. W. Fletcher, L. Ren, A. Kwon, M. van Dijk, and S. Devadas, "Freecursive oram:[nearly] free recursion and integrity verification for position-based oblivious ram," *ACM SIGARCH Computer Architecture News*, vol. 43, no. 1, pp. 103–116, 2015.

[24] D. Gruss, C. Maurice, and S. Mangard, "Rowhammer. js: A remote software-induced fault attack in javascript," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2016, pp. 300–321.

[25] S. Gupta and B. B. Gupta, "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art," *International Journal of System Assurance Engineering and Management*, vol. 8, no. 1, pp. 512–530, 2017.

[26] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest we remember: cold-boot attacks on encryption keys," *Communications of the ACM*, vol. 52, no. 5, pp. 91–98, 2009.

[27] A. Hastings and S. Sethumadhavan, "Are Computer Architects to Blame for the State of Security Today?" 2019. [Online]. Available: https://www.sigarch.org/are-computer-architects-to-blame-for-the-state-of-security-today/

[28] M. Henson and S. Taylor, "Memory encryption: A survey of existing techniques," *ACM Computing Surveys (CSUR)*, vol. 46, no. 4, p. 53, 2014.

[29] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[30] S. Hinaga, M. Koledintseva, J. L. Drewniak, A. Koul, and F. Zhou, "Thermal effects on pcb laminate material dielectric constant and dissipation factor," *IPC APEX EXPO*, 2010.

[31] Jupiter Instruments. (2019) I2C bus monitor. [Online]. Available: http://www.jupiteri.com/

[32] J. S. Kim, M. Patel, H. Hassan, and O. Mutlu, "The DRAM latency PUF: Quickly evaluating physical unclonable functions by exploiting the latency-reliability tradeoff in modern commodity DRAM devices," in *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*. IEEE, 2018, pp. 194–207.

[33] V. Kiriansky, I. Lebedev, S. Amarasinghe, S. Devadas, and J. Emer, "DAWG: A defense against cache timing attacks in speculative execution processors," in *2018 51st Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*. IEEE, 2018, pp. 974–987.

[34] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, and Others, "Spectre attacks: Exploiting speculative execution," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1–19.

[35] D. Lee, J. Sung, and J. Park, "A 16ps-resolution random equivalent sampling circuit for tdr utilizing a vernier time delay generation," in *2003 IEEE Nuclear Science Symposium. Conference Record (IEEE Cat. No. 03CH37515)*, vol. 2. IEEE, 2003, pp. 1219–1223.

[36] D. Lie, C. Thekkath, M. Mitchell, P. Lincoln, D. Boneh, J. Mitchell, and M. Horowitz, "Architectural support for copy and tamper resistant software," *Acm Sigplan Notices*, vol. 35, no. 11, pp. 168–177, 2000.

[37] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, and Others, "Meltdown: Reading kernel memory from user space," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 973–990.

[38] X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang, "When good becomes evil: Keystroke inference with smartwatch," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 1273–1285.

[39] M. Maas, E. Love, E. Stefanov, M. Tiwari, E. Shi, K. Asanovic, J. Kubiatowicz, and D. Song, "Phantom: Practical oblivious computation in a secure processor," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 311–324.

[40] S. Manich, M. S. Wamser, and G. Sigl, "Detection of probing attempts in secure ics," in *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, 2012, pp. 134–139.

[41] Maxim Integrated. (2020) DS3645: 4KB Secure Memory with Tamper Protection for Network Server Applications. [Online]. Available: https://www.maximintegrated.com/en/products/embedded-security/security-managers/DS3645.html

[42] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar, "Innovative instructions and software model for isolated execution." *Hasp@ isca*, vol. 10, no. 1, 2013.

[43] C. Meijer and B. Van Gastel, "Self-encrypting deception: weaknesses in the encryption of solid state drives," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 72–87.

[44] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE transactions on computers*, vol. 51, no. 5, pp. 541–552, 2002.

[45] S. Paley, T. Hoque, and S. Bhunia, "Active protection against pcb physical tampering," in *2016 17th International Symposium on Quality Electronic Design (ISQED)*. IEEE, 2016, pp. 356–361.

[46] B. Park, M. Tehranipoor, D. Forte, and N. Maghari, "A metal-via resistance based physically unclonable function with 1.18% native instability," in *2019 IEEE Custom Integrated Circuits Conference (CICC)*. IEEE, 2019, pp. 1–4.

[47] M. C. L. Purisima, J. S. Marciano, R. D. De Joya, P. P. Mogatas, and C. A. Salazar, "Fpga implementation of a time domain reflectometry (tdr) system for slope monitoring applications," in *TENCON 2010-2010 IEEE Region 10 Conference*. IEEE, 2010, pp. 1198–1202.

[48] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *International Conference on Research in Smart Cards*. Springer, 2001, pp. 200–210.

[49] R. Raguram, A. M. White, D. Goswami, F. Monrose, and J.-M. Frahm, "iSpy: automatic reconstruction of typed input from compromising reflections," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 527–536.

[50] L. Ren, C. W. Fletcher, A. Kwon, M. Van Dijk, and S. Devadas, "Design and implementation of the ascend secure processor," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 2, pp. 204–216, 2017.

[51] S. Rixner, W. J. Dally, U. J. Kapasi, P. Mattson, and J. D. Owens, "Memory access scheduling," in *ACM SIGARCH Computer Architecture News*, vol. 28, no. 2. ACM, 2000, pp. 128–138.

[52] B. Rogers, S. Chhabra, M. Prvulovic, and Y. Solihin, "Using address independent seed encryption and bonsai merkle trees to make secure processors os-and performance-friendly," in *Proceedings of the 40th Annual IEEE/ACM International Symposium on Microarchitecture*. IEEE Computer Society, 2007, pp. 183–196.

[53] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 2015, pp. 1–6.

[54] G. Saileshwar, P. Nair, P. Ramrakhyani, W. Elsasser, J. Joao, and M. Qureshi, "Morphable counters: Enabling compact integrity trees for low-overhead secure memories," in *2018 51st Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*. IEEE, 2018, pp. 416–427.

[55] G. Saileshwar, P. J. Nair, P. Ramrakhyani, W. Elsasser, and M. K. Qureshi, "Synergy: Rethinking secure-memory design for error-correcting memories," in *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*. IEEE, 2018, pp. 454–465.

[56] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards Trusted Cloud Computing." *HotCloud*, vol. 9, no. 9, p. 3, 2009.

[57] M. Seaborn and T. Dullien, "Exploiting the DRAM rowhammer bug to gain kernel privileges," *Black Hat*, vol. 15, 2015.

[58] N. Sehatbakhsh, A. Nazari, H. Khan, A. Zajic, and M. Prvulovic, "Emma: Hardware/software attestation framework for embedded systems using electromagnetic signals," in *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*, ser. MICRO 52. New York, NY, USA: Association for Computing Machinery, 2019, p. 983995. [Online]. Available: https://doi.org/10.1145/3352460.3358261

[59] S. W. Smith and S. Weingart, "Building a high-performance, programmable secure coprocessor," *Computer Networks*, vol. 31, no. 8, pp. 831–860, 1999.

[60] E. Stefanov, M. Van Dijk, E. Shi, C. Fletcher, L. Ren, X. Yu, and S. Devadas, "Path ORAM: an extremely simple oblivious RAM protocol," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 299–310.

[61] G. E. Suh, D. Clarke, B. Gassend, M. Van Dijk, and S. Devadas, "AEGIS: architecture for tamper-evident and tamper-resistant processing," in *ACM International Conference on Supercomputing 25th Anniversary Volume*. ACM, 2014, pp. 357–368.

[62] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.

[63] G. E. Suh, C. W. O'Donnell, I. Sachdev, and S. Devadas, "Design and implementation of the AEGIS single-chip secure processor using physical random functions," in *ACM SIGARCH Computer Architecture News*, vol. 33, no. 2. IEEE Computer Society, 2005, pp. 25–36.

[64] Trusted Computing Group, "Trusted Platform Module (TPM) Summary," 2008. [Online]. Available: https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/

[65] J. Van Bulck, M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx, "Foreshadow: Extracting the keys to the intel {SGX} kingdom with transient out-of-order execution," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 991–1008.

[66] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, "Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis." in *NDSS*, vol. 2007, 2007, p. 12.

[67] R. Wang, Y. Zhang, and J. Yang, "D-ORAM: Path-ORAM delegation for low execution interference on cloud servers with untrusted memory," in *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*. IEEE, 2018, pp. 416–427.

[68] Y. Wang, A. Ferraiuolo, D. Zhang, A. C. Myers, and G. E. Suh, "SecDCP: secure dynamic cache partitioning for efficient timing channel protection," in *Proceedings of the 53rd Annual Design Automation Conference*. ACM, 2016, p. 74.

[69] T. Wei and J. Huang, "Transmission Line Identification via Impedance Inhomogeneity Pattern," *IEEE Journal of Radio Frequency Identification*, 2019.

[70] O. Weisse, I. Neal, K. Loughlin, T. F. Wenisch, and B. Kasikci, "NDA: Preventing Speculative Execution Attacks at Their Source," in *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*. ACM, 2019, pp. 572–586.

[71] L. Whetsel, "An IEEE 1149.1 Based Logic/Signature Analyzer in a Chip." in *ITC*, 1991, pp. 869–878.

[72] C. Yan, D. Englender, M. Prvulovic, B. Rogers, and Y. Solihin, "Improving cost, performance, and security of memory encryption and authentication," in *ACM SIGARCH Computer Architecture News*, vol. 34, no. 2. IEEE Computer Society, 2006, pp. 179–190.

[73] J. Yang, Y. Zhang, and L. Gao, "Fast secure processor for inhibiting software piracy and tampering," in *Proceedings of the 36th annual IEEE/ACM International Symposium on Microarchitecture*. IEEE Computer Society, 2003, p. 351.

[74] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog malicious hardware," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 18–37.

[75] Z. Yao, T. Mauldin, G. Hefferman, Z. Xu, M. Liu, and T. Wei, "Low-cost optical fiber physical unclonable function reader based on a digitally integrated semiconductor LiDAR," *Appl. Opt.*, vol. 58, no. 23, pp. 6211–6216, aug 2019. [Online]. Available: http://ao.osa.org/abstract.cfm?URI=ao-58-23-6211

[76] S. F. Yitbarek, M. T. Aga, R. Das, and T. Austin, "Cold boot attacks are still hot: Security analysis of memory scramblers in modern processors," in *2017 IEEE International Symposium on High Performance Computer Architecture (HPCA)*. IEEE, 2017, pp. 313–324.

[77] V. Young, P. J. Nair, and M. K. Qureshi, "DEUCE: Write-efficient encryption for non-volatile memories," *ACM SIGPLAN Notices*, vol. 50, no. 4, pp. 33–44, 2015.

[78] F. Zhang, A. Hennessy, and S. Bhunia, "Robust counterfeit pcb detection exploiting intrinsic trace impedance variations," in *2015 IEEE 33rd VLSI Test Symposium (VTS)*. IEEE, 2015, pp. 1–6.