# Physical Characterization of Arbiter PUFs

Shahin Tajik[1], Enrico Dietz[2], Sven Frohmann[2], Jean-Pierre Seifert[1], Dmitry Nedospasov[1], Clemens Helfmeier[3], Christian Boit[3], Helmar Dittrich[2]

[1]Security in Telecommunications, Technische Universität Berlin, Germany
{shahin,jpseifert,dmitry}@sec.t-labs.tu-berlin.de
[2]Teraherz Spectroscopy, Technische Universität Berlin, Germany
{dietz,sf}@physik.tu-berlin.de
[3]Semiconductor Devices, Technische Universität Berlin, Germany
{clemens.helfmeier,christian.boit}@tu-berlin.de

**Abstract.** As intended by its name, Physically Unclonable Functions (PUFs) are considered as an ultimate solution to deal with insecure storage, hardware counterfeiting, and many other security problems. However, many different successful attacks have already revealed vulnerabilities of certain digital intrinsic PUFs. Although settling-state-based PUFs, such as SRAM PUFs, can be physically cloned by semi-invasive and fully-invasive attacks, successful attacks on timing-based PUFs were so far limited to modeling attacks. Such modeling requires a large subset of challenge-response-pairs (CRP) to successfully model the targeted PUF. In order to provide a final security answer, this paper proves that all arbiter-based (i.e. controlled and XOR-enhanced) PUFs can be completely and linearly characterized by means of photonic emission analysis. Our experimental setup is capable of measuring *every* PUF-internal delay with a resolution of 6 picoseconds. Due to this resolution we indeed require only the theoretical minimum number of linear independent equations (i.e. physical measurements) to directly solve the underlying inhomogeneous linear system. Moreover, we neither require to know the actual PUF challenges nor the corresponding PUF responses for our physical delay extraction. On top of that devastating result, we are also able to further simplify our setup for easier physical measurement handling. We present our practical results for a real arbiter PUF implementation on a Complex Programmable Logic Device (CPLD) from Altera manufactured in a 180 nanometer process.

**Keywords**: Arbiter PUF, photonic emission analysis, backside, physical characterization

## 1 Introduction

Physically Unclonable Functions (PUFs) offer a promising solution for future security problems [9]. PUFs can be utilized as the basis for many security applications, such as encryption [13, 29] and hardware fingerprinting [26, 33]. Although there are different PUF classifications in the literature regarding their

characteristics, they can generally be categorized in two distinct classes of PUFs: settling-state-based PUFs and timing-based PUFs [15]. The former is based on bistable circuits such as SRAMs, while the latter is based on intrinsic differences in timing of a set of symmetric circuit paths.

Although *unclonability* and *unpredictability* are the main PUF requirements [3, 22], previous work in the literature has shown how different PUFs can be attacked and cloned. Settling-state-based PUFs such as SRAM PUFs can be characterized and cloned physically by semi-invasive and fully invasive attacks [10, 20]. Timing-based PUFs such as Arbiter PUFs are vulnerable to machine-learning attacks, which make it possible to emulate the PUF response [12, 24]. However, machine-learning attacks require a large number of challenge-response pairs (CRP) to predict the response with high probability. Any non-linearity in the PUF response can negatively impact the effectiveness of machine-learning techniques [13, 32]. As a result substantially more CRPs together with extra side channel information are required to model the PUF response successfully [16]. However, in a real attack scenario, the intrinsic PUF response may be unavailable to the attacker [8, 14]. Moreover, trying a large set of CRPs may also be infeasible due to other countermeasures implemented on modern secure devices [23].

This work demonstrates that arbiter PUFs and more generally, timing-based PUFs can be characterized by high-resolution temporal photonic emission analysis from the chip's backside. This approach does not need any readout of PUF response nor does it require a substantial number of challenges to characterize the PUF. Our methodology is based on measuring the time difference between enabling the PUF and photon emission at the output of the last stage. For our Proof-of-concept (PoC), we have implemented an arbiter PUF on a Complex Programmable Logic Device (CPLD). The delay between the input of the PUF and the output of photodetector can be measured with an overall resolution of approximately 6 picoseconds by a Time-to-Digital Converter (TDC). As a result, the PUF response is determined by comparing the measured delays on both PUF chains. Furthermore, in our methodology, the required challenges for the physical characterization of the PUF increase linearly with PUF length. Finally, based on a mathematical approach we find the minimum number of necessary challenge combinations, which are required to characterize the PUF. Using this methodology it also possible to characterize controlled PUFs [8], where the challenge is inaccessible to the attacker. As compared to other characterization techniques, such as machine learning, this methodology greatly reduces the amount of measurements that are necessary to characterize the intrinsic PUF behavior. The main contributions of this paper are as follows:

**Physical characterization of timing-based PUFs.** We present the first physical characterization attack on timing-based PUFs with the help of photonic emission analysis. This approach is capable of physically characterizing the intrinsic behavior of the circuit by measuring the delays within the circuit with a high degree of accuracy. In the case of an arbiter PUF this consists of measuring the intrinsic delays of each individual stage of the circuit. As compared to other heuristic methodologies which require a substantially greater number of

measurements than individual PUF stages, our methodology requires just two measurements per PUF stage.

**Low-cost measurement setup for measuring the delay with the resolution of 6 ps.** We introduce an efficient and cost-effective experimental setup with a substantial temporal resolution. The setup is capable of performing temporal measurements with an approximate time resolution of 6 ps. The time resolution of the setup allows for the exact characterization of the intrinsic delays of each individual stage of the PUF. Moreover, the setup provides sufficient time resolution for modern process nodes.

**Practical evaluation against a Proof-of-Concept arbiter PUF implementation.** The PoC implementation was realized on a common programmable logic platform. To extract the device's intrinsic behavior, we performed dynamic semi-invasive backside analysis of the photonic emissions of the device. Because the analysis techniques are semi-invasive the integrity of the device's intrinsic response is not changedpre.

**Mathematical approach for measurement optimization.** In order to physically characterize the PUF, we propose a measurement technique to minimize the number of challenges that are necessary for a PUF characterization. Furthermore, we provide a mathematical approach for minimizing the effort of measurement for arbiter PUFs in general. Combined, these techniques greatly reduce the number of measurements and measurement locations that are necessary for PUF characterization.

The rest of this paper is organized as follows: Section 2 presents background information on the delay-based PUFs and photonic emission in CMOS technology. Moreover, the programmable logic architecture is explained and the related work is reviewed. In Section 3, the utilized experimental setup is presented. Section 4 introduces the mathematical approach for the optimized measurement. Section 5 demonstrates the practical results, where we were able to measure the small delay differences. In Section 6, we present additional considerations about our methodology. Finally in Section 7, we conclude the paper.

## 2 Background

### 2.1 Arbiter-based PUF

Due to manufacturing variations, there are small random delay differences on symmetrical electrical paths on a chip. The entropy of the delays is sufficient to ensure a unique PUF response for each individual device instance. Arbiter and Ring-oscillator PUFs are two examples of timing-based PUFs [15]. Arbiter PUFs utilize the intrinsic timing differences of two symmetrically designed paths to a single bit of the response at the output of the circuit [12]. It consists of multiple connected stages and an arbiter at the end of the chain, see Figure 1. Each stage consists of two outputs and three inputs, a single bit of the challenge and the two outputs from the previous stage. The inputs of the first stage are connected to a common enable signal. The outputs of the last stage are connected to a so-called arbiter, which determines which signal arrived first. Based on this result,

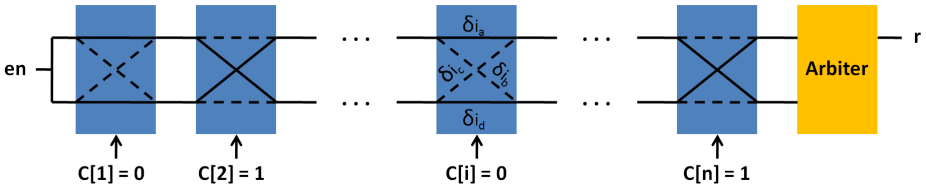



Fig. 1: Arbiter PUF

the arbiter generates a single bit known as the response. Although the nominal delays of direct paths and crossed paths are equal ($\delta_{i_a} = \delta_{i_d}$ and $\delta_{i_b} = \delta_{i_c}$), due to the intrinsic delays of the circuit, different challenges produce different results. The differences between two identical device instances will be sufficient to differentiate the unique responses of the devices.

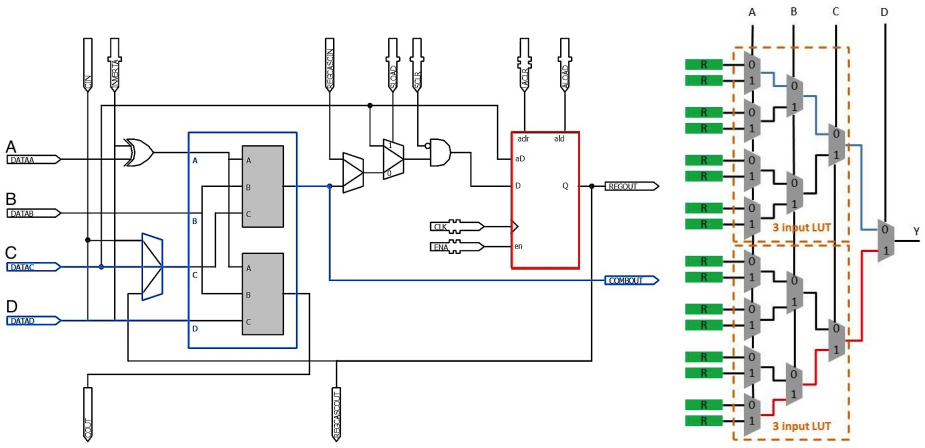
### 2.2 Photonic Emission in CMOS

Individual logic gates are implemented on the Complementary Metal Oxide Semiconductor (CMOS) Integrated Circuits (ICs) by a set of connected p-type and n-type Metal Oxide Semiconductor (MOS) transistors. In a static state, where no transistor devices are switching, there is at least one transistor in the off region between the supplied power (VDD) and ground (GND). Therefore, the current consumption of the gate is minimal. However, during a switching event a substantial current passes through the circuit. As a result, the transistors enter an operating region known as *saturation* for a short period of time. During saturation, the kinetic energy of accelerated hot carriers can be released via photon emission [4]. n-type transistors emit significantly more photons as compared to p-type transistors, due to the higher mobility of electrons than holes. Hence, only photons emitted by n-type transistor can be observed in general. The emission rate of the transistors is proportional to the switching frequency of the circuit. However, raising the supply voltage also increases the amount of photons emitted by the device exponentially.

Due to multiple interconnect layers on the frontside of modern IC designs, the optical path is obstructed [23]. Therefore, it is almost impossible to observe photonic emissions from the frontside. However, photonic emissions can be observed from the IC backside as well. Although, silicon substrate is highly absorptive for wavelengths shorter than the bandgap energy, the silicon substrate is transparent to near infrared (NIR) emissions. Hence, any NIR photons emitted by the device will pass through the silicon substrate and can be observed from the IC backside.

### 2.3 Programmable Logic Architecture

PUFs can be realized in different types of hardware implementations. Timing-based PUFs can also be implemented on a programmable logic device, i.e. FPGAs and CPLDs. The architecture of modern CPLDs and FPGAs is very similar




(a) Logical Element (b) Lookup Table

Fig. 2: (a)Architecture of a Logical Element in an Altera MAX V CPLD: A configurable 4-input combinatorial circuit (blue). Additionally each LE consists of multiple control inputs as well as global signals such as clock and enable [2]. (b)The LUT is realized by multiple multiplexers, which are controlled by the data inputs. The output of the LUT is loaded from the existing SRAM cells inside the LUT. In our PUF design, each signal path is connected to one of the LUT's inputs (input A). The challenge signal is connected to all other three inputs (B, C and D) in order to limit the routing only to two paths inside the LUT.

and the architectures of any given vendor share many commonalities. The primary architectural differences of modern CPLDs and FPGAs are logical size, the complexity of the routing network and the hard macros available to the design. Moreover, CPLDs generally store the configuration within the same device package, whereas FPGAs generally require external memory for storing the device configuration. Programmable logic devices consist of an array of configurable Logic Elements (LEs), see Figure 2. The configuration determines the logical behavior of each individual LE. The LEs themselves are commonly realized using so called Look-Up-Tables (LUTs) in which the output values are stored for a particular input combination. Combinatorial logic of a particular design can be entirely realized using LUTs. The Altera Max V architecture utilized in this work utilizes two 3-input LUTs to realize a 4-input LE, see Figure 2(a). Each LE also provides an additional configurable register with multiple control inputs and an output for realizing sequential logic. LEs are organized into groups of ten which form so called Logical Array Blocks (LABs). In addition to global routing resources, each LAB provides additional routing to each LE within the LAB.

### 2.4 Related Work

In recent years, many different attacks on PUFs have been proposed. Settling-state based PUFs, such as SRAM PUFs, can be physically cloned by semi-invasive attacks [10]. The authors of this work demonstrated how SRAM PUF responses can be characterized by a Focused Ion Beam (FIB) circuit edit. Moreover, SRAM PUFs are also vulnerable to fully-invasive attacks, due to lack of tamper detection mechanism [20]. It was also shown that timing-based PUFs, such as Ring-oscillator PUFs, are also vulnerable to semi-invasive electromagnetic (EM) side channel attacks [18].

However, to this date, arbiter PUFs are only the target of mathematical modeling attacks. Modeling attacks require a subset of CRPs to build a model on that and predict the PUF response for all possible challenges [12]. One of the first utilized modeling techniques was linear programming to model the timing-based PUF [21]. Machine-learning tools such as Logistic Regression (LR) can also be utilized to model the arbiter PUF successfully [24]. The modeling attacks becomes more difficult by introducing non-linearities to the PUF delays and responses. Two example of non-linear PUFs are Feed-forward arbiter PUFs [13] and XOR-PUFs [32]. However, it has been shown that Feed-forward PUFs are vulnerable to evolutionary algorithm [25]. Moreover, a modeling attack based on higher number of CRPs and power side channel information can be applied successfully to XOR-arbiter PUFs [16]. Other modeling techniques include solving integer equations utilize the CMOS noise as a side channel information or environmental changes as a fault injection technique to model the timing-based PUFs [6, 5].

Photonic emission analysis is introduced as a new side channel attack to analyze security applications on the chip such as cryptographic ciphers [7]. In order to bypass the multiple interconnect layers on the frontside of the chip, photonic emission analysis and photonic fault injection attacks can be conducted from the backside [31, 30]. It has been shown that chips, such as microcontrollers, can be functionally analyzed by their optical emissions during runtime [19]. Simple Photonic Emission Analysis (SPEA) is another approach that can recover the full AES secret key by monitoring access to S-Box [28]. Furthermore, the full AES secret key can be recovered by a similar approach called Differential Photonic Emission Analysis [11].

## 3 Experimental Setup

### 3.1 Measurement Setup

The experimental setup, shown schematically in Figure 3, is an optimized infrared microscope equipped with a scientific Si-CCD camera and an InGaAs avalanche diode as detectors for spatial and temporal analysis [27]. The Si-CCD is a back illuminated deep depletion type featuring high quantum efficiency in the NIR region. To minimize dark current it is cooled down to $-70\,^{\circ}\mathrm{C}$, which

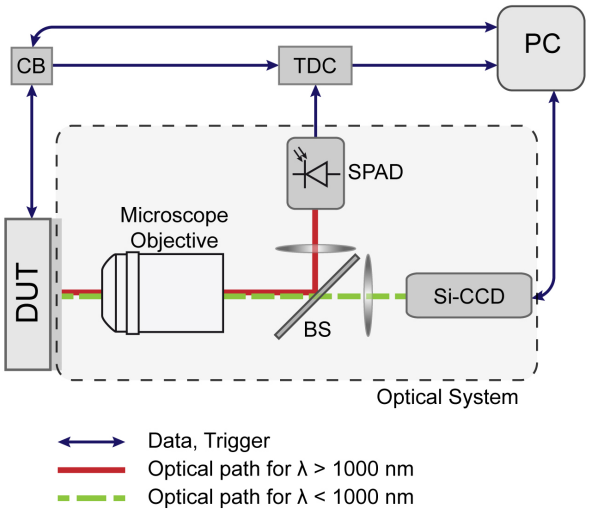



Fig. 3: Controlling the DUT with the CB and capturing emitted photons from the DUT by SI-CCD camera and InGaAs-SPAD

allows long exposure times to accumulate enough photons from the weak hot carrier emission. Due to the long integration time of several seconds and the limited readout speed of the CCD sensor, it is used for spatial analyses only. The temporal analysis of the photonic emission requires a very fast infrared detector. Therefore a free-running InGaAs avalanche detector in Geiger Mode (SPAD) is used to detect single photons. Its sensitivity covers a wavelength range between 1 to 1.6 $\mu$m with peak quantum efficiency of 20%. Thermoelectrical cooling reduces the dark count rate below 2 kHz.

The Device under Test (DUT), is controlled by a computer via a control box (CB), which provides the enable signal for the PUF and a time reference signal for the time to digital converter (TDC). Photons emitted from the DUT are collected by the microscope objective (NA = 0.45) and divided into two optical paths by a short-pass beam splitter (BS). Short-wave photons below 1 $\mu$m are transmitted to the Si-CCD camera while the long-wave photons are reflected onto the InGaAs-SPAD. This configuration allows capturing images with the CCD and time resolved measurements with the SPAD simultaneously. An incoming photon from the DUT causes the avalanche breakdown of the SPAD and the resulting electrical pulse is registered by the TDC. The FPGA-based TDC time tags each occurring event with a resolution of 81 picoseconds. This way both the enable signal of the PUF chain and the detected photons from the chain's output transistor are time tagged allowing a direct calculation of the their delay. Due to jitter in the response time of the SPAD and electrical jitter in the CB and TDC the overall time uncertainty for a single photonic event is 190 ps rms. An accumulation of multiple photonic events is used to improve the time

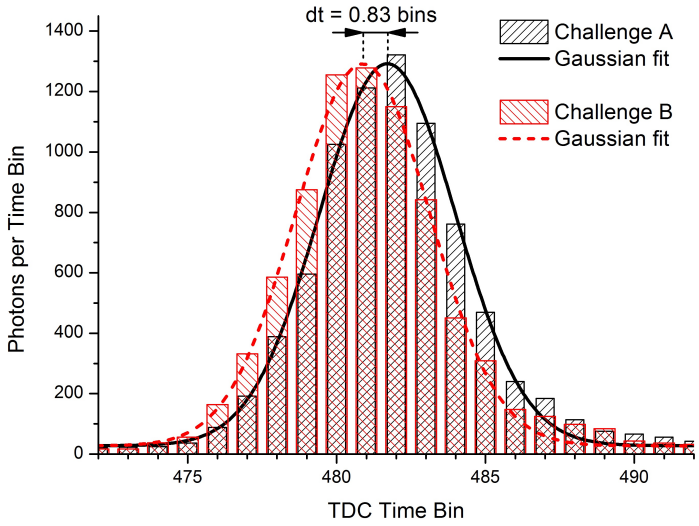



Fig. 4: Timing difference of two different challenges at the output of last stage. The time bin width is 81 ps

resolution by calculating the centroid of the Gaussian-like distribution of the delay time histogram, see Figure 4. This super-resolution technique enhances the time resolution significantly beyond the 81 ps granularity of the TDC and allows measurements of very small shifts in the delay time. Experiments showed that the accuracy of our current setup is limited by drifts in the electronics to 6 ps rms. Apart from the custom made holding of the DUT to a 3-dimensional moving stage and electronics to control and communicate with the CPLD, the setup consists of commercially available components. As the focus of the setup is on time resolved measurements, it can be realized for about 30000 Euros.

### 3.2 Device Under Test

In this work, Altera MAX V CPLD devices (part number `5M80ZT100C5N`) were utilized for the physical experiments [1]. A backside reflectance image of the CPLD shows the presence of 240 LEs on the device, see Figure 6. However, this device allows the use of 80 Logic Elements (LE) in total. The device contains 24 Logic Array Blocks (LAB) with 10 LEs each. The non-volatile memory and additional infrastructure logic is located on the upper half in Figure 6, I/O pads are clearly visible on the perimeter of the device. The devices were decapsulated using the Ultratec ASAP-1 mechanical polishing machine exposing the backside. The bulk silicon material of the devices was thinned down significantly. The silicon surface was polished to expose a surface suitable for optical imaging.

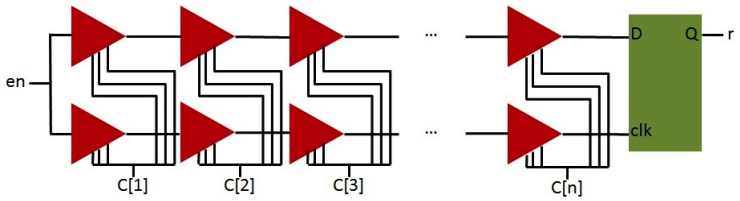



Fig. 5: Implementation of arbiter PUF by two independent buffers chains.

To further improve the surface quality and optical properties of the devices, an anti reflective coating (ARC) was applied to the devices. Finally, the devices were soldered onto a custom printed circuit board (PCB) to allow capturing of images from the exposed backside of the device while maintaining full electrical connectivity.

### 3.3 PUF implementation on CPLD

One possibility for implementing arbiter PUFs is to utilize digital multiplexers. In this case, each PUF stage requires two multiplexers. As each multiplexer is realized by a LUT, two inputs out of four available inputs of LUT are utilized, see Figure 2(b). Based on *don't-care* inputs, the output of multiplexer can be loaded from different SRAM cells inside the LUT and take different routes to the output. This fact leads to different propagation delays, and consequently, delay imbalances for the two PUF routes. Therefore, due to routing constraints in a LUT of CPLD, we have implemented the stages by two independent LUTs as in [17], see Figure 5. To validate our concept, the design consists of an 8-bit arbiter PUF on the CPLD. Each stage is placed manually in an individual LAB on the CPLD to make the PUF chains symmetric. Due to very little delay differences between two chains, the arbiter can sample a meta-stable signal. Moreover, due to asymmetric length of data and clock lines, the delay between the outputs of the last stage and the inputs of the arbiter cannot be designed symmetrically. Hence, instead of using an arbiter, we readout the response by measuring the overall delays of both chains with the help of photonic emission analysis.

## 4 Measurement Approach

For completeness we present in this section two approaches to solve the underlying linear system of arbiter PUFs — first, the slightly more elaborate approach for MUX-based PUFs although it is unnecessary for our PoC implementation. Second, the related but simpler approach for our delay-based PUF implementation.

### 4.1 Optimized Measurement for ordinary MUX-based PUF Characterization

In a MUX-based arbiter PUF, each stage consists of four different propagation delays: two direct path delays and two switching path delays, see Figure 1. In order to completely characterize an $n$-stage arbiter PUF, all propagation delays of each stage have to be known, hence, 4n delays must be characterized in total. One conceivable way would be to naively measure all 4 propagation delays at all $n$ stages individually by moving the optical setup *over* both inputs and both outputs of each stage, and simply try both challenge states. However, this technique would require the movement of the chip and adjusting the focus for each movement. However, this process could be automated as well, but our measurement setup lacked this capability. As our setup has a very high spatial resolution, a precise aperture movement would be very time consuming, but eventually yield the $4n$ arbiter delays. While practically certainly feasible and also theoretically optimal, we can do much better in terms of physical measurement efforts. A more intelligent solution will simply try to measure the overall propagation delays of each PUF chain at the outputs of the very last stage for sufficiently many selected challenge combinations. As the overall delay at the outputs of the last stage is the sum of all $n$ delays in each stage, cf. additive linear model due to [13, 13], every measurement has to consider for every chosen challenge the complete propagation time of two distinct but possible paths — the upper output (D input to sampling flip-flop) and the lower output (C input to sampling flip-flop). If we denote by $r_i$ the resulting overall time of an individual challenge measurement, we conclude that we get an inhomogeneous system of linear equations

$$\mathbf{C} \cdot \boldsymbol{\delta} = \mathbf{r}$$

for our $4n$ unknowns $\delta_{i_a}, \delta_{i_b}, \delta_{i_c}$, and $\delta_{i_d}$ and the challenge matrix $\mathbf{C}$ with entries from $\{0, 1\}$ which encode the different valid paths through the arbiter chain. We call a path $\mathbf{c}_i \in \{0,1\}^{4n}$ *valid* if its respective challenge setting within $\mathbf{C}$ allows a full signal propagation of length $n$, i.e., until its very end. By induction the following is easy to see.

**Proposition 1.** *For an arbiter PUF of length $n \geq 1$ let $\mathbf{C}$ be the $(2^{n+1}) \times (4n)$ matrix consisting of all valid paths through the respective arbiter chain. Then* $\mathrm{rk}(\mathbf{C}) = 2n + 2$.

Seeing now that we have only $2n+2$ linear independent equations in $\mathbf{C}$, we need to generate the remaining $2(n-1)$ linear independent equations to completely solve our system in another way. Thus, we are forced to consider also partial valid paths instead of full propagation paths. Let $\mathbf{c}_i \in \{0,1\}^{4n}$ be a valid path; for integers $1 \leq u, v \leq n$ a vector of the form

$$(0, \ldots, 0, c_{4u}, c_{4u+1}, c_{4u+2}, c_{4u+3}, \ldots, c_{4v}, c_{4v+1}, c_{4v+2}, c_{4v+3}, 0, \ldots, 0) \in \{0,1\}^{4n}$$

will be called a *partial valid* path.

*Note 1.* For a partial valid path we will measure its signal time only from the inputs of arbiter stage $u$ until its output at stage $v$ and deliberately denote this partial time simply also by $r_i$.

Including such partial measurements $r_i$ (i.e. including measurements within the arbiter chain) and their corresponding paths $\mathbf{c}_i$ we also get by induction.

**Proposition 2.** *For an arbiter PUF of length $n \geq 1$ and its $2n+2$ valid paths (corresponding to the linear independent row vectors) there exist $2(n-1)$ appropriate partial valid paths such that their combined challenge matrix $\mathbf{C}$ has full rank $4n$.*

This Proposition implies that we only need $2(n-1)$ partial measurements which we classify with respect to $u$ and $v$ into three classes:

1. $u = 1$ and $1 \leq v < n$: Measurement begins at the inputs of the first stage and ends in the middle of the chain.
2. $1 < u, v < n$: Measurement starts at some inputs in the middle of the chain and also ends in the middle of the chain.
3. $1 < u \leq n$ and $v = n$: Measurement starts at the inputs in the middle of the arbiter chain and and ends after the last stage.

In order to keep the previously discussed physical measurement efforts minimal, it is therefore obvious to generate the missing linear independent equations out of group 1 or 3 — dependent on varying setup advantages. This completes our description of an optimized measurement for a classical MUX-based PUF with $n$ stages.

### 4.2 Simplified Measurement for delay-based PUFs

As we already pointed out in Section 2.1, we have $\delta_{i_a} = \delta_{i_d}$, and $\delta_{i_b} = \delta_{i_c}$ for their respective buffers. Moreover, as the two paths, i.e., the upper and the lower path are not crossing at all, in other words they are disjoint, we can consider them completely separately, see Figure 5. Towards this, let us consider the upper path and simply denote its $n$ unknown delays by $\delta_1, \ldots, \delta_n$. I.e., setting the respective $i^{\text{th}}$ challenge bit to 1 adds the delay $\delta_i$ to the overall complete signal propagation time which will be denoted by $r_j$ for the $j^{\text{th}}$ measurement from the first input until the last output — just through all $n$ stages. If we now define the distinguished variable $\Delta_{n+1}$ as the overall complete signal propagation time for setting all $n$ challenge bits to 0 we get the (already solved) linear system

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \Delta_1 \\ \Delta_2 \\ \vdots \\ \Delta_n \\ \Delta_{n+1} \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \\ r_{n+1} \end{pmatrix}$$

for which we simply require the measurements $r_i$, $i = 1, \ldots, n+1$. The lower path can be handled in an analog way, say $\mathbf{C}' \cdot \boldsymbol{\Delta}' = \mathbf{r}'$. Moreover, using the unit vectors $\mathbf{e}_i \in \{0,1\}^{n+1}$, $i = 1, \ldots, n+1$, we find that we get from

$$\mathbf{e}_i \cdot \boldsymbol{\Delta} - \mathbf{e}_{n+1} \cdot \boldsymbol{\Delta} \quad = r_i - r_{n+1}, \quad \text{and}$$

$$\mathbf{e}_i \cdot \boldsymbol{\Delta}' - \mathbf{e}_{n+1} \cdot \boldsymbol{\Delta}' = r'_i - r'_{n+1}$$

the two individual buffer delays $\delta_i$ and $\delta'_i$ of stage $i$ incurred by setting the $i^{\text{th}}$ challenge bit to 1. We thus conclude that we need only $2n+2$ "full path" measurements to completely characterize a delay-based PUF with $n$ stages.

## 5 Results

We have chosen the challenge 00000000 as the reference challenge for our measurements. In order to measure the effect of each challenge bit, we have tried the challenge combinations with hamming distance one to see the effect of each challenge bit individually. The enable signal was switched with a frequency of 4 MHz and the chip was supplied with 2.2 V. The optical emission of the PUF circuit reveals the position of each stage, see Figure 6. Moreover, the inputs and output of each stage for measurement can also be found on this emission image. In case of controlled PUFs, where no electrical access to challenges is available [8], comparing the optical emission of the PUF stages can also reveal the state of individual challenge bits. By changing each challenge bit, the emission pattern of each LE is changed, and therefore, the challenge can be read without any electrical access to it, see Figure 7. Therefore, the equations provided in Section 4 can still be used to characterize the PUF by finding challenges with hamming distance one from each other. We repeated the measurement 50 million cycles to capture enough number of photons for analysis. The reference challenge also has been measured multiple times during our experiments to compare the consistency of measurements. The measurement results of 8 challenge combinations compared to the reference challenge can be found in Figure 8. Positive timing difference means that the delay is decreased in comparison to reference challenge and vice versa. It can be seen that flipping the challenge bit from 0 to 1, makes in most cases both upper and lower chains faster. Moreover, the timing differences between both chains can also be found in the table. Based on the overall delay difference of two chains, the response can be predicted. In this case, if the timing difference between two chains is positive, the response is 1, otherwise the response is 0.

According to the measured values, we can predict the behavior of both chains for all other challenge combinations based on the linear additive model of the arbiter PUF. To prove the applicability of this model, we predicted theoretically the overall delay of both chains for a set of arbitrary challenge combinations, and then measured the timings in practice. For instance, the calculated timing difference between both chains for the challenge 00000111 is the sum of measured differences of challenges 00000001, 00000010 and 00000100, which is 195 ps.

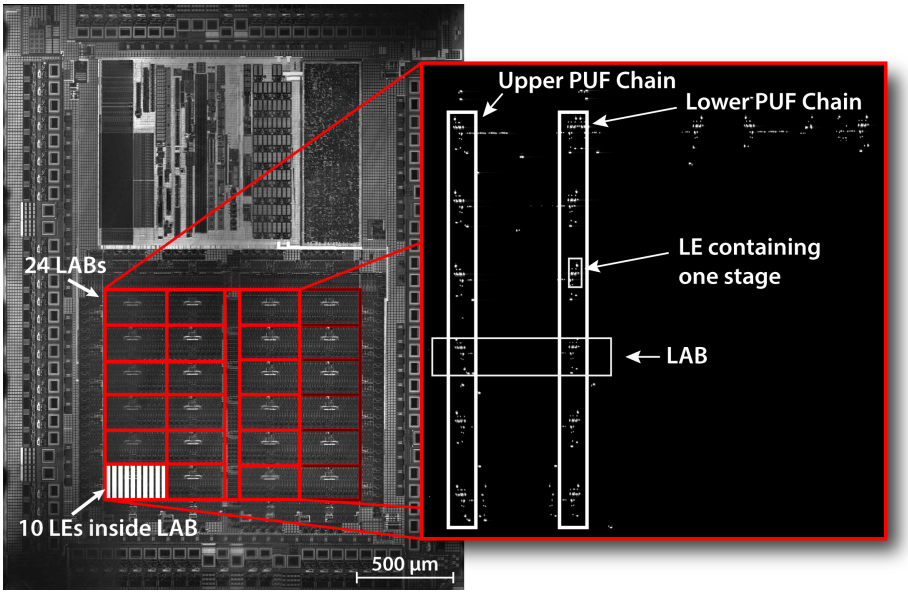



Fig. 6: The backside reflectance image acquired using a laser scan microscope (left). Inside the framed area, all programmable logic cells are located. The grid corresponds to the placement of 4 by 6 LABs with additional routing infrastructure in-between. Within each LAB, 10 LEs are located (only a single LAB is shown containing the LEs). Optical emission of the 8-bit arbiter PUF on the CPLD (right). Each stage is realized by two LEs in a LAB in parallel.

The measured value is 199 ps, with 4 ps deviation from the predicted value. However, the response can be clearly predicted as logical 1 due to large positive difference. Another example shows that by applying a set of challenges, such as 00100101, the timing difference between two chains will be quite small both in calculation and measurement. Hence, these combinations can drive the arbiter into a metastable condition, and the response will not be consistent. It can also be seen in the results that although the PUF is implemented symmetrically on the hardware, a set of challenge bits can have much more effect on the delay of the chain than others. For example, when the second challenge bit is flipped, large delay difference on the lower chain is observed. As it can be seen in Figure 8, by applying the challenge 10101010, four challenge bits are flipped from the reference challenge. Although the flipping effect of 4th, 6th and 8th bits are comparable to each other, the 2nd bit has much more effect that make the response prediction much easier. These *dominant* stages have more influence on the response than other stages, and make the response prediction easier. Therefore, finding these stages can potentially turn out a threat for arbiter PUFs.

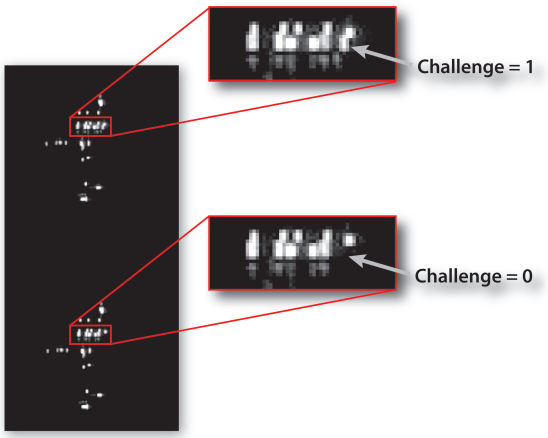



Fig. 7: Reading challenge bit from the emission image of each LE

## 6 Discussion

In order to obtain spatial orientation of the PUF circuit by the CCD detector, the chip has to be thinned. Thinning the silicon substrate from the backside of the chip can destruct the PUF. However, the InGaAs SAPD is still able to detect photons without thinning the substrate. Therefore, only one IC sample has to be thinned, if we want to apply the same approach on multiple IC samples. While our proof of concept implementation utilized a CPLD, the results are directly applicable to all classes of arbiter PUFs realized in CMOS. All CMOS devices are vulnerable to photonic emission analysis, as the transistors emit photons during switching. Therefore, the same measurement methodology can be applied to all platforms, such as FPGAs or Application Specific Integrated Circuits (ASICs).

Although our experiment was conducted with an 8-bit arbiter PUF, the same delay measurement technique can be applied to arbiter PUFs with higher number of stages. In comparison to machine learning attacks, our methodology requires far less challenges to predict the response. Furthermore, no response is required to physically characterize the PUF. Logistic regression classification model requires 2555 and 18050 CRPs for a response prediction rate of 99% for an 64-bit and 128-bit Arbiter PUF, respectively [24]. Our approach requires only the measurement of 65 challenges for 64-bit and 129 challenges for 128-bit. Moreover, XOR-arbiter PUFs with 9 parallel 64 and 128 stages are modeled with 200000 and 500000 CRPs, receptively, plus the power side channel information for a 95% response prediction rate [16]. In this case, our methodology requires only $9 \times 65$ and $9 \times 129$ challenges for 64-bit and 128-bit arbiter PUF, respectively. This shows that the number of required challenges in our approach increases only linearly with the increase of number of stages. Furthermore, having XOR at the end of multiple chains has no impact on the linearity of our approach. However, trying the same challenge more than one million times to capture enough

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Challenge | | 1<br>0<br>0<br>0<br>0<br>0 | 0<br>1<br>0<br>0<br>0<br>0 | 0<br>0<br>1<br>0<br>0<br>0 | 0<br>0<br>0<br>1<br>0<br>0 | 0<br>0<br>0<br>0<br>1<br>0 | 0<br>0<br>0<br>0<br>0<br>1 | 0<br>0<br>0<br>0<br>1<br>0 | 0<br>0<br>0<br>0<br>0<br>1 | 1<br>1<br>1<br>0<br>0<br>0 | 1<br>0<br>1<br>0<br>1<br>0 | 1<br>0<br>1<br>0<br>0<br>1 | 0<br>0<br>0<br>0<br>1<br>0 | 0<br>1<br>1<br>1<br>1<br>1 | 0<br>0<br>0<br>0<br>1<br>1 | 0<br>1<br>0<br>1<br>0<br>1 | 1<br>1<br>1<br>1<br>1<br>1 |
| measured Δt in ps | chain u | 43 | 79 | 48 | 63 | 29 | 76 | 39 | 76 | 174 | 179 | 181 | 127 | 313 | 217 | 356 | 510 |
| | chain l | 33 | -106 | 45 | 74 | 45 | 91 | 59 | 74 | -20 | 185 | 208 | 156 | 143 | 237 | 190 | 368 |
| | diff. | 10 | 185 | 3 | -11 | -16 | -14 | -20 | 3 | 195 | -6 | -27 | -29 | 170 | -20 | 166 | 141 |
| measured response | | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | **1** | **0** | **0** | **0** | **1** | **0** | **1** | **1** |
| calculated Δt in ps | chain u | | | | | | | | | 170 | 167 | 159 | 115 | 295 | 192 | 319 | 453 |
| | chain l | | | | | | | | | -28 | 168 | 182 | 150 | 132 | 224 | 162 | 314 |
| | diff. | | | | | | | | | 199 | -1 | -23 | -35 | 162 | -32 | 157 | 140 |
| calculated response | | | | | | | | | | **1** | **0** | **0** | **0** | **1** | **0** | **1** | **1** |

Fig. 8: Measurement results of challenge combinations with hamming distance one (the 8 combinations from the left). Measurement results of set of arbitrary challenge combination (the last 8 combinations from the right). The reference challenge is 00000000.

photons by the detector, is the disadvantage of this methodology. Besides, our attack requires direct physical access to the DUT, while it may not be required by modeling attacks.

Measuring the effect of each challenge takes approximately 12.5 seconds by supplying the chip with 2.2 V and enabling the PUF input with 4MHz frequency. Supplying the chip with 1.8 V, for example, reduces the number of emitted photons by a factor of 3, and the measurement time increases consequently by a factor of 3. However, we can increase the frequency to 100MHz to increase the number of emitted photons and to reduce the measurement time. Furthermore, immersion objectives or objective lenses with larger numerical aperture can be utilized to reduce the measurement time for each challenge to under 1s. Our physical characterization of an arbiter PUF can also find the dominant stages in the chain. Measuring a set of dominant stages can make the response prediction much easier. Therefore, this technique can help to improve the PUF behavior by designing and constructing more balanced routes and stages.

## 7 Conclusion

In this work, we demonstrated how photonic emission analysis from the backside of the chip can help us to physically characterize arbiter PUF. The experimental results with minimum number of measurements have shown that the arbiter PUF can be effectively characterized. The comparison between our approach and modeling techniques has shown that our methodology requires far less challenges than modeling attacks. Furthermore, our technique does not require any PUF

response. Although we carried out our experiments on a CPLD PUF implementation, the same methodology can be applied to other hardware implementations. As a result, it is revealed that the timing-based PUFs, specifically arbiter PUFs, are vulnerable to photonic emission analysis.

**Acknowledgements.** The authors would like to acknowledge the support of the German Federal Ministry of Education and Research in the project PhotonFX and the Helmholtz Research School on Security Technologies.

## References

1. Altera: MAX V Device Handbook. Altera Corporation, San Jose (2011)
2. Altera: Quartus II Web Edition Software (2013), http://www.altera.com/products/software/quartus-ii/web-edition/qts-we-index.html
3. Armknecht, F., Maes, R., Sadeghi, A., Standaert, O.X., Wachsmann, C.: A Formalization of the Security Features of Physical Functions. In: Security and Privacy (SP), 2011 IEEE Symposium on. pp. 397–412. IEEE (2011)
4. Boit, C.: Fundamentals of Photon Emission (PEM) in Silicon – Electroluminescence for Analysis of Electronic Circuit and Device Functionality. In: Microelectronics Failure Analysis: Desk Reference. p. 356 ff. ASM International (2004)
5. Delvaux, J., Verbauwhede, I.: Fault Injection Modeling Attacks on 65nm Arbiter and RO Sum Pufs via Environmental changes. Tech. rep., Cryptology ePrint Archive: Report 2013/619, 2013, https://eprint. iacr. org/2013/619 (2013)
6. Delvaux, J., Verbauwhede, I.: Side Channel Modeling Attacks on 65nm Arbiter PUFs Exploiting CMOS Device Noise. In: Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on. pp. 137–142. IEEE (2013)
7. Ferrigno, J., Hlaváč, M.: When AES Blinks: Introducing Optical Side Channel. Information Security, IET 2(3), 94 –98 (2008), http://dx.doi.org/10.1049/iet-ifs:20080038
8. Gassend, B., Clarke, D., Van Dijk, M., Devadas, S.: Controlled Physical Random Functions. In: Computer Security Applications Conference, 2002. Proceedings. 18th Annual. pp. 149–160. IEEE (2002)
9. Gassend, B., Clarke, D., Van Dijk, M., Devadas, S.: Silicon Physical Random Functions. In: Proceedings of the 9th ACM conference on Computer and communications security. pp. 148–160. ACM (2002)
10. Helfmeier, C., Boit, C., Nedospasov, D., Seifert, J.P.: Cloning Physically Unclonable Functions. In: Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on. pp. 1–6. IEEE (2013)
11. Krämer, J., Nedospasov, D., Schlösser, A., Seifert, J.P.: Differential Photonic Emission Analysis. In: Constructive Side-Channel Analysis and Secure Design, pp. 1–16. Springer (2013)
12. Lee, J.W., Lim, D., Gassend, B., Suh, G.E., Van Dijk, M., Devadas, S.: A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications. In: VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on. pp. 176–179. IEEE (2004)
13. Lim, D., Lee, J.W., Gassend, B., Suh, G.E., Van Dijk, M., Devadas, S.: Extracting Secret Keys from Integrated Circuits. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 13(10), 1200–1205 (2005)

14. Maes, R., Van Herrewege, A., Verbauwhede, I.: PUFKY: A Fully Functional Puf-based Cryptographic Key Generator. In: Cryptographic Hardware and Embedded Systems–CHES 2012, pp. 302–319. Springer (2012)
15. Maes, R., Verbauwhede, I.: Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In: Towards Hardware-Intrinsic Security, pp. 3–37. Springer (2010)
16. Mahmoud, A., Rührmair, U., Majzoobi, M., Koushanfar, F.: Combined Modeling and Side Channel Attacks on Strong PUFs. Tech. rep., Cryptology ePrint Archive: Report 2013/632, 2013, https://eprint. iacr. org/2013/632 (2013)
17. Majzoobi, M., Koushanfar, F., Devadas, S.: FPGA PUF using Programmable Delay Lines. In: Information Forensics and Security (WIFS), 2010 IEEE International Workshop on. pp. 1–6. IEEE (2010)
18. Merli, D., Schuster, D., Stumpf, F., Sigl, G.: Semi-invasive EM Attack on FPGA RO PUFs and Countermeasures. In: Proceedings of the Workshop on Embedded Systems Security. p. 2. ACM (2011)
19. Nedospasov, D., Schlösser, A., Seifert, J.P., Orlic, S.: Functional Integrated Circuit Analysis. Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on pp. 102–107 (2012)
20. Nedospasov, D., Seifert, J.P., Helfmeier, C., Boit, C.: Invasive PUF Analysis. In: Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on. pp. 30–38. IEEE (2013)
21. Oztiirk, E., Hammouri, G., Sunar, B.: Towards Robust Low Cost Authentication for Pervasive Devices. In: Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on. pp. 170–178. IEEE (2008)
22. Parusiński, M., Shariati, S., Kamel, D., Xavier-Standaert, F.: Strong PUFs and their (Physical) Unpredictability: A Case Study with Power PUFs. In: Proceedings of the Workshop on Embedded Systems Security. p. 5. ACM (2013)
23. Rankl, W., Effing, W.: Smart Card Handbook. Wiley, fourth edn. (2010)
24. Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S., Schmidhuber, J.: Modeling Attacks on Physical Unclonable Functions. In: Proceedings of the 17th ACM conference on Computer and communications security. pp. 237–249. ACM (2010)
25. Rührmair, U., Sölter, J., Sehnke, F.: On the Foundations of Physical Unclonable Functions. IACR Cryptology ePrint Archive 2009, 277 (2009)
26. Sadeghi, A.R., Visconti, I., Wachsmann, C.: Enhancing RFID Security and Privacy by Physically Unclonable Functions. Springer (2010)
27. Schlösser, A., Dietz, E., Frohmann, S., Orlic, S.: Highly Resolved Spatial and Temporal Photoemission Analysis of Integrated Circuits. Measurement Science and Technology 24(3), 035102 (2013)
28. Schlösser, A., Nedospasov, D., Krämer, J., Orlic, S., Seifert, J.P.: Simple Photonic Emission Analysis of AES. In: Cryptographic Hardware and Embedded Systems–CHES 2012, pp. 41–57. Springer (2012)
29. Škorić, B., Tuyls, P., Ophey, W.: Robust Key Extraction from Physical Uncloneable Functions. In: Applied Cryptography and Network Security. pp. 407–422. Springer (2005)
30. Skorobogatov, S.: Optical Fault Masking Attacks. In: Fault Diagnosis and Tolerance in Cryptography (FDTC), 2010 Workshop on. pp. 23–29. IEEE (2010)
31. Skorobogatov, S.P., Anderson, R.J.: Optical Fault Induction Attacks. In: Cryptographic Hardware and Embedded Systems-CHES 2002, pp. 2–12. Springer (2003)

32. Suh, G.E., Devadas, S.: Physical Unclonable Functions for Device Authentication and Secret Key Generation. In: Proceedings of the 44th annual Design Automation Conference. pp. 9–14. ACM (2007)
33. Tuyls, P., Batina, L.: RFID-tags for Anti-Counterfeiting. In: Topics in Cryptology–CT-RSA 2006, pp. 115–131. Springer (2006)