# No Place to Hide: Contactless Probing of Secret Data on FPGAs

Heiko Lohrke[1](✉), Shahin Tajik[2](✉), Christian Boit[1], and Jean-Pierre Seifert[2]

[1] Semiconductor Devices, Technische Universität Berlin, Berlin, Germany
lohrke@mailbox.tu-berlin.de, christian.boit@tu-berlin.de
[2] Security in Telecommunications, Technische Universität Berlin, Berlin, Germany
{stajik,jpseifert}@sec.t-labs.tu-berlin.de

**Abstract.** Field Programmable Gate Arrays (FPGAs) have been the target of different physical attacks in recent years. Many different countermeasures have already been integrated into these devices to mitigate the existing vulnerabilities. However, there has not been enough attention paid to semi-invasive attacks from the IC backside due to the following reasons. First, the conventional semi-invasive attacks from the IC backside — such as laser fault injection and photonic emission analysis — cannot be scaled down without further effort to the very latest nanoscale technologies of modern FPGAs and programmable SoCs. Second, the more advanced solutions for secure storage, such as controlled Physically Unclonable Functions (PUFs), make the conventional memory-readout techniques almost impossible. In this paper, however, novel approaches have been explored: Attacks based on Laser Voltage Probing (LVP) and its derivatives, as commonly used in Integrated Circuit (IC) debug for nanoscale low voltage technologies, are successfully launched against a 60 nanometer technology FPGA. We discuss how these attacks can be used to break modern bitstream encryption implementations. Our attacks were carried out on a Proof-of-Concept PUF-based key generation implementation. To the best of our knowledge this is the first time that LVP is used to perform an attack on secure ICs.

**Keywords:** FPGA security · Laser voltage probing · Physically unclonable function · Semi-invasive backside attack.

## 1 Introduction

Modern Field Programmable Gate Arrays (FPGAs) and programmable System on Chips (SoCs) are used nowadays in different critical applications. Since most FPGAs and programmable SoCs store their configuration in SRAM cells, they have to be configured in an untrusted field through bitstreams stored in an external non-volatile memory (NVM) upon each power-on. Due to the lack of protection against side-channel leakage in an adversarial environment,

H. Lohrke and S. Tajik— These authors contributed equally to this work.

B. Gierlichs and A.Y. Poschmann (Eds.): CHES 2016, LNCS 9813, pp. 147–167, 2016.
DOI: 10.1007/978-3-662-53140-2_8

the transmission of the bitstream (even in an encrypted format) can expose the design [23,30,31,46]. Furthermore, volatile Battery Backed RAMs (BBRAMs) and eFuses, which can be used to store the secret key for decryption of the bitstream, are unreliable and vulnerable to scanning electron microscopy (SEM) [46].

FPGA vendors always attempt to add more advanced countermeasures to their devices, to effectively mitigate physical attacks. While DPA vulnerabilities of the decryption cores can be solved by DPA-resistant IP cores and asymmetric authentication schemes, Physically Unclonable Functions (PUFs) can mitigate the insecurity of eFuses and BBRAMs [46]. Moreover, different physical sensors inside the FPGAs can monitor the environmental changes to detect glitching and fault injection attacks. However, a proper physical protection against semi- and fully-invasive attacks from the IC backside is still missing on these modern platforms.

There are good reasons for FPGA vendors to be less concerned about the security of the IC backside. First, the latest generations of SRAM-based FPGAs are manufactured with 20 nm technology and the next generation of FPGAs will be built with 16 and 14 nm technologies [13,19]. Yet, it has already been demonstrated that, even for larger FPGA technologies such as 45 nm and 60 nm, conventional semi-invasive attacks from the IC backside, such as Laser Fault Injection (LFI) [39] and Photonic Emission Analysis (PEM) [41], are onerous tasks. Therefore, such attacks cannot be scaled down efficiently along with the trend of shrinking transistor technologies. Second, FPGA vendors believe that integration of new storage solutions, such as PUFs, raises the security level of key storage against backside attacks [7,25,35], as no key is stored permanently on the chip to be read-out by the adversary.

**Our Contribution.** In this work we introduce a novel semi-invasive attack against FPGAs using a known failure analysis technique, called Laser Voltage Probing (LVP) [24]. We demonstrate how the attacker can use LVP and derivatives to locate circuitry of interest, such as registers and ring oscillators (ROs), by knowing or estimating the frequency of different operations. Estimation of aforementioned frequency characteristics can be achieved by either having knowledge of implementations or by performing power analysis in the frequency domain. Moreover, we explain how LVP enables us to probe different *volatile* and *on-die-only* signals and data streams on the chip without having any physical contact to the wires or transistors. Besides, with the help of LVP one can characterize high frequency signals, such as the output of ROs, which are used in RO PUFs and True Random Number Generators (TRNGs). For our practical evaluation, we consider a PUF in key generation mode inside an FPGA to decrypt the bitstream. The PoC implementation was realized on an FPGA manufactured in a 60 nm process technology. Due to lack of proper protection, we were able to perform our analysis from the IC backside. This work is presenting the first results to evaluate the potential of LVP for possible future attacks on small technologies, where conventional backside semi-invasive attacks, such as PEM and LFI, would require much more efforts.

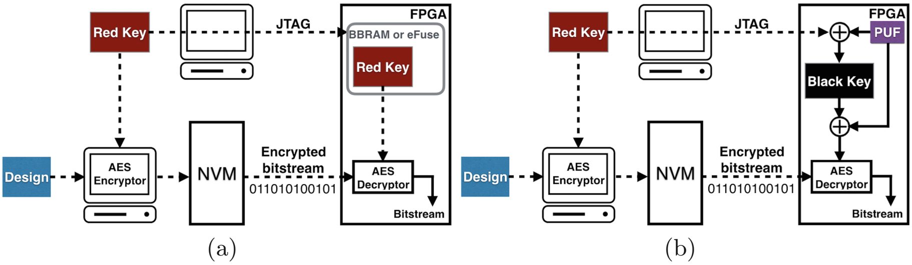


**Fig. 1.** (a) Bitstream encryption and decryption using a red key [46]. (b) Bitstream encryption and decryption using a black key, PUF key and red key [35].

## 2 Background

### 2.1 FPGA Security During Configuration

Bitstream encryption is a conventional solution to prevent the piracy of IPs during FPGA configuration. In this case a secret "red key" (i.e., an unencrypted key) is transferred to the FPGA in a safe environment, see Fig. 1(a). This key will be stored either in the Battery Backed RAM (BBRAM) or eFuses on the chip. At the same time, the application design is encrypted by the red key and stored in an external non-volatile memory (NVM). Each time the FPGA is powered up in the untrusted field, the encrypted bitstream is transmitted to the chip and it will be decrypted by the stored red key inside the chip. Although this technique raises the security of the bitstream transmission against interception, it has been shown that the decryption cores on different FPGAs, responsible for decoding the bitstream, are vulnerable to electromagnetic (EM) and differential power analysis (DPA) [23,30,31]. Moreover, the key storage technologies on FPGAs such as eFuses are vulnerable to semi-invasive attacks and can be read out with a scanning electron microscope (SEM) [46].

Utilizing updatable protected soft decryption cores and asymmetric authentication can defeat non-invasive side-channel attacks, such as differential power analysis (DPA) [35]. Moreover, Physically Unclonable Functions (PUFs) [15,34] can remedy the shortcomings of insecure storage in modern FPGAs [46]. Instead of storing the secret key in an insecure memory, PUFs exploit the manufacturing variability on identical devices to generate virtually unique secret keys for each device. Therefore, PUFs can be used for secure key generation and key obfuscation in an untrusted environment, where the adversary has access to the device and is able to launch a physical attack. In addition to key generation, PUFs can be utilized as unique identifiers to restrict access to FPGAs and prevent cloning and spoofing attacks [16,17,26,40].

PUF and DPA-resistant decryptors can be implemented either by dedicated logic inside the FPGA (i.e., hard cores) or by configuring the FPGA logic cells (i.e., soft cores). Although the principle of using PUFs for key obfuscation and DPA-resistant decryptors to defeat physical attacks are similar among different

FPGA vendors, the implementation details differ. In this work, we explain the red key wrapping technique using soft PUFs and soft decryptors, which is used by Xilinx SoCs [35]. The main idea is to generate a "black key" (i.e., an encrypted key, which in itself is useless to an attacker), to generate the secret red key on the fly during configuration. This black key can then be stored safely in an insecure NVM and the red key will only exist as volatile, internal-only data. The preparations for this technique are as follows. In the trusted field a boot loader containing the red key and a soft PUF IP is transferred into the volatile configuration SRAM of the FPGA. After the boot loader is loaded, the PUF is configured on the programmable logic of the device and its responses are used in conjunction with the red key to generate the black key [35], see Fig. 1(b). The black key generated in this way can only be converted back to the red key with the correct, chip-specific, internal-only PUF response (i.e., PUF key). In the untrusted field an encrypted first stage boot loader with the black key, the same soft PUF IP and a DPA-resistant decryption IP core is loaded into the device. The chip-specific PUF response is then used to unwrap the black key and generate the red key on the fly. Finally, the encrypted configuration bitstream is transferred to the device and will be decrypted by the red key inside the FPGA. In this way the decryption IP core can be updated against future side-channel analysis threats. Furthermore, the soft PUF in conjunction with the black key provides volatile, internal-only and updatable key storage, and therefore, the red key is in memory only during the configuration of the device.

## 2.2 Current PUF Implementations

Current FPGA market leaders have already started to integrate PUFs into their latest products [7,25,35]. Hard SRAM PUFs from Intrinsic-ID Inc. have already been integrated into the Microsemi SmartFusion2 and IGLOO2 FPGAs [7] and are going to be implemented on Altera Stratix 10 SoCs and FPGAs [25]. Moreover, Xilinx has patented a key generation technique based on hard RO PUFs which might be used in their next generation FPGAs and SoCs [45]. Currently, the Xilinx Zynq-7000 SoCs enables the user to implement soft PUF IP cores as well as DPA-resistant soft decryptor IPs to protect the red key during configuration [35]. Furthermore, selected Microsemi flash-based SmartFusion2 and IGLOO2 FPGAs can be utilized as a Root of Trust to transfer soft PUF IP cores to target SRAM-based FPGAs for secure authentication [26]. Soft PUFs can be purchased from third-party developers, such as Verayo Inc. [6], Intrisic-ID Inc. [4], Lewis Innovative Technology Inc. [5] and Helion Technology Limited. [3].

Since the implemented soft or hard PUFs inside of FPGAs are controlled PUFs, where a non-invasive electrical access to the challenges and responses of the PUFs is restricted by either physical or algorithmic countermeasures, most of the reported modeling [9,14,37] and semi-invasive [29,33,42,43] attacks in the literature are ineffective. In this case the unprocessed challenges can be transmitted with the first stage boot loader to the FPGA, which will be processed later on the device by non-linear functions and applied to the PUF. The response of the PUF will also be generated and processed inside the device and cannot be observed in a non-invasive way.

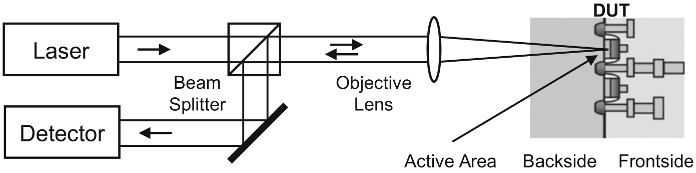


**Fig. 2.** Simplified illustration of LVP signal acquisition.

### 2.3 Laser Voltage Probing and Laser Voltage Imaging

Several techniques have been introduced into failure analysis to allow contactless probing of Devices Under Test (DUTs). One category of such techniques uses optical beams and is therefore, referred to as *contactless optical probing*. These techniques allow failure analysis engineers to probe electrical signals through the silicon backside and to also create 2D activity maps of active circuitry. Turnkey solutions for optical probing are readily available from different manufacturers, among them Hamamatsu Photonics, Checkpoint Technologies, DCG Systems (now part of FEI) and Semicaps. In the literature optical probing can be referred to as Laser Voltage Probing (LVP), Electro Optical Probing (EOP), Laser Timing Module (LTM) or Laser Time Probe (LTP). Acquisition of 2D activity maps is similarly referred to as Laser Voltage Imaging (LVI), Electro Optical Frequency Mapping (EOFM) or Signal Mapping Image (SMI). In this paper we choose to refer to waveform probing as Laser Voltage Probing (LVP) and to acquisition of 2D activity maps as Laser Voltage Imaging (LVI). Both techniques together will be referred to as LVx.

The actual technical realisation of LVx varies depending on the manufacturer, however, the basic principles remain the same. For optical probing as used in LVP a laser beam is focussed through the silicon backside, traverses the active device area, is reflected of, for instance, metal structures and leaves the device again through the silicon backside, see Fig. 2. The returning beam is then fed to an optical detector to measure its intensity. Usually near infrared (NIR) wavelengths are used to prevent the absorption of light by the silicon. Inside the active area the electrical parameters of the device, such as electrical fields and currents, lead to changes in the absorption coefficient and refractive index. Because of this, the optical beam intensity is altered either directly through absorption or in some cases indirectly through interference effects because of the changed refractive index. Empirical studies have shown, that a linear approximation is often sufficient to describe the relationship between the voltage at the electrical node and the reflected light signal. Therefore, the detector signal waveform recreates the electrical waveform from inside the device. This allows optical probing of electrical waveforms by just pointing the laser beam at the electrical node of interest. However, since the light modulation is very small (on the order of 100 ppm) the detector signal usually needs to be averaged while the device is running in a triggered loop to achieve a decent signal to noise ratio. As this is just a rough sketch of the principles of optical probing, readers interested in a detailed discussion of the underlying physical interactions are referred to [24] and the references mentioned therein.

On the other hand, optical frequency mapping, as used in Laser Voltage Imaging (LVI), can be seen as an extension to optical probing as explained above. In one typical LVI setup, the detector signal is not averaged but instead fed into a spectrum analyzer, which is set to some frequency of interest and zero span. Therefore, the spectrum analyzer effectively acts as a narrow frequency filter with adjustable bandwidth. Using galvanometric x/y mirrors the laser beam is then scanned across the device and the filter output of the spectrum analyzer is sampled for every scanned pixel. Afterwards, a PC with appropriate software is used to assemble the sampled frequency filter values into a 2D picture using a grey-scale representation. If an electrical node operates at the frequency of interest, it will modulate the light reflected of it with said frequency. This will in turn lead to a detector signal modulated with this frequency, which will be able to pass through the frequency filtering spectrum analyzer. Therefore all nodes operating at this frequency will show up as white spots in the LVI image. All nodes operating at a different frequency or areas which are not modulating the laser light will stay black. It should be noted that it is enough if some frequency component of the waveform present at the node can pass the frequency filter. Hence, this method can be used to detect nodes operating with arbitrary waveforms, as long as the first harmonic frequency or other strong frequency components of that waveform can be determined. As soon as the nodes of interest are found in this way, the galvanometric mirrors can be set to directly probe the waveform of one specific node with Laser Voltage Probing using a stationary beam within seconds. An advantage of LVI over LVP is, that for LVP waveform acquisition a loop trigger signal is always needed, whereas for LVI the device can be free-running.

In practice LVx systems are often incorporated into Laser Scanning Microscopes (LSMs). LSMs acquire optical images by scanning a laser beam across a sample and detecting the reflected light. They are therefore already equipped with scanning mirrors and an optical illumination and detection path, and thus, LVx systems can be used as an add-on.

## 3 Attack Scenario

We propose two LVP-based attacks against FPGAs during configuration. In the first attack scenario we demonstrate how the adversary can probe the red, black and PUF key using Laser Voltage Imaging (LVI). This allows the attacker to extract the red key, and therefore, enables her to decrypt the encrypted bitstream offline, which can lead to reverse engineering or cloning of the design. In the second attack, we will show how the attacker can characterize an RO PUF based on a combination of LVI, Laser Voltage Probing (LVP) and power analysis. Characterization of the individual oscillators of the RO PUF enables the attacker to model the PUF, and therefore, to clone its functionality. Knowing the *approximate* location of the key registers and the PUF components on the chip is the main assumption of our proposed attacks.

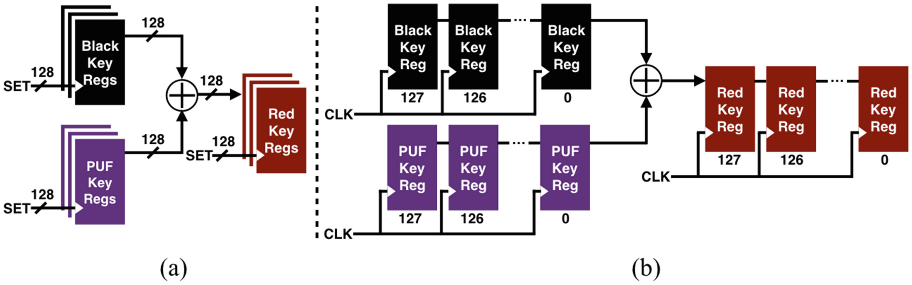


**Fig. 3.** (a) Parallel generation of the red key, (b) serial generation of the red key.

### 3.1 Key Extraction

The principle of key generation inside an FPGA has been discussed in Sect. 2.1. All three key values can be either shifted serially through a shift register or they can be loaded into the registers in parallel based on the implementation, see Fig. 3. We will first discuss the case, where the register values are loaded and processed in parallel. In this case the attacker can utilize LVI directly to extract all three values. As discussed in Sect. 2.3, LVI reveals nodes switching with a certain frequency, or more precisely, having certain frequency components. Therefore, to locate registers of interest, the attacker has to know a frequency or frequency component, which reveals the registers and is ideally data-dependent. Thus, she will need to take a look at the switching frequencies during red key generation. It is evident that after power-on all registers are first initialized to their default value by the reset circuitry. Following that, all black key registers are loaded in parallel and the PUF circuit is started. As soon as the PUF has finished generating its output, its values are also loaded onto the corresponding registers simultaneously. In a final step, the red key, which is now available at the XOR output, can be loaded onto all red key registers. Consequently, we can see that all register blocks of interest (black key, PUF key, red key) receive data — exactly once per power-on. This can be exploited to generate suitable frequency components by placing the device in a reset loop. In such a scenario, the first harmonic of the waveforms on these registers will be the reset frequency, as they change their states once per reset. If we now take a detailed look at the data dependency of these waveforms, we notice that there is a fundamental difference between registers carrying a zero bit and registers carrying a one bit. In Fig. 4 the waveforms of two registers receiving a one and a zero bit as well as the reset signal $RST$ are depicted. For the register receiving a one bit ($REG_A$) it is evident that the register starts at logic low level and then changes its state, as soon as the time needed for the preceding calculations ($T_{CALC}$) has elapsed. As soon as the reset input goes high, the register is reset and afterwards the power-on cycle is restarted once reset goes low again. Since we can expect $T_{CALC}$ to be constant for consecutive power-ons we can see that $REG_A$'s period will be $T_{RST}$ and we can expect its first harmonic to be at $1/T_{RST}$. For register $REG_B$,

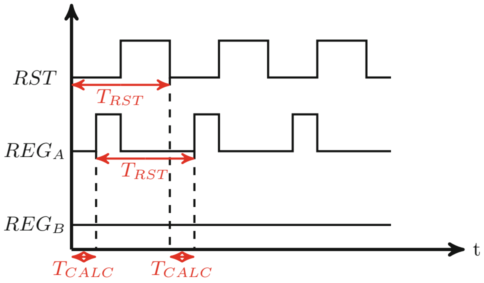


**Fig. 4.** Waveforms of the reset signal ($RST$) and two registers, receiving a one ($REG_A$) and a zero ($REG_B$) bit.

carrying a zero, the case is much simpler. $REG_B$ will not change its value at all, and therefore, will not to have any harmonics at the reset frequency. Thus the attacker can expect the registers carrying a one to modulate the reflected light with a first harmonic of $1/T_{RST}$. Registers carrying a zero are expected to not modulate the reflected light at all. The interaction will be the same for black key, PUF key and red key register blocks. Although $T_{CALC}$ will change for each register block, the first harmonic will still be at $1/T_{RST}$ for all of them. Therefore, to extract the register values the attacker can perform an LVI measurement on the register block of interest while setting the spectrum analyzer filter frequency to the reset loop frequency. If the LVI measurement is then grayscale encoded, registers carrying a one are expected to show up white while registers carrying a zero will remain black.

For the case of the serial implementation the situation is slightly different. Here the data will be processed bit by bit and the individual registers in the relevant register blocks will be connected together to form one shift register for each block. The data bits will then be shifted out of the black key and PUF key shift registers, passed through the XOR and shifted into the red key shift register. As a result, each individual register would show a different waveform depending on its position in the shift register and the actual data values. The waveforms of the individual registers would still have the reset frequency as their first harmonic, however, detecting the bit values can not be broken down to a simple black/white distinction as for the parallel case. Nevertheless, the attacker will still detect the registers of interest in an LVI image, although with varying signal strength. Since she is able to determine the precise register locations this way, she can then move on to directly probe the waveforms of individual registers using Laser Voltage Probing (LVP). This might be a tedious task, depending on the number of bits, however, she should be able to find the first register of each shift register this way. As soon as the first register of the red key shift register is found, the attacker can extract the key from its waveform, as the complete key gets shifted through this register during calculation.

Therefore, using just LVI or a combination of LVI and LVP the attacker should be able extract the key data regardless of the chosen implementation.

### 3.2 RO PUF Characterization

In order to characterize an RO PUF, the attacker has to be able to measure the frequencies of the ring oscillators (ROs) with high precision. PUF characterization enables the attacker to clone the RO PUF. If the attacker can estimate the frequency of the ROs at least approximately, she will be able to directly take an LVI measurement at that specific frequency. This can be achieved by electromagnetic or power analysis in the frequency domain. Using one of these methods the attacker will not be able to observe individual RO frequencies, but rather the superposition of all running ROs. Nevertheless, if she performs an LVI measurement at this approximate frequency with a large enough bandwidth, she should be able to see the nodes of the ROs in the LVI image. As soon as the nodes of the ROs are identified in this way the attacker can proceed to probe them individually. However, since the ROs are free-running, there is no trigger signal available for waveform acquisition, and therefore conventional Laser Voltage Probing (LVP) will fail. Yet, the attacker is free to connect the reflected light signal of the LVP directly to the spectrum analyzer of the LVP/LVI setup while probing one individual RO. Through setting the spectrum analyzer to conventional frequency sweep mode she will then be able to see the spectrum of the reflected light signal. As the laser beam will just probe one node of one RO, the waveform of that specific RO will be modulated onto the reflected light signal. Thus, the precise frequency of that individual RO will be visible on the spectrum analyzer. This will eliminate the need for a trigger signal and allow the attacker to characterize that specific RO. She can then proceed to characterize the whole RO PUF by pointing the laser at the nodes of the remaining individual ROs.

## 4 Setup

### 4.1 Device Under Test

The samples used for our experiments were Altera Cyclone IV FPGAs with part number EP4CE6E22C8N manufactured in a 60 nm process [8]. In this sample all Logic Elements (LEs) contain 4-input Lookup Tables (LUTs) and a dedicated register. The device contains 6272 Logic Array Blocks (LAB) with 16 LEs each. We chose the 144 pin TQFP package in order to simplify the sample preparation. The first step of preparation was the removal of the exposed ground pad on the backside of the package. The samples were then thinned by an Ultratec ASAP-1 polishing machine to a remaining silicon thickness of 25 µm. However this step would not have been necessary. Modern ICs only have to be depackaged and are sufficiently thin as-is for NIR analysis, just leading to a lower signal level if used directly. In the second step, the prepared samples were inversely soldered to a custom PCB. Bond wires originally leading to the exposed ground pad were then reconnected using silver conductive paint. A JTAG connection was used for configuring the FPGA after power-on.

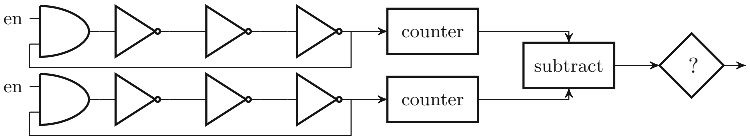


**Fig. 5.** A simplified schematic of an RO pair in the RO PUF construction. After a predefined period of oscillation, the states of both counters are compared to each other to generate a binary response.

### 4.2 PoC FPGA Implementation

For our Proof-of-Concept we have implemented an RO PUF and a red key (See Sect. 2.1.) calculation. To make the design less complex, we have connected the outputs of the ROs directly to individual counters, see Fig. 5. Each RO in our design has been realized with 21 inverters. All components of the ROs and the counters have been placed manually inside the FPGA using the Altera Quartus II integrated development environment. The LEs in every RO were placed as close as possible, directly next to each other. We have emulated the rebooting and configuration of the FPGA by adding a reset signal to our implementation. The black key and PUF key in our design have 8-bit length. As discussed in Sect. 3, unwrapping the black key can be carried out either in a parallel or serial way. Hence, for the first scenario, we have implemented the red key generation by XORing all values of the black key with the PUF key in parallel, see Fig. 3. For the second scenario, we have realized two shift registers for the black key and PUF key, where those values are shifted serially to an XOR gate and the result is shifted into the red key registers.

### 4.3 Measurement Setup

The core of our optical setup (Fig. 6(a)) is a Hamamatsu "PHEMOS-1000" laser scanning microscope. The PHEMOS is equipped with an optical probing and frequency mapping option. This option consists of a highly stable laser light source (Hamamatsu C12993), a Laser Voltage Probing and Laser Voltage Imaging preamplifier (Hamamatsu C12323), an Agilent "Acqiris" digitizer card and an Advantest U3851 spectrum analyzer. The laser light source emits radiation at 1319 nm which is input into the optical path, deflected by galvanometric mirrors and then focussed through an objective lens into the backside of the DUT. The reflected light from the DUT is passed on to a detector and the detector signal is fed into the preamplifier. The signal leaving the preamplifier can then either be routed to the spectrum analyzer for LVI or to the digitizer card for acquisition of LVP waveforms. For all measurements shown in this paper a Hamamatsu 50x/0.76NA lens with silicon thickness correction was used. The approximate laser power with this lens on the DUT is 50 mW for 100 % laser power. Additionally 5x and 20x objective lenses were used for navigation. The whole optical setup is controlled by a PC running the PHEMOS control software.

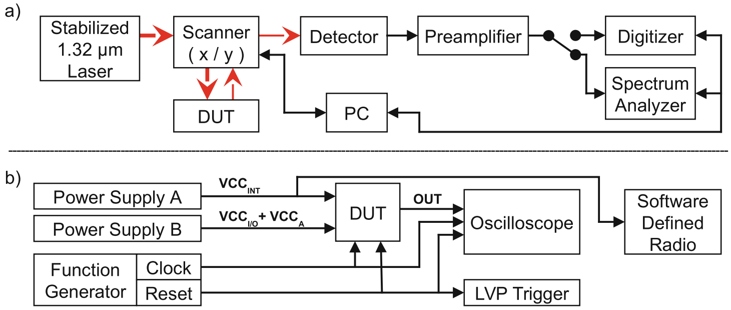


**Fig. 6.** Optical (a) and electrical (b) setup block diagram

Our electrical setup (Fig. 6(b)) is as follows: Two power supplies are connected to the DUT. The first one (Agilent E3645A) provides $V_{CCINT} = 1.2V$ (internal logic), the second one (Power Designs Inc. 2005) supplies $V_{CCIO} = 2.5V$ (I/O) and $V_{CCA} = 2.5V$ (PLL and analog). All voltages were within recommended levels [8]. A Rigol DG4162 two channel function generator produces clock and reset signals which are fed into the DUT. The clock and reset signals as well as an auxiliary DUT output are also connected to a LeCroy WaveMaster 8620 A oscilloscope for testing and control purposes. The reset signal is furthermore fed into the Laser Voltage Probing (LVP) trigger input. To be able to conduct basic power analysis in the frequency domain, a Software Defined Radio (SDR) is AC-coupled to the $V_{CCINT}$ power rail. The SDR is an inexpensive USB dongle which uses a Realtek RTL2832U chipset and a Rafael Micro R820T tuner. For controlling the SDR, free and open source software is used. "Gqrx" [2] is used for measurements with a spectral bandwidth below 2.4 MHz and the python script "RTLSDR Scanner" [1] for higher bandwidths.

## 5 Results

### 5.1 Key Extraction

For our first measurements we used a parallel implementation as described in Sect. 4.2. The black key was set to 10101101, the PUF key to 11011011 and the resulting red key was 01110110. The measurement was conducted with 5 MHz reset frequency and 50 MHz clock. Both were 50 % duty cycle and 2.4 V high level and 0 V low level. The laser power was 10 % and the pixel dwell time 3.3 ms. The filter frequency for LVI was set to the reset frequency and the bandwidth to 300 Hz.

First, we performed an overview LVI image of an area containing all three register blocks, see Fig. 7(a). There are clearly nodes whose waveforms contain frequency components at the reset frequency, and therefore, give rise to an LVI signal. Since it is known in which LABs the black key, PUF key and red key registers have been placed, it is now straight forward to assign the blocks to their

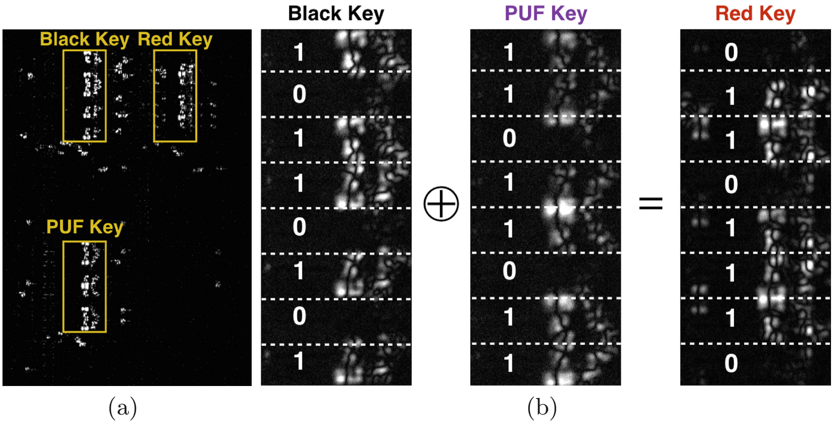


**Fig. 7.** LVI images of the parallel implementation. (a) All three register blocks taking part in the red key calculation. (b) Detail view of the individual register blocks. Dashed lines denote the LE boundaries. Each LE is approx. 6 µm in height.

respective keys. To analyze the data content of the registers, a higher resolution is helpful. The measurement has thus been repeated on each register block while applying a scanner zoom. The resulting LVI images can be seen in Fig. 7(b) and the expected behaviour discussed in Sect. 3.1 is observed. As expected, registers carrying a zero do not contribute to the LVI signal while registers carrying a one can clearly contribute. We can see that there are slight differences in the appearance of the nodes from measurement to measurement, which are probably due to focus drift. Nevertheless, we can observe that the attacker is easily able to extract the relevant values of the black key, PUF key and red key directly from these LVI images. For the serial implementation we used the same basic measurement setup. However, the reset signal and LVI frequency were modified to be 1 MHz, as the serial implementation needs more clock cycles to execute. The reset duty cycle was set to 58 % as a makeshift trigger delay, causing only full bits to show up in the result before reset assertion. The laser power was increased to 15 % and the pixel dwell time decreased to 1 ms. Following that, an LVI image of the red key register block was taken, which is shown in Fig. 8. It is evident that there is no simple black/white data dependency, as discussed in Sect. 3.1. Still, we can see a difference in signal strength for the registers, with the ones at the top giving less signal than the ones at the bottom. To get a rough idea of which points could be promising for Laser Voltage Probing (LVP) we used a fast Fourier transform calculator to analyze the amplitude of the first harmonic component for different expected waveforms. We observed that for our case of one to eight bits shifted with a comparatively large reset "dead time" following, the waveforms with more bit shifts gave us a stronger first harmonic component. Our conclusion was therefore that the lower half area was the most promising to probe. Direct probing of the lower-half registers was successful and revealed the lowest register to be the "shift-in" register. However, it was noticed that

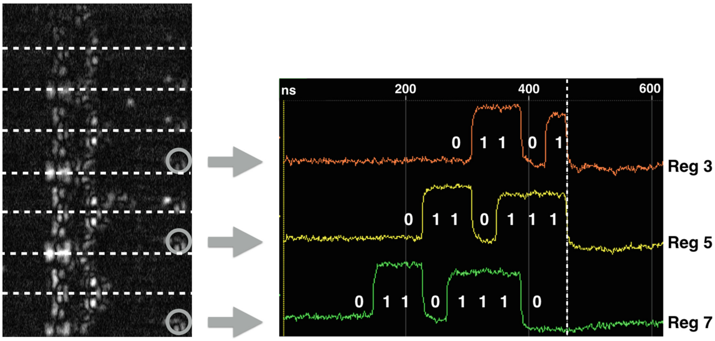
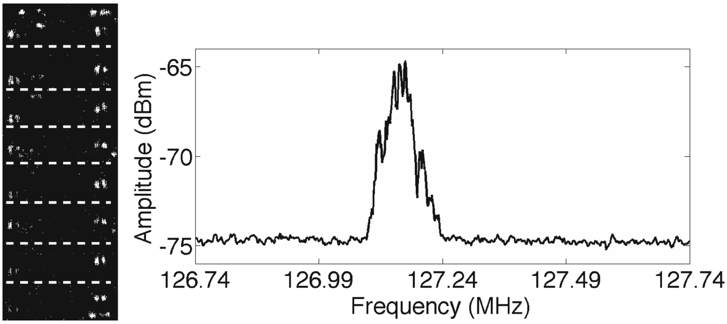


**Fig. 8.** LVI image of the red key register block and probed waveforms for the serial implementation. Reset assertion is marked by a dashed vertical line.

waveforms with a better signal to noise ratio could be acquired on the locations right of the actual register area. We assume that these locations are associated with routing and therefore the signal has already been buffered before reaching them. Furthermore, these locations are more isolated signal-wise which also leads to a better signal waveform. Hence, the final measurements were carried out on these locations for the shift-in register and two other registers further down the signal path. The resulting waveforms can be seen in Fig. 8. It is obvious that the red key can be extracted from the lowest LVP waveform of the shift-in register by an attacker. We acquired further waveforms while setting the integration number down to 100.000 loops, which is the current limit in the PHEMOS software, and were still able to distinguish the bit states easily. Therefore, we expect this approach to work with even less loop counts, as soon as the limit is removed from the software.

### 5.2 RO Characterization

For characterisation of the ring oscillators (ROs) we used the approach discussed in 3.2. In this section we will demonstrate the frequency measurement for one of the ROs. We first used the Software Defined Radio (SDR) to get a rough estimation for the LVI frequency by taking a look at the superposition of all RO frequencies in the spectral domain on the power rail. By slight adjustments of this estimate we were then able to create LVI overview images of the LEs forming the different ROs, one of which is depicted in Fig. 9(a). The parameters used for this LVI measurement were: 127.3539 MHz spectrum analyzer filter frequency, 60 % laser power, and 0.33 ms pixel dwell time. The ROs showed much more short term frequency fluctuations than the previously used conventional clock sources. Therefore, the LVI filter bandwidth had to be set to 100 kHz to account for the more widespread RO spectrum. After being able to identify the nodes of interest inside the LEs in this way, the beam was held stationary on one of them and the preamplified light detector signal was fed into the spectrum analyzer. The spectrum analyzer was then configured to show



(a) (b)

**Fig. 9.** (a) LVI image of 8 LEs of an RO, each approx. 6 µm in height. Dashed lines denote the LE boundaries. Each LE shows multiple potential probing locations. (b) LVP spectrum of the same RO.

the spectrum of this signal, which was modulated by the RO waveform present at the electrical node. For this measurement the laser power was set slightly higher, to 73 %, the spectrum analyzer frequency span to 1 MHz, resolution bandwidth to 30 kHz and video bandwidth to 10 Hz. The resulting spectrum in Fig. 9(b) shows the RO frequency approximately 10 dBm above the noise floor. Thus, the attacker is able to determine the current RO frequency precisely using only contactless optical probing methods. It should be noted that the resolution bandwidth mentioned before is not the resolution to be expected for the frequency measurement. As the attacker will only be interested in the average frequency of the RO, she is free to use multiple frequency sweeps to get a smooth spectrum and determine its peak value. The frequency of this peak value will then deliver the average frequency with a precision only depending on the number of averaged sweeps. By analysing the average frequency acquired this way it can be seen that the RO frequency was shifted by approximately 0.15 % when the laser power was increased from 60 % to 73 %. As long as the individual ROs are probed in the same way with the same laser power, this should not lead to problems for the attacker. Since the important question for the attacker is just which RO is faster, characterizing the RO PUF will still be successful if she takes care to probe all ROs in the same way, generating the same shift. Nevertheless, we will discuss this aspect in detail in Sect. 6.

# 6 Discussion

## 6.1 Locating the Registers and IP Cores on the Chip

As mentioned in Sect. 3, knowing the approximate location of the key registers and PUF IP core is the main assumption of our proposed attacks. Different scenarios can be considered to understand how realistic this assumption is.

As discussed in Sect. 2.1, the soft PUF IP cores, black key and their placements are transmitted in the first stage boot loader. If the first stage boot loader or Boot0 is not encrypted, the attacker can intercept the boot loader on the board and gain knowledge about the configuration of the PUF and the red and black key registers. For instance, the Microsemi Root of Trust solution [26] permits either the transfer of unencrypted or encrypted first stage boot loaders to the target SRAM-based FPGA. If the boot loader is encrypted, it will be decrypted by the hard dedicated AES core inside the target FPGA. While in the unencrypted case the boot loader can be easily intercepted, for the encrypted case DPA vulnerabilities of dedicated AES cores might be used to extract the encryption key and decrypt the boot loader [23,30–32]. However, in the case of asymmetric authentication as used by Xilinx SoCs, it is much harder for the attacker to expose the boot loader configuration [32]. Because of the authentication, the attacker cannot launch a DPA attack against the hard AES core and therefore might not be able to decrypt the first stage boot loader.

If the first stage boot loader cannot be intercepted, the attacker has to have access to the used IP cores prior to the attack. Though difficult, it is conceivable that the adversary can get access to the IP cores via an insider or by posing as a potential customer to IP core suppliers. Having the IP cores, the attacker can synthesize the PUF on an identical FPGA model and analyze the design either in the IDE (if no obfuscation is used) or by looking at the generated bitstream to find the circuitry of the interest.

If the attacker cannot get access to the IP cores, the attack will be more difficult due to the unknown location of the circuitry of interest. In this case, if the utilized soft PUF is an RO PUF, one could launch the attack proposed in Sect. 3.2 to find the ROs and the counters connected to them on the chip. The location of the RO PUF can then be a reference point to localize other parts of the design inside the FPGA. Furthermore, one can estimate the operational frequency of different registers to apply LVI and localize the related registers individually on the chip. After a successful localization of the key registers, the attacker can extract data from them by LVP/LVI based on the implementation (See Sect. 5.1). In the case of a parallel implementation, if the key registers are naively implemented in the right order (i.e., from LSB to MSB), the attacker can easily extract the key by using LVI. Otherwise, if the keys are latched in an obfuscated way, the attacker can only read the state of the permuted registers and might not find the right order of the registers to assemble the key. For a serial implementation, if the order of the registers is obfuscated, the attacker can probe all registers to find the one through which the whole key is shifted.

The proposed attacks to key registers can in principle also be applied, if a hard PUF and a hard AES are in use. In this case, the attacker has to reverse-engineer the ASIC configuration circuit of the FPGA to locate the circuitry of interest. Although the search space for the region of interest might be reduced, the attacker has to probe and reverse-engineer more compact and dense ASIC circuits in comparison to FPGA logic cells, which might be challenging.

### 6.2 Feasibility and Scalability of the Attack

The process technology of FPGAs and programmable SoCs, which are supporting partial reconfiguration for soft PUF implementation, are equal to or smaller than 60 nm. Since our LVI and LVP experiments have been carried out on an FPGA with 60 nm technology, the question of the applicability of the same technique on smaller technologies might be raised. The real size of the transistors is normally 7 to 8 times larger than the nominal technology node [18]. Besides, the size of the LEs and the routing (intra and inter LEs) of FPGAs is much larger than the size of the transistors, see Fig. 7. Hence, the optical resolution requirements for data extraction are much less severe than for probing individual transistors. Based on our measurements, the LE height in an Altera Cyclone IV is about 6 $\mu$m. The theoretical expected resolution of our laser spot is approximately 1 $\mu\text{m}^2$. Thus, optical probing should still be possible on an LE approx. six times smaller. It is worth mentioning that for LVP and LVI typical FPGAs are an advantageous target, as multiple transistors close together will carry the same waveform in an LE.

There are also solutions for increasing the optical resolution of LVP and LVI techniques. For instance, one can use solid immersion lenses (SILs) to get 2 to 3 times better resolution, which already enables *single transistor* probing at 14 nm [18]. Moreover, lasers with shorter wavelengths (e.g., in the visible light spectrum) can be used to further increase the resolution [10,12]. However, in the latter case, the substrate of the chip has to be thinned to 10µm or less to prevent the absorption of the photons.

Meanwhile, it is still interesting to understand why other backside semi-invasive attacks, such as PEM or LFI, have limited efficiency on small technologies in comparison to LVP and LVI. In the case of PEM, the photon emission rate is proportional to the core voltage of the chip. However, the core voltage of technologies smaller than 60 nm is too low [41] and the attacker therefore has to integrate over a large number of iterations to capture enough photons for analysis. LFI attacks on the other hand target mostly single memory cells, which requires the system used for the attack to be able to resolve single transistors on the chip.

### 6.3 Tamper Evidence

Tamper evidence is believed to be one of the main advantages of PUFs [27]. In other words, it is assumed that semi-invasive and fully-invasive attacks on the PUF implementation alter the challenge-response behavior of the PUF, and therefore, the secret information is lost. Tamper-evidence against fully-invasive attacks is experimentally verified only for optical and coating PUF so far [36,47]. However, the core of most soft and hard PUFs are *intrinsic* PUFs (i.e., delay-based PUFs and memory-based PUFs) [27]. Unfortunately, for these constructions limited information on tamper-evidence is available in the PUF-related literature. Fortunately, results on constructions similar to delay-based PUFs can be found in the failure analysis literature. For instance, it has been reported that mechanical stress from depackaging and substrate thinning have negligible effects on the absolute and relative frequencies of ring oscillators (ROs) [11]. In another experiment, it has been shown that removing most of the bulk silicon, down to the bottom of the n-wells, does not alter the delays of the inverter chains [38]. Additionally, without affecting the challenge-response behavior of the PUFs, different successful semi-invasive attacks have been reported on silicon intrinsic PUF instances in the literature [20,29,33,43,44]. On the other hand, PUF developers do their best to mitigate the noisy response of the PUF by different error correction techniques [22,28]. Therefore, if few CRPs are changed by the physical tampering, they will be corrected by such error correction techniques. Based on these results, depackaging the chip and thinning the substrate does not destruct the target PUF.

Although passive semi-invasive attacks do not affect the behavior of the PUF, the laser beam in our proposed attack can change the temperature of the transistors. Temperature variations have transient and reversible effects on the delay and frequency of the inverter chains in arbiter PUFs and RO PUFs. In our experiments, a shift of frequency has been observed while performing LVI and LVP on the ROs. However, the attacker is still able to precisely characterize and measure the frequencies of the ROs by performing LVI and LVP, if she takes care to probe all ring oscillators under the same conditions. If the attacker is not able to fulfill this requirement, she might also probe the registers of the counters which are connected to the RO output. Assuming the counters or other circuitry connected to the RO PUFs are located far enough away she will be able to mount her attack without influencing the ROs. Finally she might take measurements of one individual RO frequency for different laser powers and extrapolate from that to the frequency for zero laser power. Therefore, a precise physical characterization of the RO PUF is certainly feasible.

### 6.4 Countermeasures

Silicon light sensors have been proposed to detect the photons of the laser beam. However, in our experiments we have used a laser beam which has a longer wavelength than the silicon band gap. Hence, no electron-hole pairs will be generated by the laser photons. A silicon photo sensor is therefore unlikely to trigger.

A potential algorithmic countermeasure can be randomization of the reset states of the registers for the parallel implementation. As a result, the simple black/white data distinction (see Sect. 3.1) would be severely impeded, as there now would be switching activity during the reset loop on all registers. For the serial case, a randomization of the relation of the outer reset signal to the internal reset signal would destroy the needed trigger relationship and make waveform probing on the registers impossible. Another simple countermeasure includes the obfuscation of the key registers by randomizing their order, see Sect. 6.1.

Finally, the ROs in a ring oscillator network with virtually equal frequencies can be placed in different areas of the FPGA. Using LVP will then slightly shift the frequencies of ROs which are in or close to the probed area. Hence, the frequency deviation of these ROs in comparison to the mean frequency of all

ROs can be used to raise an alarm. Similarly, delay-based PUFs might be useful as sensors, if their elements are placed in different regions of the chip.

## 7 Conclusion

In this paper, we have proposed novel semi-invasive attacks from the IC backside using LVP and LVI techniques. We have demonstrated that these techniques can be potentially used against modern FPGAs and programmable SoCs during configuration. Based on these considerations, it becomes apparent that replacing the eFuses or BBRAMS with controlled PUFs does not raise the security level of key storage as high as one would expect in the first place. Even recent controlled stateless PUF constructions [22] are vulnerable to contactless probing. Moreover, while the size of the transistors is shrinking, novel inexpensive failure analysis techniques are developed to debug and probe nanoscale manufactured circuits in a semi-invasive and contactless way. It is worth mentioning that much less time is required for optical contactless probing of different signals than for conventional techniques, such as FIB microprobing [21]. Using our approach the amount of time needed to probe multiple nodes is on the order of minutes while for FIB microprobing it will be on the order of days. Furthermore, it is obvious that our attack technique has the potential to directly probe the bitstream after on-chip decryption, circumventing all security measures in place. However, there are several requirements for probing such a large amount of data and finding a suitable probing location in the much smaller and denser ASIC area, which might not be fulfilled by a standard LVP setup. Nevertheless, we strongly believe that future generations of FPGAs remain vulnerable to contactless probing, if proper protections or countermeasures for the IC backside are not implemented.

**Acknowledgements.** This research was supported by the German Federal Ministry of Education and Research in the project Photon FX$^2$ and by the Helmholtz Research School on Security Technologies. We would also like to acknowledge Hamamatsu Photonics for support. We gratefully thank Andreas Eckert and Helmar Dittrich at TU Berlin for sample and PCB preparation.

## References

1. Ear to Ear Oak. http://eartoearoak.com/software/rtlsdr-scanner/. Accessed 6 June 2016
2. Gqrx SDR. http://gqrx.dk. Accessed 6 June 2016
3. Helion Technology Limited. http://www.heliontech.com. Accessed 6 June 2016
4. Intrisic-ID Inc. https://www.intrinsic-id.com. Accessed 6 June 2016
5. Lewis Innovative Technology Inc. http://lewisinnovative.com. Accessed 6 June 2016
6. Verayo Inc. http://www.verayo.com. Accessed 6 June 2016
7. White Paper: Overview of Data Security Using Microsemi FPGAs and SoC FPGAs. Microsemi Corporation, Aliso Viejo, CA (2013)

8. Altera: Cyclone IV Device Handbook. Altera Corporation, San Jose (2014)
9. Becker, G.T.: The gap between promise and reality: on the insecurity of XOR arbiter PUFs. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 535–555. Springer, Heidelberg (2015)
10. Beutler, J.: Visible light LVP on bulk silicon devices. In: 41st International Symposium for Testing and Failure Analysis, 1–5 November 2015. ASM (2015)
11. Boit, C., Kerst, U., Schlangen, R., Kabakow, A., Le Roy, E., Lundquista, T., Pauthnerb, S.: Impact of back side circuit edit on active device performance in bulk silicon ICs. In: International Test Conference. vol. 2, p. 1236 (2005)
12. Boit, C., Lohrke, H., Scholz, P., Beyreuther, A., Kerst, U., Iwaki, Y.: Contactless visible light probing for nanoscale ICs through 10 μm bulk silicon. In: Proceedings of the 35th Annual NANO Testing Symposium - NANOTS 2015, pp. 215–221 (2015)
13. Davidson, A.: WP-01220-1.1: A New FPGA Architecture and Leading-Edge FinFET Process Technology Promise to Meet Next-Generation System Requirements. Altera Corporation, San Jose (2015)
14. Ganji, F., Tajik, S., Seifert, J.-P.: Why attackers win: on the learnability of XOR arbiter PUFs. In: Conti, M., Schunter, M., Askoxylakis, I. (eds.) TRUST 2015. LNCS, vol. 9229, pp. 22–39. Springer, Heidelberg (2015)
15. 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)
16. Guajardo, J., Kumar, S.S., Schrijen, G.-J., Tuyls, P.: FPGA intrinsic PUFs and their use for IP protection. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 63–80. Springer, Heidelberg (2007)
17. Güneysu, T., Markov, I., Weimerskirch, A.: Securely sealing multi-FPGA systems. In: Choy, O.C.S., Cheung, R.C.C., Athanas, P., Sano, K. (eds.) ARC 2012. LNCS, vol. 7199, pp. 276–289. Springer, Heidelberg (2012)
18. von Haartman, M.: Optical fault isolation and nanoprobing techniques for the 10nm technology node and beyond. In: 41st International Symposium for Testing and Failure Analysis, November 1–5, 2015. ASM (2015)
19. Hansen, L.: White Paper WP470: Unleash the Unparalleled Power and Flexibility of Zynq UltraScale+ MPSoCs. Xilinx, Inc., San Jose, CA (2015)
20. Helfmeier, C., Boit, C., Nedospasov, D., Seifert, J.P.: Cloning physically unclonable functions. In: 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 1–6. IEEE (2013)
21. Helfmeier, C., Nedospasov, D., Tarnovsky, C., Krissler, J.S., Boit, C., Seifert, J.P.: Breaking and entering through the silicon. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer Communications Security, pp. 733–744. ACM (2013)
22. Herder, C., Ren, L., van Dijk, M., Yu, M.D.M., Devadas, S.: Trapdoor computational fuzzy extractors and stateless cryptographically-secure physical unclonable functions. IEEE Trans. Dependable Secur. Comput. **2016**(99), 1–1 (2016)
23. Hori, Y., Katashita, T., Sasaki, A., Satoh, A.: Electromagnetic side-channel attack against 28-nm FPGA device. In: Pre-proceedings of WISA (2012)
24. Kindereit, U., Woods, G., Tian, J., Kerst, U., Leihkauf, R., Boit, C.: Quantitative Investigation of laser beam modulation in electrically active devices as used in laser voltage probing. IEEE Trans. Device Mater. Reliab. **7**(1), 19–30 (2007)
25. Lu, T., Kenny, R., Atsatt, S.: White Paper WP-01252-1.0: Stratix 10 Secure Device Manager Provides Best-in-Class FPGA and SoC Security. Altera Corporation, San Jose, CA (2015)

26. Luis, W., Richard Newell, G., Alexander, K.: Differential power analysis countermeasures for the configuration of SRAM FPGAs. In: IEEE Military Communications Conference, MILCOM 2015–2015. pp. 1276–1283. IEEE (2015)
27. Maes, R.: Physically Unclonable Functions: Constructions: Properties and Applications. Springer, Heidelberg (2013)
28. Maes, R., van der Leest, V., van der Sluis, E., Willems, F.: Secure key generation from biased PUFs. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 517–534. Springer, Heidelberg (2015)
29. 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)
30. Moradi, A., Barenghi, A., Kasper, T., Paar, C.: On the vulnerability of FPGA bitstream encryption against power analysis attacks: extracting keys from xilinx virtex-II FPGAs. In: Proceedings of the 18th ACM Conference on Computer and Communications Security. pp. 111–124. ACM (2011)
31. Moradi, A., Oswald, D., Paar, C., Swierczynski, P.: Side-channel attacks on the bitstream encryption mechanism of altera stratix II: facilitating black-box analysis using software reverse-engineering. In: Proceedings of the ACM/SIGDA International Symposium on Field Programmable Gate Arrays. pp. 91–100. ACM (2013)
32. Moradi, A., Schneider, T.: Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series, COSADE 2016, Graz, Austria, 14 April 2016
33. Nedospasov, D., Seifert, J.P., Helfmeier, C., Boit, C.: Invasive PUF analysis. In: 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 30–38. IEEE (2013)
34. Pappu, R., Recht, B., Taylor, J., Gershenfeld, N.: Physical one-way functions. Science **297**(5589), 2026–2030 (2002)
35. Peterson, E.: White Paper WP468: Leveraging Asymmetric Authentication to Enhance Security-Critical Applications Using Zynq-7000 All Programmable SoCs. Xilinx, Inc., San Jose (2015)
36. Ravikanth, P.S.: Physical one-way functions. Ph.D. thesis, Massachusetts Institute of Technology (2001)
37. Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S., Schmidhuber1, J.: Modeling attacks on physical unclonable functions. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. pp. 237–249 (2010)
38. Schlangen, R., Leihkauf, R., Kerst, U., Lundquist, T., Egger, P., Boit, C.: Physical analysis, trimming and editing of nanoscale IC function with backside FIB processing. Microelectron. Reliab. **49**(9), 1158–1164 (2009)
39. Selmke, B., Brummer, S., Heyszl, J., Sigl, G.: Precise laser fault injections into FPGA BRAMs in 90 nm and 45 nm feature size. In: 14th Smart Card Research and Advanced Application Conference - CARDIS 2015 (2015)
40. Simpson, E., Schaumont, P.: Offline hardware/software authentication for reconfigurable platforms. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 311–323. Springer, Heidelberg (2006)
41. Tajik, S., Dietz, E., Frohmann, S., Dittrich, H., Nedospasov, D., Helfmeier, C., Seifert, J.P., Boit, C., Hübers, H.W.: Photonic side-channel analysis of arbiter PUFs. J. Cryptol. 1–22 (2016). doi:10.1007/s00145-016-9228-6
42. Tajik, S., Dietz, E., Frohmann, S., Seifert, J.-P., Nedospasov, D., Helfmeier, C., Boit, C., Dittrich, H.: Physical characterization of arbiter PUFs. In: Batina, L., Robshaw, M. (eds.) CHES 2014. LNCS, vol. 8731, pp. 493–509. Springer, Heidelberg (2014)

43. Tajik, S., Ganji, F., Seifert, J.P., Lohrke, H., Boit, C.: Laser fault attack on physically unclonable functions. In: 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), IEEE (2015)
44. Tajik, S., Nedospasov, D., Helfmeier, C., Seifert, J.P., Boit, C.: Emission analysis of hardware implementations. In: 2014 17th Euromicro Conference on Digital System Design (DSD), pp. 528–534. IEEE (2014)
45. Trimberger, S.M.: Copy protection without non-volatile memory. US Patent 8,416,950 (2013)
46. Trimberger, S.M., Moore, J.J.: FPGA security: motivations, features, and applications. Proc. IEEE **102**(8), 1248–1265 (2014)
47. Tuyls, P., Schrijen, G.-J., Škorić, B., van Geloven, J., Verhaegh, N., Wolters, R.: Read-proof hardware from protective coatings. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 369–383. Springer, Heidelberg (2006)