Comprehensive laser sensitivity profiling and data register bit-flips in 65 nm FPGA

He, Wei; Breier, Jakub; Bhasin, Shivam; Jap, Dirmanto; Ong, Hock Guan; Gan, Chee Lip

2016

He, W., Breier, J., Bhasin, S., Jap, D., Ong, H. G., & Gan, C. L. (2016). Comprehensive Laser Sensitivity Profiling and Data Register Bit-Flips for Cryptographic Fault Attacks in 65 Nm FPGA. International Conference on Security, Privacy, and Applied Cryptography Engineering, 47-65.

https://hdl.handle.net/10356/82156

https://doi.org/10.1007/978-3-319-49445-6_3

Comprehensive Laser Sensitivity Profiling and Data Register Bit-Flips for Cryptographic Fault Attacks in 65 nm FPGA

Wei He[†$], Jakub Breier[†$], Shivam Bhasin[†$], Dirmanto Jap[†*], Hock Guan Ong[‡$], and Chee Lip Gan[‡$]

[†]Lab of Physical Analysis and Cryptographic Engineering
[*]School of Physical and Mathematical Sciences
[‡]School of Materials Science and Engineering
[$]Temasek Laboratories
Nanyang Technological University, Singapore
{he.wei,jbreier,sbhasin,djap,hgong,clgan}@ntu.edu.sg

Abstract. FPGAs have emerged as a popular platform for security sensitive applications. As a practical attack methodology, laser based fault analyses have drawn much attention in the past years due to its superior accuracy in fault perturbation into security-critical Integrated Circuits (ICs). However, due to the insufficient device information, the practical injections work are not so efficient as expected. In this paper, we thoroughly analyze the laser fault injections to data flip-flops, instead of the widely studied configuration memory bits, of a modern nanoscale FPGA. A profiling campaign based on laser chip scan is performed on an exemplary 65 nm Virtex-5 FPGA, through the delayered silicon substrate, to identify the laser sensitivity distribution of the resource array and the fundamental logic cells. The sophisticated flip-flop bit flips are realized by launching fine-grained laser perturbations on an identified Configurable Logic Block (CLB) region. The profiled laser fault sensitivity map to FPGA resource significantly facilitate high-precision logic navigation and fault injection in practical cryptographic fault attacks. We show that the observed single- and multiple-bit faults are compatible with most proposed differential or algebraic fault analyses (DFA/AFA). Finally, further discussions on capability of reported fault models to bypass fault countermeasures like parity and dual-rail logic are also given.

Keywords: Cryptographic Fault Attack, Laser Fault Injection, Data Bit-Flip, FPGA

1 Introduction

Modern Field Programmable Gate Arrays (FPGAs) and programmable System on Chips (SoCs) come with interesting features like rich logic resource, real-time reconfiguration, high-density memories, clock managers, environment sensors, etc. Owing to such features and low time-to-market, it enables deployment of

FPGAs in many kinds of applications. FPGAs also find wide application in security-critical domains due to constantly evolving protection requirements like aerospace, defence etc. However, like other devices, FPGAs are also vulnerable to physical attacks, i.e., side-channel attacks [12], fault attacks [5] and probing [3].

Side-channel attacks (SCA) are passive and exploits unintentional physical leakages, while probing tries to read out sensitive values directly from the circuit [13]. Fault attacks stay in between SCA and Probing by operating the target device in a non-friendly environment and exploiting secrets from the faulty behaviors. The most common fault attack in context of cryptography is the differential fault analysis (DFA) [4] and the recently published algebraic fault analysis (AFA) [9]. For instance, in AES, DFA can extract the secret key by a single well-located fault [23]. 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 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 needs expensive equipments and more preparation efforts.

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

An alternative to laser method is the electromagnetic injection (EMI [17]) 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 set-up time violation in flip-flops or faulty timing in internal clock generator [15]; (c) bias critical logic, e.g., key generation PUF [22]. However, the generated EM field is difficult to be restricted only to the Point-of-Interest (POI), so the accuracy of EMI is still comparatively lower than LFI.

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

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. Finally, conclusions are drawn in Sec. 6.

2 Related Work

Many techniques have been proposed in previous literatures for disturbing values processed and stored in ICs [10, 1, 18, 19, 8, 6]. In general, results on microcontrollers show high degree of repeatability, mainly because of a 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 instruction execution on these devices, leading to instruction skip or alteration faults. Previous papers about fault injection on FPGAs mostly aim at memory disturbances both on configuration memory of SRAM FPGAs and data Block RAM [16, 7, 21].

The fault injection into the configuration memory of SRAM FPGAs intrinsically incurs the alterations on logic functions or routings, and hence lead to permanent circuit malfunction until the device is reconfigured with a new bitstream. The faults are typically found and analyzed by *readback* the bitstream from device after each fault injection, to be compared with the unaffected *golden* sample [2, 14], in order to figure out the affected tiles on the logic array. So the comparison efficiency is low and static, and furthermore the method is becoming challenging to apply to newer FPGAs with more obscured bitstream format.

In this work, we target the data bit flips in registers and perform the dynamic fault injection to a lightweight block cipher in a 65 *nm* commercial FPGA. Since the faults are inserted by flipping the data bit/bits, instead of the configuration faults in SRAM, the circuit function will not be disrupted. So it is more practical to be applied to real fault attack scenarios. The fault comparison is to analyze the faulty cipher outputs where the bitstream readback is not required, which makes the efficiency is much higher than bitstream comparison. In our work, we used a diode pulse laser with different lens fixed into a 2D (X-Y) motorized stage. The selected chip is encapsulated in a flip-chip package, hence a mechanical preprocess is conducted for thinning down the substrate for achieving better laser penetration.

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, backside), fault precision (bit, random), and purpose of fault injection.

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

- proposes a new methodology for laser sensitivity profiling of a nano-scale FPGA, ranging from the global resource array to the slice flip-flops. This method can be practically applied to a wider spectrum of FPGA devices.
- reports precise bit-flip faults exclusively to specific flip-flops in logic resource, instead of the configuration memory faults, inside the FPGAs.

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

Work	Platform	Tech.	Target	Fault Model	Position	Purpose
Dutertre et al.[10, 1, 19]	μC	350nm	SRAM	byte	Front	Attack
Courbon et al.[8]	ASIC	90nm	FlipFlops	bit	Back	Attack
Breier et al. [6]	μC	350nm	Register	bit	Back	Attack
Pouget et al. [16]	FPGA	150nm	CLB/BRAM	random	Back	Reliability
Canivet et al. [7]	FPGA	150nm	Logic	random	Back	Attack
Selmke et al.[21]	FPGA	90/45nm	BRAM	bit	Back	Attack
This Work	**FPGA**	**65nm**	**Flip-Flops**	**bit**	**Back**	**Attack**

– realises fault models in FPGA that are compatible with almost all proposed differential/algebraic fault analysis (DFA/AFA) on unprotected cryptographic primitives.
– discusses the possibilities of counteracting dual-rail or parity protected cryptographic primitives.

3 Chip Preparation and Device Configuration

For modern FPGAs, two packages 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 to a 65nm Virtex-5 FPGA (LX50T) with flip-chip package on Digilent's *Genesys* board. To allow effective laser impact to the internal logics, we have pre-processed the FPGA chip by thinning down the substrate layer using a mechanical solution.

3.1 Optical Property of Silicon

To understand laser effects in silicon we have to study its physical properties and the way how the energy traverse and affect the active logic layer. Schmid [20] provided a deep overview of optical absorption of Si:As and Si:B samples and addressed ionization process of pulsed lasers that produces electron-hole pairs. For linear absorption of semiconductor we can derive the linear transfer energy (LET), expressed in Eq. 1 as a function of the depth penetration z.

$$LET(z) = \frac{\alpha \lambda E_{e/h}}{\rho h c} E_{laser} e^{-\alpha x} \tag{1}$$

where $\alpha[cm^{-1}]$ is the absorption coefficient, $\lambda[nm]$ represents the wavelength of a pulse laser, the energy required to induce an electron-hole pair is denote as $E_{e/h}[eV]$, and $\rho[mg/cm^3]$ means the density of silicon, h, c and E_{laser} presents the Planc constant, the light velocity and the laser energy respectively.

Previous equation works for particles, however for laser we need to take a radial exposure into account. This is expressed in Eq. 2.

$$l(r,z) = l_0(z)e^{\frac{2r^2}{\omega(z)^2}}E_{laser}e^{-\alpha z} \tag{2}$$

where $\omega(z)^2$ expresses the radial properties of the laser as a function of the beam width, focalization point and refraction index.

Another important parameter to be identified is how deep we can reach the logic elements under the silicon surface. For this purpose we have to use absorption coefficient from Eq. 3.

$$\alpha = \frac{4\pi k}{\lambda} \tag{3}$$

where k is the extinction coefficient.

Values for absorption coefficients for silicon can be found in literatures. We plotted combined results from [11, 24] in Fig. 1 for wavelengths that are mostly used for laser fault injections (530 nm – 1070 nm). It is seen that for green laser (532 nm), the absorption depth is $\approx 1.58\ \mu m$, for near infrared (NIR) laser (808 nm) it is $\approx 12.79\ \mu m$, and for NIR laser (1064 nm) it is $\approx 1100\ \mu m$. Accordingly, a conclusion can be drawn that for our case study, where the thickness of the thinned silicon substrate from the backside is $\approx 130\ \mu m$, it is necessary to use a laser with near infrared wavelengths or higher. Hence the diode pulse laser with 1064 nm wavelength is selected for our experiments.

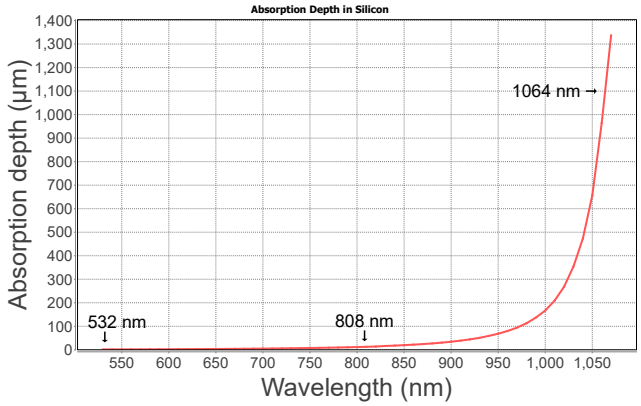
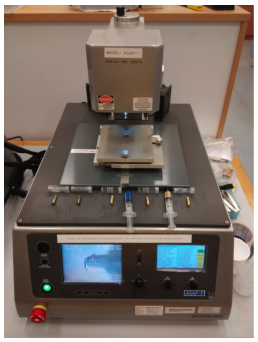


Fig. 1: Absorption depth in silicon for wavelengths from 530 nm to 1070 nm.

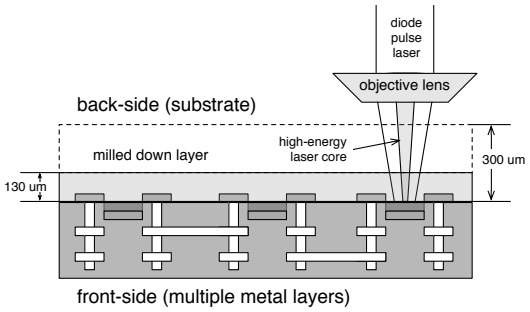
3.2 Backside Substrate Thinning of Virtex-5

We have employed a backside polishing technique, which involves the thinning down of the chip substrate layer. This process is typically useful in experiments

where access from the back of a die is required for testing, such as laser probing, fault isolation and thermal imaging. A 1064 nm diode pulse laser is used to generate charges in the desired location in the silicon, with a thick silicon substrate, the amount of charges that are generated at the POIs in the active logic layer are rather limited because of the laser refraction and energy absorption. By thinning down the substrate, the amount of charges induced at the POIs can be significantly increased which makes flip-flop upsets possible. We performed backside polishing on our FPGA sample using *Ultra Tec ASAP-1* polishing machine (Fig. 2a). The heat-sink metal lid of the FPGA sample was removed to expose the backside substrate, and this substrate was mechanically reduced to $\approx 130\ \mu m$, removing $\approx 170\ \mu m$, as illustrated in Fig. 2b. The thinning process can be bypassed if the strength of laser source is high enough such that laser injection after absorption is enough for realizing event upsets. On the other hand, the silicon substrate can also be further thinned down to $\approx 50\ \mu m$ to have, perhaps, very slight improvement in result, but the risk taken will be higher. As the silicon substrate is being thinned down, the integrity of the silicon structure will experience a bigger force. This will cause die warping and in some cases where the strain is too big, the sample will crack. Thus in our approach, we will want to achieve sample preparation able for testing with the least risk to be involved. Thinner silicon substrate is a much seek out goal in a lot of the backside sample preparation for other form of testing and/or with other wavelength of laser. However, in our experiment context, the advantage to have a much thinner substrate is being overshadowed by the risk of spoiling the onboard sample.



(a) Ultra Tec ASAP-1 polishing machine.



(b) Laser penetration through thinned silicon substrate to active transistor layer.

Fig. 2: Mechanical chip process for realizing effective laser penetration to transistor layer in FPGA.

3.3 Device Under Test and Configuration

The target 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. 3 (left) illustrates the basic architecture of the selected device. The CLB structure in Xilinx FPGA contains 2 slices, together with the route channel to a switch-box, as sketched in Fig. 3 (right).

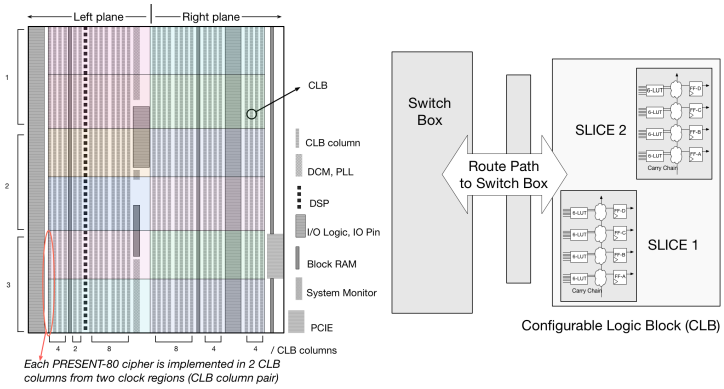


Fig. 3: Simplified view of the architecture of the target FPGA and CLB cell.

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 hinder the laser focalization, we have 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 is around $60 \times 14\ um^2$. The output power of the laser can 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. 4.

Importantly, solid experiments prove that only the very center part of the claimed laser beam is powerful enough to trigger the faults (*'high-energy laser core'* illustrated in Fig. 2b), which is empirically tested to be roughly 1/10 of the claimed spot size ($\approx 60\ um^2$). This phenomenon is based on the nature of diode laser, and the *optical refraction* and *energy absorption* through the residual substrate ($\approx 100\ um$). We do not suggest a further substrate process since it potentially causes side-effects on the electrical characteristics of FPGA, and also it risks physical damage to transistors or interconnects.

A lightweight block cipher `PRESENT` was used for profiling the logic array, which is a Substitution-Permutation Network (SPN) cipher with 64 bit block

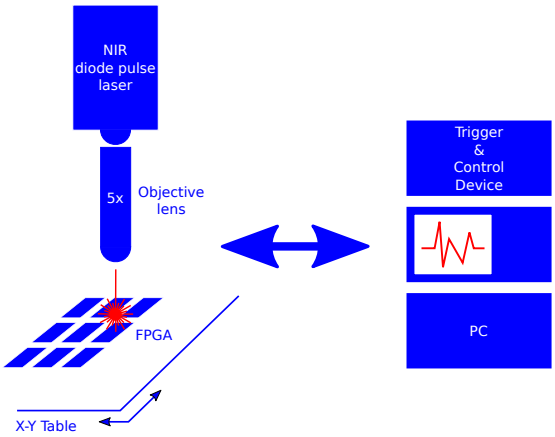


Fig. 4: Laser setup used for the experimental fault injection.

size, 80/128 bit key and 31 computation rounds. Each round contains `AddRoundKey`, Sbox `Substitution` and `pLayer` permutation. Fig. 5 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. 3 (left). We chose a CLB column pair as the cipher couldn't fit in a single CLB column. Moreover, the chosen CLB column must be vertically adjacent, as horizontally adjacent CLB columns would hinder establishment of column boundaries during the profiling.

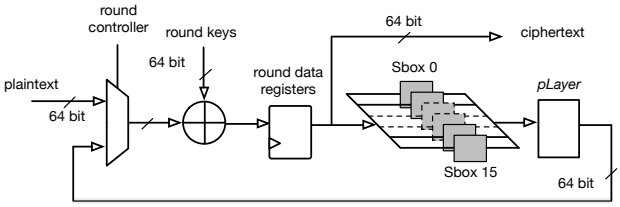


Fig. 5: Implemented PRESENT-80 cryptographic algorithm.

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, and 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 big 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 to 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 [16]. Concretely, the malfunction stays for the following encryptions untill the FPGA is reconfigured with an uninfected bitstream. So, a practical algorithm (e.g., a cipher) used here shows if 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 if 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 to the left side, and vice versa, to avoid control interruption. Total 48 PRESENT cores are implemented in the right region and 42 in the left side, corresponding to the device architecture. The results are 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. 6. The `X` and `Y` axis are the dimensions of the thinned chip i.e., 12×12 mm^2. The blue dots represent the valid faults by laser injection (occurring in any single cipher). The red ones represent the unexpected (exceptional) invalid faults that simultaneously affected multiple ciphers. Based on this analysis, we could investigate the laser sensitivity on a specific CLB column.

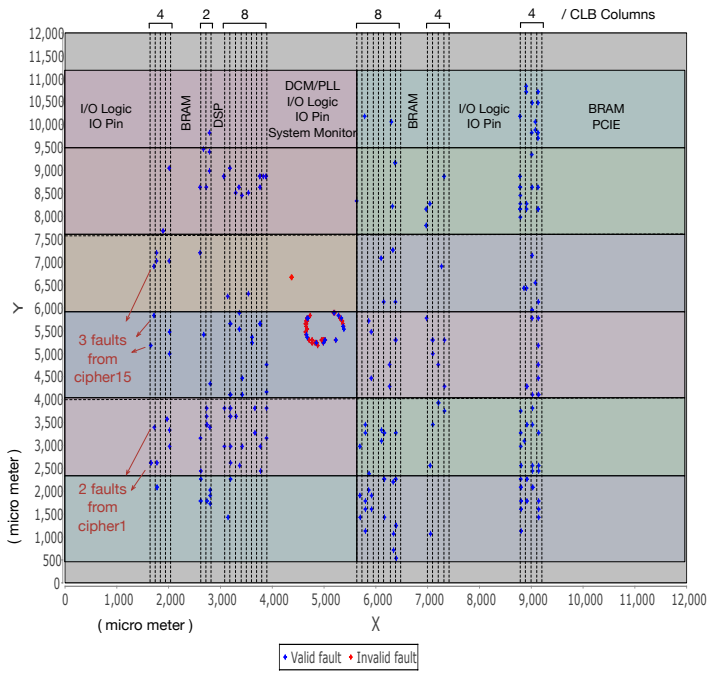


Fig. 6: Laser sensitivity properties of device under test (DUT), profilied by mapping tagged faults from implemented algorithm and scan coordinates. The plotted faults reveal the logic resource architecture of the exemplary FPGA.

CLB Column According to our initial results, the faults from the same cipher come from the same rectangular region in Fig. 6. It also matches the user placement constraints. Since the coordinates base on the real dimensions of FPGA, not the virtual floor plan or FPGA editor view, Fig. 6 provides the exact scales of the on-chip instances. Comparing to the architectural view in Fig. 3, dimensions of other logic resources can be estimated. It is shown that the IO pad (IO Logic and IO Pin) and PCIE occupies 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 further continue with a fine-grained scan within the CLB column to identify laser sensitivity for slices.

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 to the center part of the chip, which exactly match the position and shape (ring shape) of the exceptional invalid faults in the center die, as shown in Fig. 6. The phenomenon demonstrates that only a specific center part of the chip without any substrate thinning is sensitive to the laser impacts. Noticeably, we are not able to trigger any events in the active CLB logic array where the ciphers are implemented, even with the maximum laser power. Thus substrate thinning enables exploitable transient fault injection with laser. The fault mechanism of center die will be discussed in Sec. 5. Please note that the coordinates in all the following figures are preserved with respect to Fig. 6.

4.2 Configurable Logic Block Column Scan

The laser fault tests with higher scan resolution are executed exclusively to a part of the CLB column where totally 10 CLBs (e.g., 20 slices) are occupied. We only implemented the `round data registers` of PRESENT-80 into the flip-flops of these CLBs. The scan matrix is 100×1400, so totally 140,000 positions will be evaluated by laser in this CLB column, and one injection is executed in each location. Note that either single-bit or multiple-bit fault from the 4 flip-flops of the each slice are tagged with the same color, which returns 20 different fault types to be observed, as plotted in Fig. 7. Hence the fault sensitivity distribution of the 10 CLBs can be distinctly identified, and the relative sensitivity positions of the 2 slices inside each CLB can also be established.

Fig. 8 gives a closer view of the slice faults of CLB_6 from Fig. 7. Because the effective laser spot possibly impacts flip-flops from both slices in this CLB, the fault regions from the 2 slices show an overlapped region, as shown in Fig. 8. For most of the CLB regions, only the faults from the 2 slices of this CLB appear, but not symmetrically. This phenomenon is mainly due to the variant energy attenuations of laser beam through the residual but uneven substrate layer due to process variations. The thickness variation across the $12mm \times 12mm$ die is within $15\mu m$ and thus the substrate thinning is rather uniform.

Given the coordinates from both Fig. 7 and Fig. 8, 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, and regions are symmetrically divided by a global-clock routing channel. In Fig. 7, half of the clock region are 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 heigh 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 these dimensions are the laser fault sensitivity regions, instead of the precise component sizes. However, they shows the critical scales that

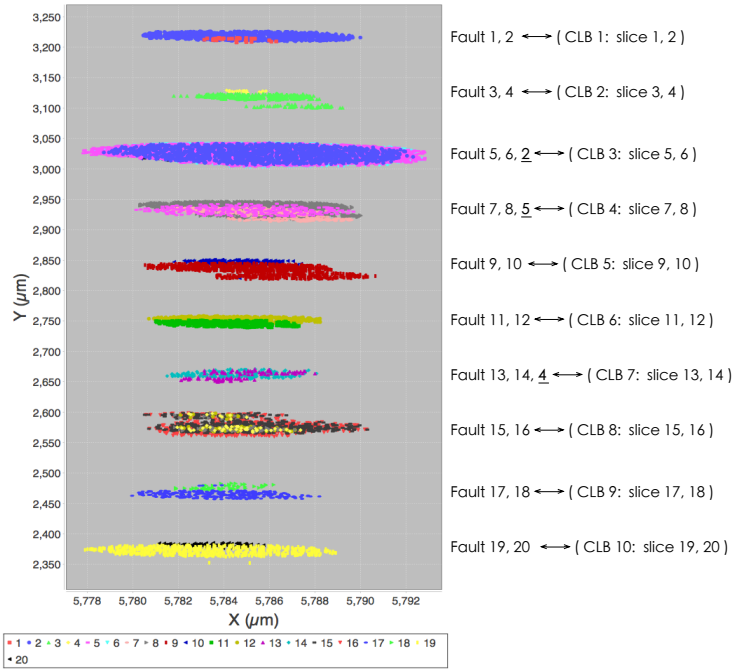


Fig. 7: 2D laser sensitivity map from CLB column (faults from difference slices are coloured differently).

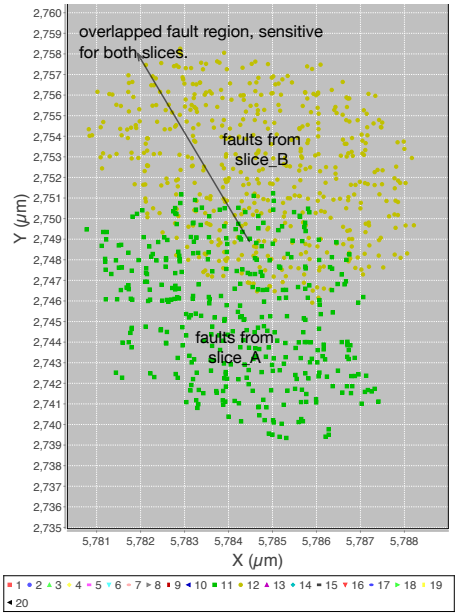


Fig. 8: Slice-exclusive faults for a single CLB.

sensitive to the laser attacks, upon logic bits on devices. These parameters helps to efficiently navigate the laser to the POIs, for performing precise bit-level fault attacks against FPGA implemented ciphers. The estimated regions and dimensions are used in the following subsections.

Discussion of exceptional fault appearance: For some CLB regions, unexpected faults appeared. Note that *fault_2* (denoted as blue dot) is supposed to only appear in CLB_1. However it unexpectedly occurs when the laser targets to CLB_3 also. This phenomenon is mainly because the signal paths for register bit [4-7], that were deployed in slice_2, pass the routing channel close to CLB_3, and hence are affected by laser disturbance on CLB_3.

4.3 Flip-Flop Scan

Recall the mapped device from Fig. 6, we could navigate the laser spot to a specific slice. Without loss of generality, we focus on a particular slice where 4 out of the total 64 round registers of PRESENT are deployed. In this slice registers storing bits 0, 1, 2 and 3 are respectively placed in its 4 flip-flops, and the 4 LUTs inside this slice are unused. In 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 new bitstream. So, no matter if the LUTs are used or not, it does not affect the registers implemented in this 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 laser strength varying between 75%-100%, we have received 3918 faulty encryptions out of 10,000, with 1 injection for 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 the flip-flops that were affected, most of the faults flipped flip-flop `A`, as can be seen in Tab. 2, following similar proportions of faults for the other three flip-flops. In Tab. 3 we can see numbers for different fault models we have obtained. More than one half of all the faults were 1-bit flips, following with $\approx 1/3$ 2-bit flips. 3- and 4-bit flips were less likely to occur, however still possible to obtain. Moreover, with high-precision scan, we can find the POI affecting only one slice without having the laser injecting faults in neighbouring slices.

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

Flip-Flop Laser Sensitive Region Four flip-flops (FF-A, FF-B, FF-C, FF-D) are placed inside each slice in Xilinx FPGAs, therefore each injection could cause multiple bit flips if the laser spot is bigger than the flip-flop scale. We show the faults when 2 adjacent registers flipped in Fig. 9. The red, blue, and green 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 have slight offsets in X axis, and this offset is because the size of the effective laser beam covers two neighbouring registers in most. More specifically, $X1$ and $X2$ constitute middle lines of registers (C, D) and (A, B) in X axis ($X1 \approx 5782.4445\ \mu m$, $X2 = 5781.9900\ \mu m$). 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 register structure varies for devices manufactured with different technologies and devices, therefore this estimation is valid only for the tested Virtex-5 FPGA. However, the analysis solution is applicable to other FPGA devices.

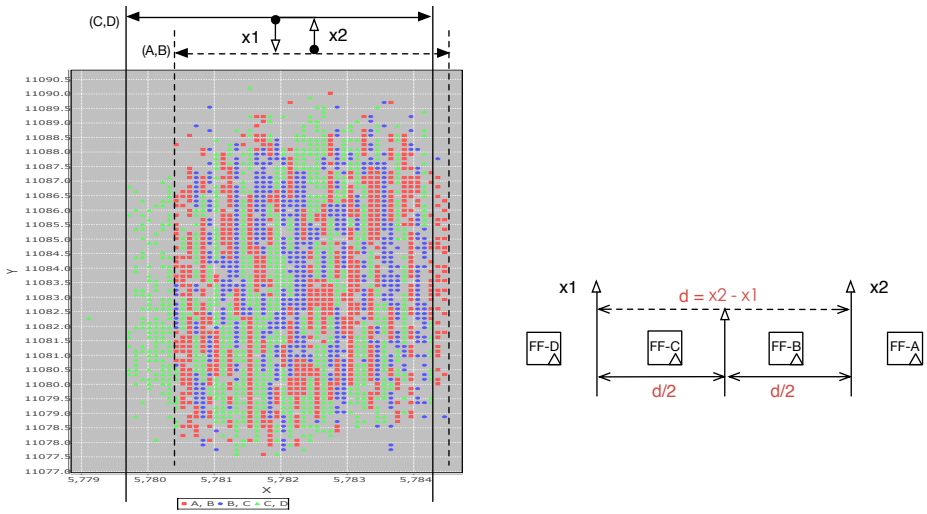


Fig. 9: Estimation of flip-flop laser sensitivity region basing on 2-bit faults from adjacent flip-flops.

As mentioned before, none of the faults were found in the configuration memory. Our laser equipement was operating at its maximum capability, we couldn't fiind advanced parameters to inject configuration faults. This could be due to different structure and/or layer placement for flip-flops and configuration memory.

5 Results and Discussions

In this section, we present more 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 and fault countermeasures. Finally, we shed some light on the invalid faults found in the central region of the FPGA.

5.1 Success Rate

Apart from different kind 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 or random byte faults, etc. The objective is to ascertain the minimum power required for fault injection with each fault model.

The experiment is conducted by injecting laser with varying power in the range 0%–100%. The injection campaign is performed on the POI of a slice region where 4-bit round data registers are implemented in the 4 flip-flops of this slice. 100 injections are performed per laser power, using PRESENT-80 encryption with random plaintext and fixed key. In Fig. 10, it can be observed that faults started appearing at 81% laser power. With $>$ 85% laser power, over 90% injections resulted in faults. The fault injection success is 100%, when laser power is over 96%. These faults included both bit-flips as well as random byte/nibble.

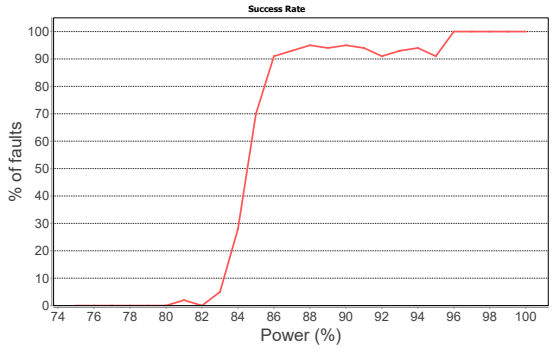


Fig. 10: Fault success rate for random byte flips.

5.2 Discussion on Central Fault Region

A dense fault region appeared in the center of FPGA die. This region is not an active CLB region and no user logic is implemented in this area. The nature of injected faults in this region is also very different from the `valid` fault, i.e., several cores are faulted by 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 in this lens is $15 \times 3.5\ \mu m^2$. The energy density of the 20x lens is higher than that of the 5x lens. We varied the laser power from 17% to 25% of the full laser strength. Fig. 11 gives the fault plot after the laser scan in this section. Points in different colours represent different laser strengths. Most faults are located in two regions, hereafter named `"Region A"` and `"Region B"` respectively. A very few number of faults are seen in some remote spots. A bitstream modification was never observed.

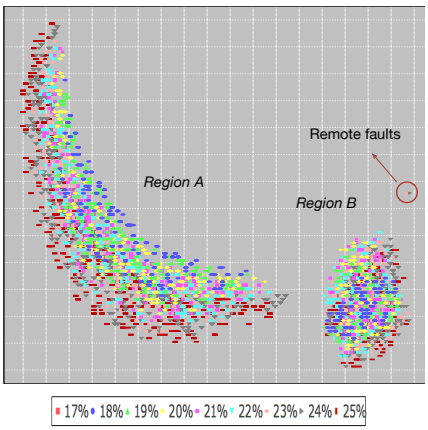


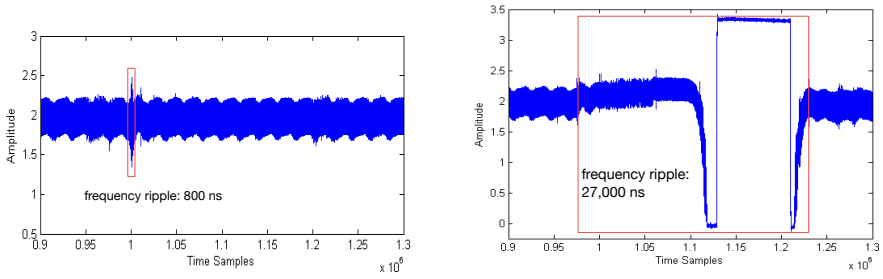
Fig. 11: Position and strength of faults in precise laser scan to the center of FPGA.

Due to the undisclosed transistor-level device information, clarifying the internal mechanism of the faults here is challenging. Even when the cipher and its peripheral logics are placed in far 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 is conducted under two assumptions:

- The faults are triggered by the `global clock network`. Since the clock buffer that fans out the global clock is deployed in the die center, 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 are triggered by the *system monitor*. System monitor is an environment sensor system (power supply, temperature etc.), deployed near the center of 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 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 is composed of a single inverter (LUT) and routing wires, implemented in a CLB region to cover 9 CLBs through square routing, which results in a stable oscillation frequency of 230 MHz. We observed the signal oscillation of the RO from an oscilloscope, and the results are shown in Fig. 12. When the laser is shot in the CLB area, where the RO is deployed, we can see that laser injection disturbs the RO response for a short period of time with a oscillation ripple lasting around 800 ns, and then RO returns to the stable oscillation, as shown in Fig. 12 (a). On the other hand, when the laser is shot on either of `"Region A" or "B"`, the response of the RO is more noticeable. As shown in Fig. 12 (b), the RO stops to oscillate for a bigger period of time of roughly $27,000$ ns. From an oscillating state, the RO response is pulled down to zero and then the RO starts again to oscillate and lock itself. The phenomena can be described as a `soft` reset which occurs probably due to triggering of certain sensors or some impact on the power delivery network, which are not present in the documentation. We call it as soft reset because only the signals are disarmed but flip-flops and logic values are held. We could not carry the analysis further without knowing the architectural details of the commercial FPGA, and the reason for these faults at the center stays an open question.



(a) (b)

Fig. 12: RO response against laser injection targeting (a) CLB area; (b) `Region "A"`, respectively.

6 Conclusions

In this paper, a laser based FPGA profiling technique towards the nanometer-level FPGAs is proposed for exploiting the bottom-level device architecture and

realizing various bit-level fault attacks against cryptographies. The work relies on the diode pulse laser to trigger the bit events from algorithmic data, instead of the widely studied memory configuration bits of FPGAs, as to profile the device architecture and fundamental CLBs basing on the fault sensitivity distribution. Without loss of generality, a Xilinx 65 nm FPGA is selected as the DUT, and a series of laser scan campaigns from the thinned chip substrate lead to successful identification of critical architecture and internal component information. With further fine-grained scan on individual slice region both single- or multiple- data bit faults in flip-flops have been enabled, which are compatible with most differential and algebraic fault attack schemes proposed in previous literatures. The precisely induced bit faults can also compromise fault attack countermeasures like dual-rail logic and parity detection. Not restricted to the studied exemplary device, the proposed techniques could be applied to other FPGAs or programmable SoCs, to perform high-precision bit-level fault attacks against cryptographic primitives. To the best of our knowledge, this is the first work that thoroughly profiled the generic FPGA architecture and fundamental logic unit using laser based fault injection.

The following work will focus on the chip profiling and laser fault perturbation to FPGAs manufactured by 28 nm technology. The practical chip analysis and laser attack to an FPGA chip from a commercial security product will also be a part of further work.

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. Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Advances in Cryptology-CRYPTO'97, pp. 513–525. Springer (1997)
5. 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)
6. 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)
7. 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)
8. 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)
9. 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)

10. 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)
11. Green, M.A.: Self-consistent optical parameters of intrinsic silicon at 300 k including temperature coefficients. Solar Energy Materials and Solar Cells 92(11), 1305 – 1310 (2008)
12. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. pp. 388–397. CRYPTO '99 (1999)
13. Kömmerling, O., Kuhn, M.G.: Design principles for tamper-resistant smartcard processors. Smartcard 99, 9–20 (1999)
14. 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)
15. 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)
16. 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)
17. Quisquater, J.J., Samyde, D.: Eddy current for magnetic analysis with active sensor. In: Esmart 2002, Nice, France (2002)
18. 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)
19. 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)
20. Schmid, P.E.: Optical absorption in heavily doped silicon. Phys. Rev. B 23, 5531–5536 (1981)
21. Selmke, B., Brummer, S., Heyszl, J., Sigl, G.: Precise laser fault injections into 90nm and 45nm SRAM-cells. In: CARDIS. pp. 1–13 (2015)
22. Trimberger, S.M., Moore, J.J.: Fpga security: Motivations, features, and applications. Proceedings of the IEEE 102(8), 1248–1265 (2014)
23. 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)
24. Wang, H., Liu, X., Zhang, Z.: Absorption coefficients of crystalline silicon at wavelengths from 500 nm to 1000 nm. International Journal of Thermophysics 34(2), 213–225 (2013)