Noname manuscript No.
(will be inserted by the editor)

Extensive Laser Fault Injection Profiling of 65 nm FPGA

Jakub Breier · Wei He · Shivam Bhasin · Dirmanto Jap · Samuel Chef · Hock Guan Ong · Chee Lip Gan

Received: date / Accepted: date

Abstract Fault injection attacks have been widely investigated in both academia and industry during the past decade. In this attack approach, the adversary intentionally induces computational faults in the security components of the integrated circuit (IC) for deducing the confidential information processed or stored inside the device. However, the internal architecture of real-world devices is typically unknown to the attacker and the insufficient information about the device internals often cannot satisfy requirements of a practical fault injection attack.

In this paper, we target Field Programmable Gate Array (FPGA) that is widely used in hardware security applications. By analyzing the faulty outputs of implemented algorithms, the scale of logic arrays and the sensitive logic cells can be precisely profiled. Using the outcome of this work, practical attacks can be significantly accelerated, without a need of time-consuming chip-scale injection scan. In addition, the observed fault models are compatible with most of the previously proposed fault models for differential or algebraic fault attacks (DFA/AFA). Moreover, a low-cost and highly-sensitive logic-level countermeasure for predicting the laser fault injection attempt is described, which can be applied into any digital IC with a minimal overhead. This paper is an extension of the paper entitled "Comprehensive Laser Sensitivity Profiling and Data Register Bit-Flips for Cryptographic Fault Attacks in 65 nm FPGA," presented at SPACE'16 conference. This version contains an extended related work, covers chip preparation in more details, discusses compatibility with cryptographic fault injection attacks, and presents a countermeasure against laser profiling.

Keywords Cryptographic Fault Attack · Laser Fault Injection · FPGA

J. Breier, D. Jap and S. Bhasin
Physical Analysis and Cryptographic Engineering
Temasek Laboratories at Nanyang Technological University
Singapore
E-mail: {jbreier,djap,sbhasin}@ntu.edu.sg

W. He
Shield Lab, Central Research Institute
Huawei International Pte. Ltd.
Singapore
E-mail: hewei48@huawei.com

S. Chef, H.G. Ong and C.L. Gan
School of Materials Science and Engineering
Temasek Laboratories at Nanyang Technological University
Singapore
E-mail: {csamuel,hgong,clgan}@ntu.edu.sg

1 Introduction

Modern Field Programmable Gate Arrays (FPGAs) and programmable Systems on Chip (SoCs) come with interesting features, like rich logic resources, real-time reconfiguration, high-density memories, clock managers, environment sensors, etc. Owing to such features and low time-to-market, FPGAs are being deployed in variety of applications. FPGAs also find wide applications in security-critical domains due to constantly evolving protection requirements like aerospace, defense etc. However, like other devices, FPGAs are also vulnerable to physical attacks, i.e., side-channel attacks [18], fault attacks [9], and probing [3].

Side-channel attacks (SCA) are passive and they exploit unintentional physical leakages, while probing tries to read out sensitive values directly from the circuit [19]. Fault attacks stay in between SCA and probing by operating the target device in a non-friendly environment and exploiting secrets from the faulty behavior. The most common fault analysis technique in

the context of cryptography is the Differential Fault Analysis (DFA) [7] and the Algebraic Fault Analysis (AFA) [14]. For instance, from AES, DFA can extract the secret key by a single well-located fault [34]. This tampering or erroneous behavior can be accomplished in several ways, which are widely classified as global or local. Global fault injections are, in general, low-cost techniques which create disturbances on global parameters like voltage and clock sub-system, etc. The resultant faults are more or less random in nature and the adversary might need repetitive injections to obtain exploitable faults. On the other hand, local injection techniques, like laser or electromagnetic injections, are more precise in terms of fault locations. This precision requires more expensive equipment and more preparation efforts.

Laser Fault Injection (LFI) falls into optical fault injection methods. It is a semi-invasive local perturbation technique, which requires decapsulation of the target device, followed by injection of a high intensity laser. The injection can be performed either through the frontside or the backside of the target chip. However, because of the dense metal wires covering the active logic layer, it is highly challenging to realize a successful fault perturbation from the frontside.

An alternative to laser method is the electromagnetic injection (EMI [27]) which uses a tiny EM probe with an intense transient pulse or a harmonic emission to (a) upset logic values in storage cells; (b) slow down the signal transmission to cause a set-up time violation in flip-flops or faulty timing in the internal clock generator [22]; (c) bias critical logic, e.g., key generation PUF [23]. However, the generated EM field is difficult to be restricted only to the point-of-interest, so the accuracy of EMI is still comparatively lower than LFI.

In this paper, the LFI on a commercial 65 nm FPGA is conducted by using a diode pulse laser on its substrate (backside). A fault injection-based laser sensitivity profiling of the exemplary FPGA is performed. We report successful data register bit flips in logic arrays. We localize interesting logic within these blocks, and sketch the laser sensitivity regions to demonstrate that the high-precision bit-flips in fundamental logic cells of the FPGA can be achieved by using a laser with μm-scale spot size. The presented results and the derivatives certify the feasibility of realizing bit-level fault injections in complex cryptographic algorithms on nanoscale FPGAs or programmable SoCs.

Our Contributions. This work presents the following improvements over the state-of-the-art. It:

- proposes a new methodology for laser sensitivity profiling of FPGAs, ranging from the global resource array to the slice flip-flops. Our method can be practically applied to a wide spectrum of FPGA devices.
- discusses the optical property of the silicon circuit under laser and details the mechanical chip preparation.
- reports precise bit-flip faults exclusively to specific flip-flops in the logic resource(s) instead of the configuration memory faults inside the FPGAs.
- realizes fault models in FPGA that are compatible with almost all the proposed differential/algebraic fault analysis (DFA/AFA) attacks on unprotected cryptographic primitives.
- discusses the possibilities of counteracting dual-rail or parity protected cryptographic primitives.
- presents a low-cost and efficient countermeasure targeting security modules of any digital IC, for foreseeing the on-going laser/EM fault injection attempt with extremely low overhead.

The rest of this paper is organized as follows. Sec. 2 discusses previous work and outlines our contributions. In Sec. 3, the related work about optical properties on silicon, chip preparation and configuration are presented. The profiling of laser sensitivity on chip and analysis methodologies are described in Sec. 4. Experimental results and further discussions are detailed in Sec. 5. Countermeasure against laser fault injection is proposed in Sec. 6. Finally, conclusions are drawn in Sec. 7.

2 Related Work

Many techniques have been proposed in the previous literature for disturbing values processed and stored in ICs [15,1,28,29,13,10]. In general, results on microcontrollers show high degree of repeatability, mainly because of the stable clock and a possibility to predict the instruction order. Precision depends on the used CMOS technology and the size of the effective laser spot. Additionally to memory disturbances, it is also relatively easy to disturb the instruction execution on these devices, leading to instruction skip or alteration faults. Previous papers about fault injections on FPGAs mostly aim at memory disturbances both on configuration memory of SRAM FPGAs and data Block RAM [26,12,31]. Some of the works are briefed as follows.

Pouget et al. [26] proposed a laser platform for evaluating the sensitivity of SRAM-based FPGAs, where the test targets are the FPGA configuration memory bits, instead of the algorithmic data. They successfully injected single and multiple bit flips into configuration

memory of a commercial FPGA manufactured on 1.5 μm technology.

Canivet et al. [12] conducted an attack on a protected AES implementation by using a laser with 20 μm spot size, targeting a 1.5 μm FPGA. Their results show that probability to flip a '1' is greater than the probability of flipping a '0'. Also, they stated that the most vulnerable components within the CLB are the look-up-table (LUT) contents and the internal multiplexers.

Selmke et al. [31] presented a precise bit-level manipulations in BRAM for two different FPGAs, with 90 nm and 45 nm transistor sizes. The spot size of their laser was 4 μm, allowing comparatively higher precision faults on Spartan-3A and a bit lower precision on Spartan-6, where vulnerable areas for different bits were overlapping. Still, they could produce bit sets/resets in the latter case, only the success rate was lower.

The fault injection into the configuration memory of SRAM FPGAs intrinsically incurs the alterations on logic functions or routings, and hence leads to permanent circuit malfunction until the device is reconfigured with a new bitstream. The faults are typically found and analyzed by a *readback* of the bitstream from the device after each fault injection to be compared with the unaffected *golden* sample [2,20], in order to figure out the affected tiles on the logic array. The comparison efficiency is low and static, and furthermore, the method is becoming challenging to apply to newer FPGAs with more obscure bitstream formats.

Lohrke et al. [21] test CPLDs manufactured with 180 nm technology by using a high-end Hamamatsu PHEMOS-1000 laser scanning microscope. In their experiment, they show how to localize AND and XOR gates and apply this method in order map the location of a ring oscillator circuit. Later [33] they show how to attack physically unclonable functions by using this method.

Another direction in disturbing FPGAs is a bitstream fault injection. Swierczynski et al. [32] show malicious bitstream modifications of Xilinx Spartan-6 and Virtex-5, attacking AES. However, as authors have mentioned, in newer FPGAs, bitstream encryption is strengthened authentication, which can prevent such bitstream fault injection. Our method, on the other hand, does not have any assumptions on bitstream security, since it is applied directly on the logic components.

Some previous works are summarized in Tab. 1 and compared with this work. The comparison is drawn in terms of platform (μC, FPGA, ASIC), technology node (Tech.), fault target (RAM, logic, flip-flop), chip position (front-side, back-side), fault precision (bit, random), and a purpose of the fault injection.

3 Chip Preparation and Device Configuration

For modern FPGAs, two package styles are typically applied to encapsulate the naked dies. The first is the `bonded-wire` package (or frontside) in which the metal layer is placed up and the chip substrate is facing down to the PCB board. On the contrary, `flip-chip` package (or backside) places the substrate up and metal layers down. Due to the metal layer placed above the active logic layer, laser injection can hardly affect the logic cells (active transistor layer) below. In this work, we target a 65nm Virtex-5 FPGA (LX50T) with a flip-chip package on Digilent's *Genesys* board. To allow effective laser impact on the internal logic, we have pre-processed the FPGA chip by thinning down the substrate layer, using a mechanical solution. This section explains the laser effects on silicon, sample preparation, and the description of the device under test.

3.1 Pulsed Laser Interaction with Silicon

The generation of carriers in semiconductor material by photoelectric effect has been used for decades in various fields such as failure analysis and defect localization [25], single event effect testing for space applications [11] and, as detailed in Sec. 2, security analysis.

When a pulsed laser irradiates silicon devices, two main mechanisms may occur:

- Single photon - Linear absorption (SPA). The photons have enough energy to induce a direct jump of the electrons from the valence band to the conduction band. The energy of the photons is bigger than the material bandgap in that case.
- Two photons - Non linear absorption (TPA). The free carriers generation results from the quasi simultaneous absorption of two photons.

The dominant process will be qualified by the wavelength of light and the pulse duration. Generation of free carriers by SPA requires a wavelength shorter than the silicon bandgap ($\approx$ 1100 nm with undoped silicon). TPA has a quadratic relationship with the irradiance, meaning that a bigger number of carriers are generated compared to SPA. In addition, it happens in a smaller volumes than SPA, providing resolution enhancement. One of the drawbacks is that triggering and detecting the effect can be more complex. Furthermore, TPA requires high peak power pulses achieved with a femtosecond laser which can be difficult to integrate to the test set-up. More details about SPA and TPA can be found in [11]. In silicon, with pulses of duration within picosecond range or longer, and at the wavelengths shorter than 1100 nm, SPA will be the dominant mechanism.

Table 1: State of the art for laser fault injection.

Work	Platform	Tech.	Target	Fault Model	Position	Purpose
Dutertre et al.[15, 1, 29]	μC	350nm	SRAM	byte	Front	Attack
Courbon et al.[13]	ASIC	90nm	FlipFlops	bit	Back	Attack
Breier et al. [10]	μC	350nm	Register	bit	Back	Attack
Pouget et al. [26]	FPGA	150nm	CLB/BRAM	random	Back	Reliability
Canivet et al. [12]	FPGA	150nm	Logic	random	Back	Attack
Selmke et al.[31]	FPGA	90/45nm	BRAM	bit	Back	Attack
This Work	**FPGA**	**65nm**	**Flip-Flops**	**bit**	**Back**	**Attack**

Once carriers are generated, if no electric field exists, charges will recombine without further effect. On the other hand, when there is a high electric field, like in a reverse bias junction, carriers surviving prompt recombination will drift and establish a transient current. The latter can have important consequences on the device behavior such as upsets, latch-up, etc.

In a modern integrated circuit, the density and the number of metal layers forbids an irradiation from the frontside of the chip. When injecting photocurrent from the backside, it is mandatory to use a wavelength that can propagate further enough through the substrate and reach the sensitive volume. As a consequence, wavelengths close to the bandgap are commonly used: absorption is limited while still triggering photoelectric effect.

Spatial resolution is another factor to consider when choosing the laser wavelength. The spot size measured at $(1/e^2)$ of the maximum intensity is linked to the wavelength by the following equation:

$$2\omega_0 = \frac{4\lambda}{\pi NA}, \tag{1}$$

where ω_0 is the beam waist, λ is the wavelength and NA is the numerical aperture of the objective. In this equation, it appears that a smaller spot size is induced either by a higher numerical aperture or a shorter wavelength, so the shorter the better from the resolution point of view.

As a summary, laser wavelength needs to be shorter than bandgap wavelength to generate free carriers but not too short to limit absorption by the substrate. For this reason, a laser wavelength of 1064 nm is used in this work. While seeking for resolution enhancement, backside application of visible wavelength have been reported in other field of work [6], but it requires to thin the substrate down to few micrometers. Such thickness is even more complex to reach using mechanical tools when the device under test is soldered on a testboard.

3.2 Sample Preparation of Virtex-5

As detailed in the beginning of this section, the Virtex-5 device was mounted on a Genesys testboard. Removing the part from the board to prepare it for the backside analysis and then solder it again may result in the damaging of the device. Thus, it was safer to prepare it still mounted on the testboard. As it is a flip-chip package, sample preparation from the top could be achieved. The compound was first removed using laser decapsulation until the metal heat-sink plate was revealed. The metal plate was then removed with tweezers to expose the silicon substrate. Before being diced and each sample individually packaged, silicon wafers are usually polished during the manufacturing process. The substrate surface quality is mirror-like, enabling IR inspection from the backside.

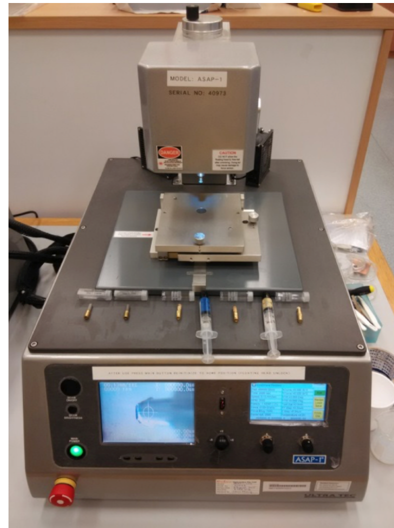


Fig. 1: Ultra Tec ASAP-1 polishing machine.

Therefore, in sample preparation, once the device is cleaned with chemicals to remove glue attaching the heat-sink, the circuit can already be observed from the backside. However, if the doping is high, absorption can limit the image quality. This is also an issue for fault injection as part of the incident light is absorbed, resulting in higher energy requirements to induce upsets. In addition, die warpage leads to a non-uniformity of the substrate. Refraction of the light beam on non-planar surface induces a poorer image quality.

The thinning of substrate aims to mitigate all these issues. For this experiment, it has been achieved with the *Ultra Tec ASAP-1* mechanical processing system (Fig. 1). The process involves two main steps: milling,

Fig. 2: ASAP-1 tools. From left to right: Diamond tool, Xylem tool and Xybove tool.

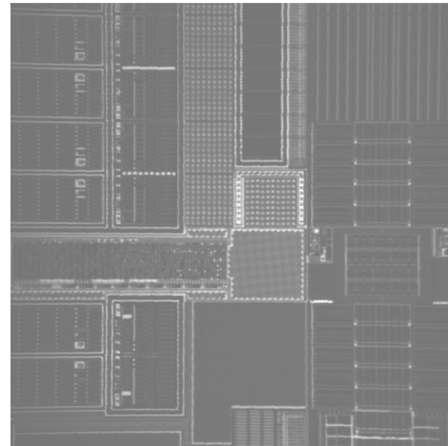
to reach the desired thickness, and polishing, to achieve a mirror-like surface quality. The later minimizes optical losses at the silicon/air interface, providing a better image quality. Depending on the step, tools of different material are used. For instance the milling of the substrate is done with a diamond tool while polishing involves Xylem and Xybove tools (Fig. 2).

Before machining, the substrate was estimated to be $\approx 300\ \mu m$ thick. After processing, it was reduced to approximately $\approx 130\ \mu m$. The estimation was performed using IR imaging and measuring the difference of focus level between the metal layers and the substrate surface. Fig. 3 shows difference in image quality of the sample before and after substrate thinning, by using IR laser imaging and 50× magnification. We can clearly see the difference in image contrast , especially in the blocks in the top-right corner.

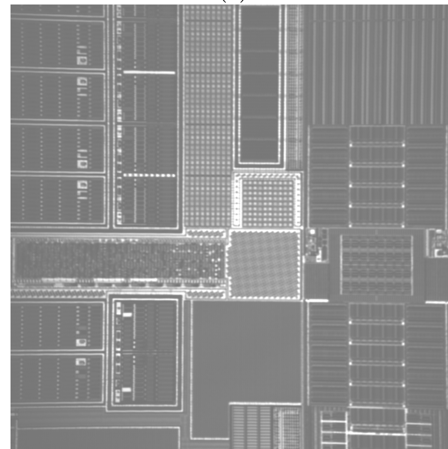
As mentioned before, it is possible to achieve thinner substrate but it is at the expenses of the device reliability. Indeed, it would induce higher mechanical constrains that can generate cracks. Such thickness is of interest for the use of high numerical aperture lenses or shorter operating wavelengths. With the current test setup, such objectives were not used and the laser wavelength was fixed to 1064 nm. As a conclusion, a thickness of 130 μm offered a good trade-off between energy maximization and keeping the device functional on the board.

3.3 Device Under Test and Configuration

The target device, Virtex-5 FPGA (LX50T), consists of 12 metal layers, manufactured in 65 nm technology in a 1136-pin flip-chip BGA package. The device provides 3,600 CLB (7,200 slices) deployed in 12 clock regions. Each slice contains 4 6-input look-up tables (LUTs) and 4 flip-flops. A number of BRAMs, digital clock mangers (DCMs), phase-locked loops (PLLs) and DSPs are located in columns of the logic resource array. A system monitor together with its temperature and power supply sensors are situated in the center of the die. Fig. 4 (left) illustrates the basic architecture of the selected



(a)



(b)

Fig. 3: Virtex-5 FPGA (a) before- and (b) after- substrate thinning.

device. The CLB structure in Xilinx FPGA contains 2 slices, together with the routing channel to a switchbox, as sketched in Fig. 4 (right).

The focal plane of the laser beam is critical for impacting the logic elements that are deployed under substrate. Due to the unrevealed bottom device information and the unknown dopant density in silicon that hinders the laser focalization, we had to empirically calibrate the focal plane to the active CLB layer relying on the number of generated faults, as an indicator, in a preliminary chip scan. As aforementioned, a diode pulse laser with a wavelength of 1064 nm was selected due to its superior penetration into silicon. The spot size of the chosen laser with a 5× lens was around $60 \times 14\ um^2$. The output power of the laser could be adjusted with an embedded attenuator with 1% precision step from 0 to 100% of its full power strength (10 Watt). The entire setup for performing fault injection experiments is depicted in Fig. 5.

Importantly, our experiments show that only the very central part of the laser beam spot is powerful

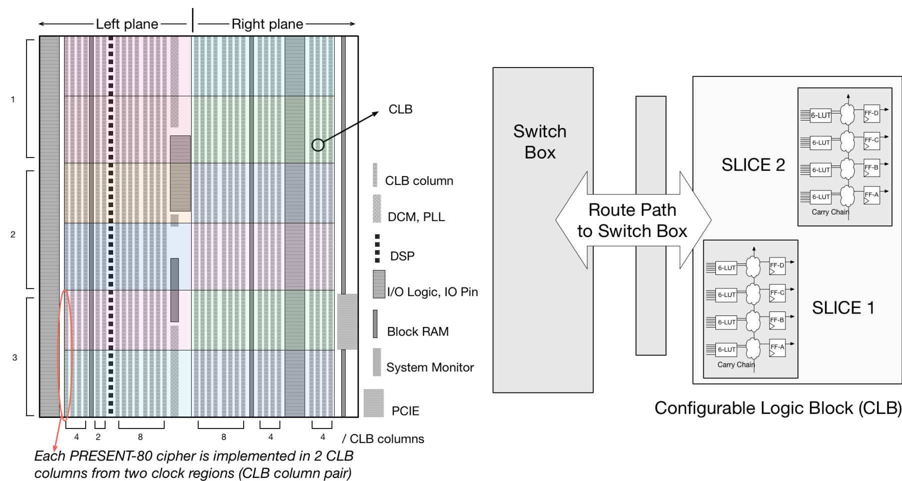


Fig. 4: Simplified architectural views of the target FPGA and CLB cell.

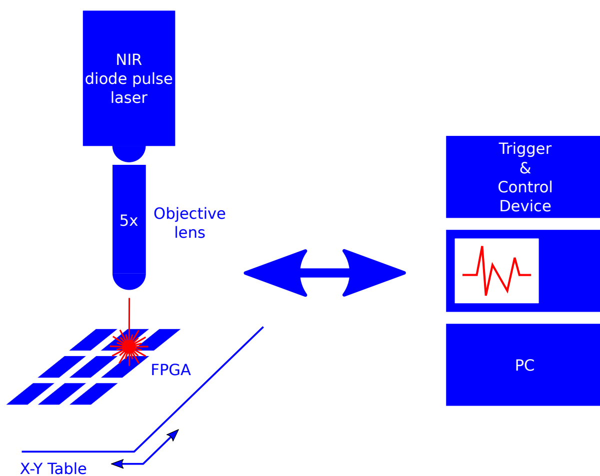


Fig. 5: Laser setup used for the experimental fault injection.

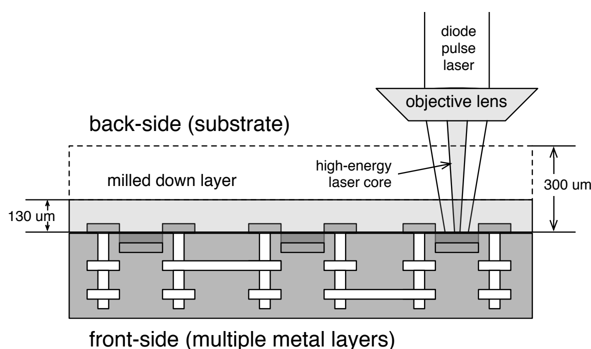


Fig. 6: Laser penetration through thinned silicon substrate to active transistor layer.

enough to trigger the faults (*'high-energy laser core'* illustrated in Fig. 6), which was empirically tested to be much smaller than the spot size at the substrate surface. This phenomenon is based on the nature of diode laser, and the *optical refraction* and *energy absorption*

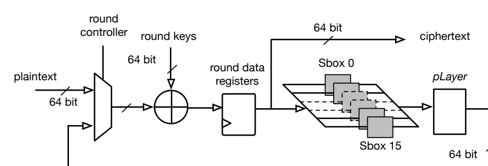


Fig. 7: Implemented PRESENT-80 cryptographic algorithm.

through the residual substrate ($\approx 100\ \mu m$). This is further explained in Section 5.3.

A lightweight block cipher PRESENT [8] was used for profiling the logic array, which is a Substitution - Permutation Network (SPN) cipher with 64 bit block size, 80/128 bit key and 31 computation rounds. Each round contains `addRoundKey`, `sBoxLayer` and `pLayer` permutation. Fig. 7 illustrates the round-based architecture of the implemented cipher. A single PRESENT can be tailored to be implemented in a `CLB column pair`. We define a CLB column pair as two adjacent CLB columns from two clock regions, as shown in Fig. 4 (left). We chose a CLB column pair as the cipher could not fit in a single CLB column. Moreover, the chosen CLB columns had to be vertically adjacent, as horizontally adjacent CLB columns would hinder establishment of column boundaries during the profiling.

4 Laser Sensitivity Profiling

After preparing the device sample, we proceeded with identifying the laser sensitivity distribution of FPGA architecture by analyzing the unique faults from a number of ciphers implemented in parallel.

4.1 Global Array Scan

We applied a strategy by implementing a large number of PRESENT-80 cipher primitives into logic resource array. Each core is restricted into a specific `CLB column pair` by applying the placement constraints at the implementation stage. It is remarked that other algorithms or even a simply cascaded logic chain could be used for this purpose as well. We have chosen a cryptographic algorithm in our work owing to the following advantages:

- the PRESENT-80 occupies almost all the logic resources for each assigned CLB column pair, which provides a good coverage of resource occupation;
- the 32 encryption rounds provide a sufficiently large time window (32 clock cycles) to test the laser injection with varying glitch offsets;
- the exact logic points and affected timings could be simply determined by finding the collision round between the faulty ciphertext decryption and plaintext encryption;
- for the bit flips in the configuration memory of SRAM-FPGA, the faults change the basic circuit configuration instead of the processed data, and it hence leads to permanent malfunction of the design [26]. Concretely, the malfunction stays for the following encryptions until the FPGA is reconfigured with an uninfected bitstream. Therefore, a practical algorithm (e.g., a cipher) used here shows whether the faults are transient data bit upsets or permanent configuration bit flips in SRAM.

All the cores encrypt the same plaintext in parallel and all the output ciphertexts are compared in the output – a *tag* bit vector. The vector width is equal to the number of the implemented ciphers, and the value of each bit represents whether the corresponding cipher is correct or faulty ('0': correct; '1': faulty). A fault in any of the PRESENT cores can be identified by the position of the exclusive tag bit. The scanning stage also records critical parameters, like scan coordinates, injection power and timing. Hence, each fault can be associated to a particular cipher and specific location on chip.

Since the peripheral logic (e.g., the output comparison) also occupies some resources, we have divided the complete die mapping into two parts: the left plane mapping and the right plane mapping. When the right part was scanned, peripheral logic was deployed in the left side, and vice versa, to avoid control interruption. In total, 48 PRESENT cores were implemented in the right region and 42 in the left side, corresponding to the device architecture. The results were then merged to construct the fault map of the entire FPGA. Relying on the recorded coordinates of each fault, we provide the 2D plot in Fig. 8. `X` and `Y` axes are the dimensions of the thinned chip i.e., 12×12 mm^2. Blue dots represent the valid faults by laser injection (occurring in any single cipher). Red dots represent the unexpected invalid faults that simultaneously affected multiple ciphers.

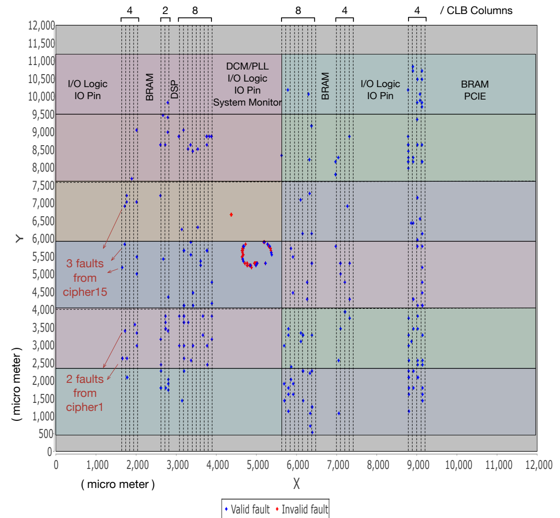


Fig. 8: Laser sensitivity properties of the device under test (DUT), profiled by mapping tagged faults from implemented algorithm. The plotted faults reveal the logic resource architecture of the DUT.

According to our initial results, the faults from each cipher could be precisely mapped w.r.t. the chip area, as depicted in Fig. 8. The coordinates correspond to real dimensions of the FPGA chip. Comparing to the architectural view in Fig. 4, dimensions of other logic resources can be estimated. It is shown that the IO pad (IO Logic and IO Pin) and PCIE occupy a significant die space, the width of BRAM and DSP are roughly equal to 4 and 2 CLB columns, respectively. Besides, there are no faults from the extreme top and bottom (grey) regions. This indicates that the active logic array does not extend to the very edge of the die. Due to the insufficient information, we could not determine the boundaries on the left IO pad region and the right BRAM&PCIE region. Nevertheless, we have clearly identified and mapped the CLB columns to the physical dimensions of the chip. Based on this mapping, we could further continue with a fine-grained scan within the CLB column to identify the laser sensitivity for slices.

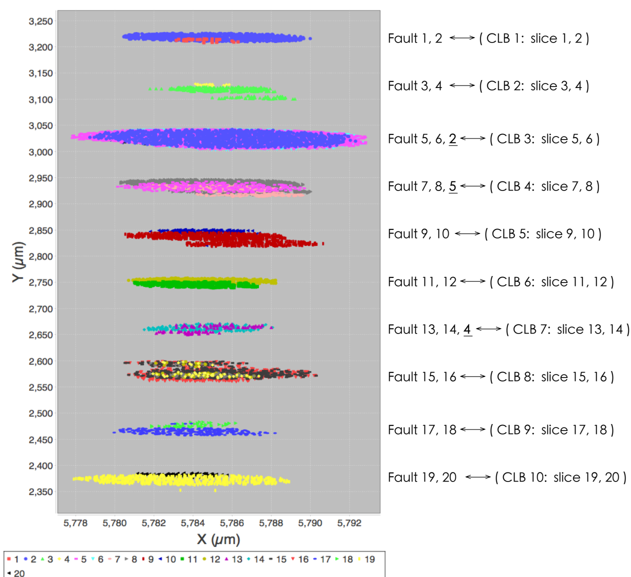


Fig. 9: 2D laser sensitivity map from a CLB column (faults from different slices are coloured differently).

Fig. 10: Slice-exclusive faults for a single CLB.

4.2 Configurable Logic Block Column Scan

Laser fault experiments with a higher scan resolution were executed exclusively in the part of the CLB column where in total 10 CLBs (e.g., 20 slices) were occupied. We only implemented the `round data registers` of PRESENT-80 into the flip-flops of these CLBs. The scan matrix was 100×1400, so totally 140,000 positions were evaluated in this CLB column, with one injection at each location. Note that either single-bit or multiple-bit faults from 4 flip-flops of each slice are tagged with the same colour, which returns 20 different fault types, as plotted in Fig. 9. Hence, the fault sensitivity distribution of the 10 CLBs can be distinctly identified, and a relative position of 2 slices inside each CLB can also be determined.

Fig. 10 gives a closer view of the slice faults of CLB_6 from Fig. 9. The effective laser spot can impact flip-flops from both slices in this CLB, therefore, Fig. 10 shows an overlapping region for this experiment. For most of the CLB regions, it was only possible to disturb the 2 slices from the CLB, however, the scanned regions had various sizes and different overlapping patterns. This phenomenon is mainly due to the uneven substrate layer because of manufacturing process variations, causing different energy levels of the laser beam at the logical layer. The thickness variation across the $12mm \times 12mm$ die was within $15\mu m$, thus the substrate thinning was rather uniform in order to cause such differences in the experiment.

Given the coordinates from both Fig. 9 and Fig. 10, the following important parameters can be estimated as follows:

– distance between the neighbouring CLBs: 60∼80 μm;
– width (`X`) of a CLB column: 7∼15 μm;
– for this DUT, each clock region has 20 CLB rows. Regions are symmetrically divided by a global-clock routing channel. In Fig. 9, half of the clock region was measured, and the middle clock routing channel occupies around 700 μm. So, the height (`Y`) of a CLB column in a clock region (e.g., the height of the clock region) in this Virtex-5 FPGA is estimated as: $(3250 - 2350) * 2\ \mu m + 700\ \mu m \approx 2500\ \mu m$.

It should be noted that these dimensions are the laser fault sensitivity regions, instead of the precise component sizes. However, they show the critical areas that are sensitive to laser attacks. These parameters can help to efficiently navigate the laser to the POIs, for performing precise bit-level fault attacks.

Discussion on the unexpected faults: For some CLB regions, we could observe faults that showed a very different behavior compared to the rest of the faults that could be easily explained. For example, *fault_2* (denoted as a blue dot) is only supposed to appear in CLB_1. However it occured when the laser was targeted at CLB_3 as well. This phenomenon is mainly because the signal paths for register bits [4-7] that were deployed in slice_2, pass the routing channel close to CLB_3, and hence are affected by the laser while targeting CLB_3.

Table 2: Percentages of faults for different registers (non-exclusive).

Register	% of faults
A	66.9
B	35.5
C	35.9
D	36.2

Table 3: Numbers of 1,2,3 and 4-bit flips from the total 3918 faults.

Fault model	# of faults
1-bit flip	2243
2-bit flip	947
3-bit flip	595
4-bit flip	135

4.3 Flip-Flop Scan

After localizing particular CLBs, we could easily navigate the laser spot to a specific slice. Without loss of generality, we focused on a particular slice where 4 out of the total 64 round registers of PRESENT-80 were deployed. In this slice, the registers storing bits 0, 1, 2 and 3 of the intermediate state, were respectively placed in 4 flip-flops. The 4 LUTs inside this slice were left unused. In an FPGA, LUT is actually a 6-input ROM by nature, and any bit upset in this memory changes the implemented Boolean function (potentially leads to computation errors), until FPGA is refreshed by a new bitstream. Therefore, no matter whether the LUTs are used or not, it does not affect the registers implemented in the slice.

By scanning the interested single slice region ($6 \times 13\ \mu m^2$), we obtained the following results. With the laser glitch length fixed to 282 ns and the laser strength varying between 75%-100%, we received 3918 faulty encryptions out of 10,000, with 1 injection per each position. In total, 6462 bits were flipped in the faulty ciphertexts, resulting to 3378 bit sets and 3084 bit resets. It shows that with the same laser settings, we can expect roughly the same number of bit sets and bit resets in flip-flops. If we focus on flip-flops that were affected, the majority of the faults changed the flip-flop `A`, as can be seen in Tab. 2. The other three flip-flops share almost the same proportion of faults. In Tab. 3 we can see the numbers for different fault models that were obtained. More than one half of all the faults were 1-bit flips, following by approximately one third of 2-bit flips. 3- and 4-bit flips were less likely to occur, however still possible to obtain. Moreover, with a high-precision scan, we could find the POIs affecting only one slice without accidentally injecting faults in neighbouring slices.

Each slice in Xilinx FPGAs contains four flip-flops (FF-A, FF-B, FF-C, FF-D). Therefore, each injection can in fact cause multiple bit flips if the laser spot is bigger than the flip-flop scale. We show the faults when 2 adjacent registers are flipped in Fig. 11. The red, green, and blue points represent 2-bit flips occurred on (FF-A, FF-B), (FF-B, FF-C), (FF-C, FF-D), respectively, being caused by single injection. It is clearly shown that different regions overlap in X axis, caused by the effective laser spot size that covers two neighbouring registers. More specifically, $X1$ and $X2$ constitute the middle lines of registers (C, D) and (A, B) in X axis ($X1 \approx 5782.4445\ \mu m$, $X2 \approx 5781.9900\ \mu m$). Due to the similarity of each register, $d/2 = (X2 - X1)/2 \approx 227\ nm$ should be roughly equal with the fault sensitive region of a single register. It is stressed that the register structure varies for devices manufactured with different technologies, therefore this estimation is valid only for the tested Virtex-5 FPGA. However, the analysis method is applicable to other FPGA devices as well.

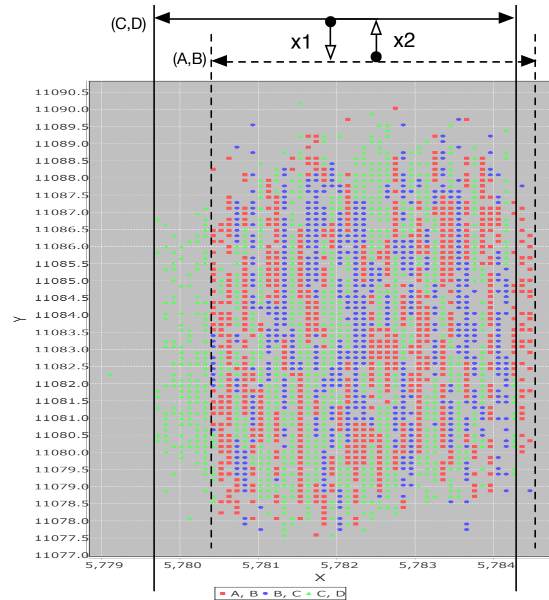


Fig. 11: Estimation of flip-flop laser sensitivity region based on 2-bit faults from adjacent flip-flops.

As mentioned before, none of the faults were found in the configuration memory. As our laser equipment was operating at its maximum capability, we could not

find advanced parameters to inject configuration faults. This could be due to different structure and/or layer placement for flip-flops and configuration memory.

4.4 Impact of Substrate Thinning

To demonstrate the impact of thinning and polishing on laser fault injection, we repeated the experiments with another copy of the test board, where the FPGA substrate was not thinned down. Only the metal lid over the FPGA was removed. A global laser scan on the entire chip was repeated. The scan result has shown that faults only occur when conducting the laser injection in the central area of the chip, similar to the same area on a thinned sample in Fig. 8. The phenomenon demonstrates that only a this area of the chip is sensitive to laser without any substrate thinning. We were not able to trigger any events in the active CLB logic array where the ciphers were implemented, even with the maximum laser power. Thus, we can conclude that substrate thinning is necessary in order to get exploitable transient faults with laser. The fault mechanism of the central area will be discussed in Sec. 5. Please note that the coordinates in all the following figures are preserved with respect to Fig. 8.

5 Results and Discussions

In this section, we first detail some other experiments to further analyze the fault topology and success probability. Next, we discuss the relevance of these fault models to fault attacks on cryptographic algorithms. Finally, we shed some light on the invalid faults found in the central region of the FPGA.

5.1 Success Rate

Apart from different types of faults, success rate is another important parameter. In this part we determine the manipulating power of the attacker for a given target. It is important to know which laser settings are the most efficient for producing bit flips, random byte faults, etc. The objective is to ascertain the minimum power required for fault injection with each fault model.

The experiment was conducted by injecting laser with varying power in the range 0%–100%. The injection campaign was performed on the POI of a slice region where 4-bit round data registers were implemented in the 4 flip-flops of this slice. 100 injections were performed per laser power, using PRESENT-80 encryption with random plaintext and fixed key. In Fig. 12, it can

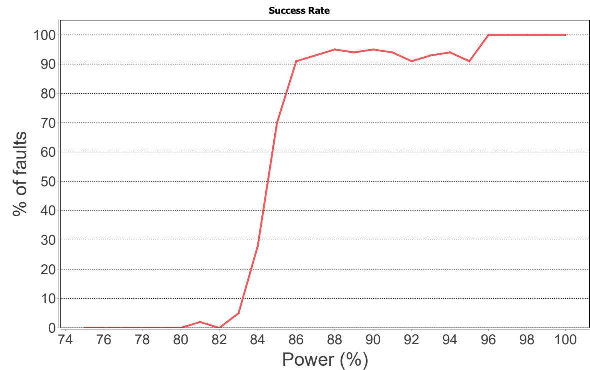


Fig. 12: Fault success rate for random byte flips.

be observed that faults started appearing at 81% laser power. With > 85% laser power, over 90% injections resulted in faults. The fault injection success went to 100%, when laser power was over 96%. These faults included both bit-flips as well as random byte/nibble.

5.2 Compatibility with Cryptographic Fault Attacks

The observed fault models can now be easily translated in terms of fault-based cryptographic attacks. Proposed experiments reported laser fault injection in Virtex-5 FPGA with **single bit-flip** and **random byte fault** models. Scanning through the literature on differential ([34, 4, 5]) and algebraic ([36, 14]) fault attacks on cryptographic primitives (block ciphers, stream ciphers, hash functions, etc.), we found that majority of proposed attacks are based on these two fault models. This means that given a detailed profiling of the target device and the underlying algorithm, any cryptographic primitives can be exploited.

Dual-rail precharge logic (DPL) has been previously shown to be intrinsically resistive against most fault injections [30]. DPL generally employs complementary duplication encoding where each single logical bit is replaced by a complementary bit pair, e.g., 1 is $(0, 1)$ and 0 is $(1, 0)$. Moreover, it is a recommended practice in DPL to place complementary bit pairs in adjacent flip-flops of a slice [17] for achieving smaller silicon process variations in order to reducing the early propagation effect (EPE) [24]. Authors of [30] demonstrated that dual-rail logic resists all faults except symmetric faults which flip encoded $(0, 1)$ to $(1, 0)$ and vice-versa. Faults which do not follow this pattern cannot be exploited for DFA or AFA, since they inevitably break the DPL and can be easily detected. As shown in previous experimental results, we found that 13% of random byte faults are actually symmetric, located in adjacent flip-flops. This fault pattern shows that various fault attacks can be practically realized in dual-rail protected

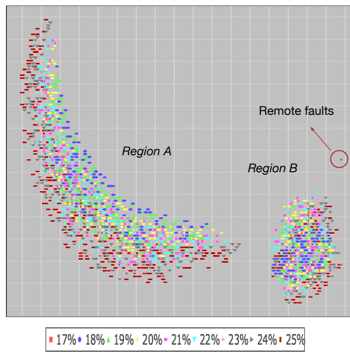


Fig. 13: Position and strength of faults in a laser scan focused on the center of FPGA.

cryptographic primitives, by stealthily injecting faults without breaking the dual-rail logic compensation. Similarly, the demonstrated fault model can also bypass error detection schemes, such as Sbox parity in [35].

5.3 Discussion on Central Fault Region

A dense fault region appeared in the center of the FPGA die. This region was not an active CLB region and no user logic was implemented in this area. The nature of injected faults in this region was also very different from the `valid` faults, i.e., several cores were faulted by a single injection. Moreover, the faults started appearing at a much lower power (18% as compared to 81% for faults in CLB columns). To study this behavior, we have specially focused on this region with better scanning precision using a 20x laser lens. The size of the laser spot with this lens was $15 \times 3.5\ \mu m^2$. The energy density of the 20$\times$ lens was higher than that of the 5$\times$ lens. We varied the laser power from 17% to 25% of the full laser strength. Fig. 13 gives the fault plot after the laser scan in this section. Points in different colours represent different laser strengths. Most faults were located in two regions, hereafter named `"Region A"` and `"Region B"` respectively. A very few number of faults were seen in some remote spots. A bitstream modification was never observed.

Due to undisclosed transistor-level device information, clarifying the internal mechanism of the faults here is challenging. Even when the cipher and its peripheral logics were placed in a distant FPGA corner, the fault characteristic of central region remained unchanged. Also, multiple ciphers could be faulted by a single injection, when targeting this region. Thus, laser injection in this region causes and propagates some global disturbance, which could affect multiple ciphers irrespective of the placement. Deeper analysis was conducted under two assumptions:

- The faults were triggered by the *global clock network*. Since the clock buffer that fans out the global clock is deployed in the die center in this FPGA, a fault on the buffer can spread to the whole chip. To validate, we removed the clock buffer and routed the clock system using the signal paths. However, the faults still persisted in the new experiment.
- The faults were triggered by the *system monitor*. System monitor is an environment sensor system (power supply, temperature etc.), deployed near the center of the FPGA die. System monitor is activated by default and physically connected to the power network, that can possibly propagate the voltage disturbance induced by laser impact. However, fresh experiments after disabling the system monitor, by connecting all of its IO pins to GND on board, still reported similar faults in central region.

To continue our analysis, we implemented a Ring Oscillator (RO) in the CLB area, far from the central region, to conduct another test. The RO was composed of a single inverter (LUT) and routing wires, implemented in a CLB region to cover 9 CLBs in a square routing, which resulted in a stable oscillation frequency of 230 MHz. We observed the signal oscillation of the RO from an oscilloscope, the results are shown in Fig. 14. When the laser was shot in the CLB area, where the RO was deployed, we could see that laser injection disturbed the RO response for a short period of time with an oscillation ripple lasting around 800 ns. Afterwards, the RO returned to a stable oscillation, as shown in Fig. 14 (a). On the other hand, when the laser was shot on Regions A and B, the response of the RO was more noticeable. As shown in Fig. 14 (b), the RO stopped to oscillate for a bigger period of time ($\approx 27,000\ ns$). From an oscillating state, the RO response was pulled down to zero and then the RO started again to oscillate and lock itself. The phenomena can be described as a `soft` reset which occured probably due to triggering of certain sensors or by some impact on the power delivery network, which are not present in the documentation. We call it a soft reset because only the signals were disarmed but flip-flops and logic values were preserved. We could not carry the analysis further without knowing the architectural details of the commercial FPGA. Therefore, the reason for these faults at the center stays an open question.

6 Countermeasure

From a high-level point of view, there are two countermeasure classes against fault injection: detection-based and correction-based. Correction-based methods often

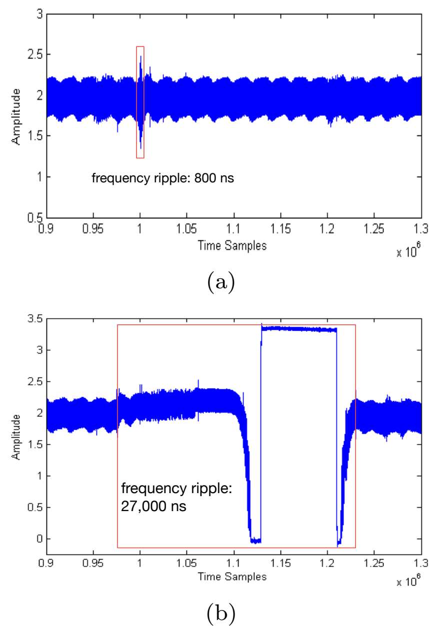


Fig. 14: RO response against laser injection targeting (a) CLB area; (b) `Region "A"`.

take concepts from failure tolerant circuits and can either be based on redundancy or error-correcting codes. In this section, we will focus on fault detection that is circuit- and fault model-independent and provides good detection rates. The main idea of the countermeasure is to prevent the attacker from profiling sensitive design on the chip. This calls for an on-chip sensor which could detect any laser injection attempt and stop sensitive computation before profiling/exploitation. In some security-critical applications, the device can even wipe the secret key after the alarm. The sensor should be such that it has a larger spatial sensitivity and a lower power sensitivity against laser as compared to the sensitive circuit.

Considering the results from the previous section, RO shows a great detection sensitivity that could be utilized for designing a countermeasure. To convert this ring oscillator into a complete sensor, we monitor the phase of the RO using a phase detector (PD) circuit. A laser injection disturbs RO phase as shown in Fig. 14(a). A monitoring PD will report phase disturbance, triggering an alarm that can be used to stop the sensitive computations. Several such RO and PD based combinations have been proposed. We have implemented the same design as proposed in [16] in order to compare the countermeasure sensitivity w.r.t. data faults induced in the circuit. High-level schematic of the circuit is depicted in Fig. 15, placement of the sensor and cipher w.r.t. area is shown in Fig. 16. Data registers of PRESENT-80 cipher were implemented into 8 CLBs in a rectangular

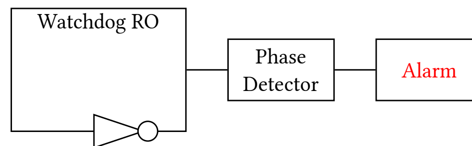


Fig. 15: Schematic of the watchdog ring oscillator-based countermeasure.

shape (4×2). The RO circuit was routed through the corner slices of the cipher in order to protect the slice registers. Area plot of fault distributions is depicted in Fig. 17, capturing area of size 3×5 CLBs. Sensitivity of the countermeasure compared with cryptographic circuit sensitivity is plotted in Fig. 18. As can be seen in the plot, the detection sensitivity is very high (98.45%), with alarm rate of 23.1:1.

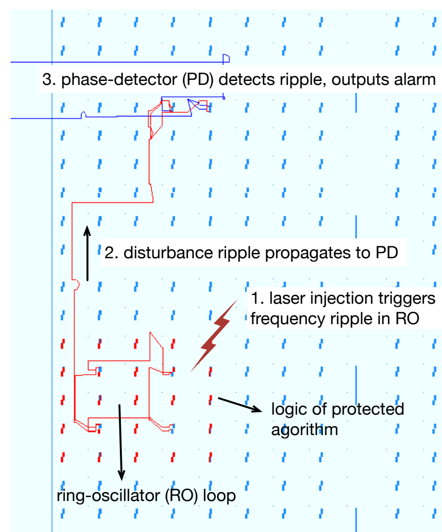


Fig. 16: Placements of the detection sensor and protected cipher.

7 Conclusions

This paper focuses on a novel profiling approach of Xilinx Virtex-5 65 *nm* FPGA, for disclosing the internal device architecture, and hence accelerating the practical fault injection attacks on the sensitive modules. The profiling was done by using a 1064 *nm* pulse laser, focused on the backside of the FPGA. In order to impact the active layer under chip surface, we relied on the mechanical solution to mill down and polish the silicon substrate. We thoroughly discussed the optical properties of the silicon circuit under laser fault injection, and detailed the chip preparation works. We conducted a chip-scale and fine-grained laser scans of the FPGA.

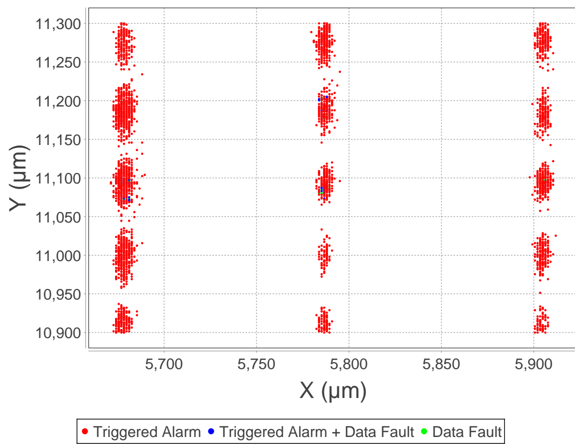


Fig. 17: Measurements for the countermeasure for fault detection.

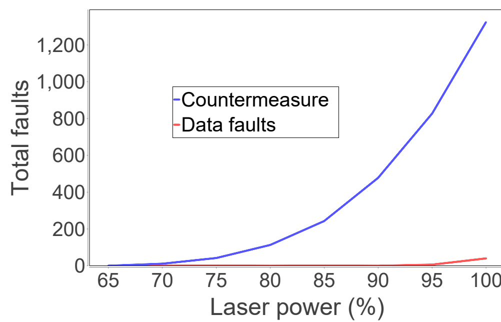


Fig. 18: Countermeasure sensitivity *vs.* data faults.

By mapping the output data, we could restore the information about the FPGA array and defer the scale of the logic elements.

This work helps to rapidly localize the sensitive modules and successfully identify the critical components of an embedded security system inside an unknown target chip. The experimental results showed that the observed fault models are compatible with most of the previously proposed differential and algebraic fault attack schemes. Besides, we proved that the fault format is capable of exploiting the dual-rail and parity based countermeasures. Finally, a laser injection digital detector was depicted, which is extremely sensitive to foresee an on-going chip injection attempt even before it really induces logic faults in the protected algorithm. Moreover, this countermeasure is lightweight and pure digital, hence it can be applied to any existing digital systems without major overhead.

References

1. Agoyan, M., Dutertre, J.M., Mirbaha, A.P., Naccache, D., Ribotta, A.L., Tria, A.: Single-bit DFA using multiple-byte laser fault injection. In: HST, 2010 IEEE International Conference on, pp. 113–119 (2010)
2. Alderighi, M., Casini, F., d'Angelo, S., Mancini, M., Pastore, S., Sechi, G.R.: Evaluation of single event upset mitigation schemes for sram based FPGAs using the FLIPPER fault injection platform. In: Defect and Fault-Tolerance in VLSI Systems, 2007. DFT'07. 22nd IEEE International Symposium on, pp. 105–113. IEEE (2007)
3. Anderson, R.: Security engineering: A guide to building dependable distributed systems. 2001
4. Bagheri, N., Ebrahimpour, R., Ghaedi, N.: New differential fault analysis on PRESENT. EURASIP Journal on Advances in Signal Processing **2013**(1), 1–10 (2013)
5. Bagheri, N., Ghaedi, N., Sanadhya, S.K.: Differential fault analysis of SHA-3. In: Progress in Cryptology–INDOCRYPT 2015, pp. 253–269. Springer (2015)
6. Beutler, J.: Visible light lvp on bulk silicon devices. In: 41st International Symposium for Testing and Failure Analysis (November 1-5, 2015), pp. 1–8. Asm (2015)
7. Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Advances in Cryptology-CRYPTO'97, pp. 513–525. Springer (1997)
8. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: Present: An ultra-lightweight block cipher. In: P. Paillier, I. Verbauwhede (eds.) Cryptographic Hardware and Embedded Systems - CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings, pp. 450–466. Springer Berlin Heidelberg, Berlin, Heidelberg (2007). DOI 10.1007/978-3-540-74735-2_31. URL `http://dx.doi.org/10.1007/978-3-540-74735-2_31`
9. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the importance of eliminating errors in cryptographic computations. Journal of Cryptology **14**(2), 101–119 (2001)
10. Breier, J., Jap, D.: Testing feasibility of back-side laser fault injection on a microcontroller. In: Proceedings of the WESS'15, pp. 5:1–5:6 (2015)
11. Buchner, S., Miller, F., Pouget, V., McMorrow, D.: Pulsed-laser testing for single-event effect investigations. IEEE Transactions on Nuclear Science **60**(3), 1852–1875 (2013)
12. Canivet, G., Maistri, P., Leveugle, R., Cldire, J., Valette, F., Renaudin, M.: Glitch and laser fault attacks onto a secure AES implementation on a SRAM-based FPGA. Journal of Cryptology **24**(2), 247–268 (2011)
13. Courbon, F., Loubet-Moundi, P., Fournier, J.J., Tria, A.: Adjusting laser injections for fully controlled faults. In: International Workshop on Constructive Side-Channel Analysis and Secure Design, pp. 229–242. Springer (2014)
14. Courtois, N.T., Jackson, K., Ware, D.: Fault-algebraic attacks on inner rounds of des. e-Smart'10 Proceedings: The Future of Digital Security Technologies (2010)
15. Dutertre, J.M., Mirbaha, A.P., Naccache, D., Tria, A.: Reproducible single-byte laser fault injection. In: PRIME, 2010 Conference on, pp. 1–4 (2010)
16. He, W., Breier, J., Bhasin, S.: Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks. In: Security, Privacy, and Applied Cryptography Engineering - 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings, pp. 27–46 (2016). DOI 10.1007/978-3-319-49445-6_2. URL `http://dx.doi.org/10.1007/978-3-319-49445-6_2`
17. He, W., Otero, A., de la Torre, E., Riesgo, T.: Customized and automated routing repair toolset towards side-channel analysis resistant dual rail logic. Microprocessors and Microsystems **38**(8), 899–910 (2014)

18. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. CRYPTO '99, pp. 388–397 (1999)
19. Kömmerling, O., Kuhn, M.G.: Design principles for tamper-resistant smartcard processors. Smartcard **99**, 9–20 (1999)
20. Lima Kastensmidt, F., Tambara, L., Bobrovsky, D.V., Pechenkin, A.A., Nikiforov, A.Y.: Laser testing methodology for diagnosing diverse soft errors in a nanoscale sram-based fpga. Nuclear Science, IEEE Transactions on **61**(6), 3130–3137 (2014)
21. Lohrke, H., Scholz, P., Boit, C., Tajik, S., Seifert, J.P.: Automated detection of fault sensitive locations for reconfiguration attacks on programmable logic pp. 1–6 (2016)
22. Maurine, P.: Techniques for em fault injection: equipments and experimental results. In: Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on, pp. 3–4. IEEE (2012)
23. 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, WESS '11, pp. 2:1–2:9. ACM, New York, NY, USA (2011). DOI 10.1145/2072274.2072276. URL `http://doi.acm.org/10.1145/2072274.2072276`
24. Moradi, A., Immler, V.: Early propagation and imbalanced routing, how to diminish in fpgas. In: Cryptographic Hardware and Embedded Systems–CHES 2014, pp. 598–615. Springer (2014)
25. Phang, J., Chan, D., Palaniappan, M., Chin, J., Davis, B., Bruce, M., Wilcox, J., Gilfeather, G., Chua, C., Koh, L., Ng, H., Tan, S.: A review of laser induced techniques for microelectronic failure analysis. In: Proceedings of the 11th International Symposium on the Physical and Failure Analysis of Integrated Circuits. IPFA 2004, pp. 255–261 (2004). DOI 10.1109/IPFA.2004.1345617
26. Pouget, V., Douin, A., Lewis, D., Fouillat, P., Foucard, G., Peronnard, P., Maingot, V., Ferron, J., Anghel, L., Leveugle, R., Velazco, R.: Tools and methodology development for pulsed laser fault injection in SRAM-based FPGAs. In: 8th LATW'07), p. Session 8. IEEE Computer Society, Cuzco, Peru (2007)
27. Quisquater, J.J., Samyde, D.: Eddy current for magnetic analysis with active sensor. In: Esmart 2002, Nice, France (2002)
28. Roscian, C., Dutertre, J.M., Tria, A.: Frontside laser fault injection on cryptosystems - Application to the AES' last round. In: HOST, 2013 IEEE International Symposium on, pp. 119–124 (2013)
29. Roscian, C., Sarafianos, A., Dutertre, J.M., Tria, A.: Fault model analysis of laser-induced faults in SRAM memory cells. In: FDTC, 2013 Workshop on, pp. 89–98 (2013)
30. Selmane, N., Bhasin, S., Guilley, S., Graba, T., Danger, J.L.: WDDL is protected against setup time violation attacks. In: FDTC, pp. 73–83 (2009)
31. Selmke, B., Brummer, S., Heyszl, J., Sigl, G.: Precise laser fault injections into 90nm and 45nm SRAM-cells. In: CARDIS, pp. 1–13 (2015)
32. Swierczynski, P., Becker, G.T., Moradi, A., Paar, C.: Bitstream fault injections (bifi) – automated fault attacks against sram-based fpgas. IEEE Transactions on Computers **PP**(99), 1–14 (2017). DOI 10.1109/TC.2016.2646367
33. Tajik, S., Lohrke, H., Ganji, F., Seifert, J.P., Boit, C.: Laser fault attack on physically unclonable functions. In: 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 85–96 (2015). DOI 10.1109/FDTC.2015.19
34. Tunstall, M., Mukhopadhyay, D., Ali, S.: Differential fault analysis of the advanced encryption standard using a single fault. In: 5th IFIP WG, WISTP, pp. 224–233 (2011)
35. Wu, K., Karri, R., Kuznetsov, G., Goessel, M.: Low cost concurrent error detection for the advanced encryption standard. In: Test Conference, 2004. Proceedings. ITC 2004. International, pp. 1242–1248. IEEE (2004)
36. Zhang, F., Guo, S., Zhao, X., Wang, T., Yang, J., Standaert, F.X., Gu, D.: A framework for the analysis and evaluation of algebraic fault attacks on lightweight block ciphers. IEEE Transactions on Information Forensics and Security **11**(5), 1039–1054 (2016). DOI 10.1109/TIFS.2016.2516905