Precise Laser Fault injections into 90 nm and 45 nm SRAM-cells

Bodo Selmke[1], Stefan Brummer[1], Johann Heyszl[1], and Georg Sigl[2]

[1] Fraunhofer Institute for Applied and Integrated Security
[2] Technische Universität München,
Department of Electrical and Computer Engineering

Abstract. In the area of fault attacks, lasers are a common method to inject faults into an integrated circuit. Against the background of decreasing structure sizes in ICs, it is of interest which fault model can be met with state of the art equipment. We investigate laser-based fault injections into the SRAM-cells of block RAMs of two different FPGAs with 90 nm and 45 nm feature size respectively. Our results show that individual bit manipulations are feasible for both, the 90 nm chip and the 45 nm chip, but with limitations for the latter. To the best of our knowledge, we are the first to investigate laser fault injections into 45 nm technology nodes. We provide detailed insights of our laser equipment and the parameters of our setup to give a comparison base for further research.

Keywords: laser-based fault injection, SRAM, high-precision, comparing 45 nm and 90 nm

1 Introduction

Electronic devices used for information security are prone to many different attacks, like e.g. probing attacks, side-channel attacks, reverse-engineering, and fault attacks. Fault attacks aim to corrupt the intended functionality of an electronic device. Faults can be generated using many different methods [3,6]. A simple method are so-called glitching attacks, where the supply voltage or clock signal of an integrated circuit is interfered for a very short time period. This does not allow any control over the location of the injected fault since every element of the circuit could be affected. For this reason, the use of laser systems has become popular. Lasers enable the injection of highly localized faults in an integrated circuit. The generated faults can be exploited in various ways: Faults can be used to circumvent simple security checks such as password verifications, but also for highly sophisticated fault attacks against cryptographic implementations. Differential Fault Attacks (DFA) try to recover a secret key by comparing the regular output of the algorithm to a falsified one. Regardless of the actual attack method, from a designer's perspective it is important to know whether an attacker is able to perform manipulations with a sufficient precision.

The fault model describes the properties of a fault in terms of timing, location, number of affected bits and the type of the bit-fault (bit-flip or forcing a specific value). Generic fault attacks (like e.g. Safe Error Attacks) or many early published DFAs as e.g. Giraud's attack on the AES [7] require to comply with a strict fault model. More advanced attacks require less demanding fault models, such as the DFA on AES by Saha et al. [10] which can cope with an arbitrary amount of bit faults within up to 12 bytes of the AES state in one round of the computation. In general an attack method is more powerful the lower the requirements on precision, allowing an attacker with less precise equipment to successfully mount an attack.

However, from a practical point-of-view, the capability to inject faults with a high precision is crucial for two reasons. First, it grants the flexibility to carry out a greater variety of fault attacks. Second, the presence of countermeasures in security devices ask for precise fault injections. Countermeasures against fault attacks can be divided into two classes: The direct detection of the actual fault injection by sensors (e.g. light sensors), and the detection by a redundant operation of the algorithm, e.g. using duplicated circuits to detect injected faults. In both cases, an increased precision of laser-based fault injection (LFI) is necessary to circumvent these countermeasures. Light sensors require additional space on the die and cannot be placed arbitrarily close to critical elements. Therefore they are possibly not triggered by highly localized fault injections. In order to circumvent the detection by duplicated circuit parts, with an increased precision it is more likely to inject the same fault in both parts. Therefore this topic is of special interest for the security chip industry.

In this contribution we investigate the achievable precision of fault injection into SRAM-cells using a state of the art laser system. We use two different high-volume FPGAs (Xilinx Spartan-3A and Spartan-6), and target the Block RAM (BRAM), which consists of a regular and dense array of SRAM-cells. Since SRAM-cells are composed of two cross-coupled inverters, the smallest gates used in CMOS logic, BRAMs are well-suited as test target to judge the LFI precision. The observed results are also interesting for the secure implementation of cryptographic algorithms in FPGAs, as efficient implementations make exhaustive use of available BRAMs [5]. However, in our opinion the derived conclusions are also generalizable for SRAM-cells on ASICs, fabricated in similar technologies. Our investigations show that the precision is sufficient to set single bits to specific values in the 90 nm Xilinx Spartan-3A under the condition, that focal plane and energy are precisely calibrated. On the 45 nm Xilinx Spartan-6, the precision decreases and in most fault injections single bits cannot be manipulated without affecting the adjacent memory cells. Nevertheless, single bit faults are still observable to a small extent and the capability to set a specific bit to a certain value is not limited.

Outline After giving a summary of related work in Sect. 2, we describe our laser fault injection setup in Sect. 3. Our experimental results are based on the test devices described in Sect. 4. The results are presented and discussed in Sect. 5. Eventually, we propose considerations for secure implementations in Sect. 6.

2 Related Work

Several papers already provided information about the achievable precision of LFI so far. We extend this current state with results for smaller feature sizes of 90 nm and 45 nm. In contrast to previous publications, we specify our setup in detail to provide a solid comparison base.

Dutertre et al. show that attacks based on single-byte faults are feasible in an SRAM-memory of a microcontroller manufactured in a 350 nm process. Using the same setup and the same device, Agoyan et al. [2,1] were able to improve this to single bit-faults. Unlike us, their results were achieved by a front-side LFI, using a wavelength of 532 nm and a spot-size of 4 µm on a chip with a much larger feature size.

Roscian et al. [9] stated that they inject single bit-faults in the memory of a microcontroller with 250 nm feature size. They use an infrared laser with 1064 nm wavelength, a spot size stated as 1 µm and a pulse length of 50 ns. In contrast, we are able to show that faults with this precision are still feasible with a larger spot size of 4 µm on devices with considerably smaller structures.

Courbon et al. [4] show that selective single-bit faults are feasible in a 90 nm microcontroller. Their setup uses a laser wavelength of 1064 nm at variable pulse lengths of down to tens of ns and a spot size of 2 µm. Though they also use a chip with 90 nm feature size, their results differ from ours in the fact that they investigate flip-flops, which consist of more transistors than SRAM cells and are therefore larger in total size. They state that the flip-flops they attacked have an approximate size of 15 μm^2, while the 90 nm SRAM-cells we attack are much smaller with a size of 3.25 μm^2. In addition they use a spot size stated as 2 µm, while we are able to show that even with a spot twice as large selective single bit faults are feasible.

Roscian et al. [8] perform a front-side fault injection with 532 nm wavelength, using very large spots of 100 µm on a 130 nm chip. They show that single-bit faults are feasible with this setup and argue that this is due to refraction of large parts of the beam. Unlike us, they do not have full control over the fault, by relying on the refraction of the metal layers.

3 Setup and Calibration

This paper examines the achievable fault injection precision in two different feature sizes. In our opinion a detailed description of the employed setup is crucial for comparable results. For this reason, we provide a detailed setup specification in this section.

3.1 Setup Overview

The experimental results in this paper are generated using a LFI-setup which is based on a diode-pumped Nd:YAG solid-state laser source, which is capable of emitting two different laser wavelengths, 532 nm and 1064 nm. An adjustable beam attenuator enables accurate control over the emitted beam energy. The pulse length of the laser source is fixed at 800 ps and supports a maximum repetition rate of 1 kHz.

In this contribution, we focus on fault injections through the backside of the die, which is common practice to avoid refraction by the metal layers of the chip. Therefore we use the 1064 nm wavelength, as it is absorbed less by the silicon substrate. To adjust the width of the collimated beam of the laser source, the beam is passed through a beam expander. By changing the beam width, the resulting spot size of the beam behind the focusing lens can be adjusted. A subsequent laser scanner supports precise and fast lateral deflection of the beam for precise control over the fault injection position. The scanner is capable of shifting the beam position within a range of ±0.25 mm on the DUT at a precision of 100 nm. Subsequently, for the visual inspection of the DUT, a digital camera is coupled in. The final element in the optical path is a 20× zoom-lens to focus the laser beam on the DUT. In order to position the DUT under the lens accurately, an *xyz*-table enables to move it in three spatial directions and to correct the tilt.

Total Energy Output The total energy output of the system was measured with a laser energy sensor for the range of 1 nJ up to 5 µJ. To retrieve measurement values that include all losses in the optical system, the sensor was placed under the focusing lens. It turned out that the emitted energy is heavily dependent on the adjusted spot size. Hence, we took samples of energy versus attenuator position for each spot size we wanted to use as shown in Fig. 1. The plotted curves are averaged over 30 samples. We observed a deviation from the mean values of <10 % at maximum.

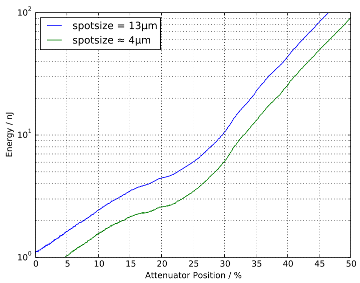


Fig. 1: Measured laser energy at DUT over attenuator settings and for two different spot-size settings

Spot Size To measure the spot size of our laser, we used a monochrome CMOS camera sensor with a pixel size of 1.67 µm. The laser beam is focused on the surface of the sensor using the camera and pulsed with the maximum frequency of 1 kHz. Subsequently the distance of the DUT to the lens was leveled to the point where the minimum spot size was obtained.

The radius of a laser beam is physically defined by the $1/e^2$ ($\approx 13.5\,\%$) drop of the intensity, which can be measured with the sensor. Ideally the energy output is adjusted so that the beam center drives the CMOS sensor into saturation to use the full range of resolution. In Fig. 2, the sensor output for the largest and the smallest spot sizes of our setup is shown. For the small spot it was not possible to determine the size computational. We estimated the size to be about 4 µm.

It is important to note, that the physical spot size is not equal to the effected area on the die. Since the local energy density of the beam must reach a certain value to produce faults, the effective spot size may be larger or smaller depending on the total energy.

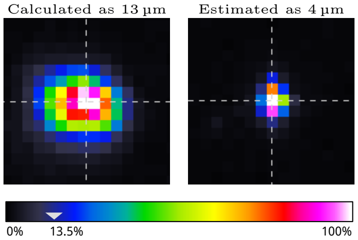
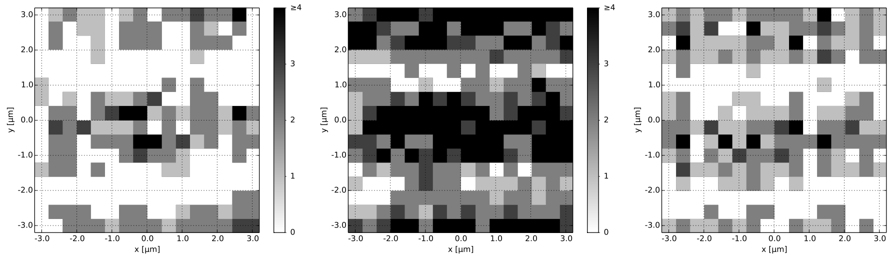


Fig. 2: Laser energy distribution and derived spot-size

Calibration of Focal Plane We chose to inject faults from the backside of the die. To achieve a minimal spot size in the active layers of the die, we have to set the focal plane below the surface. However, the exact thickness of the die, as well as the doping which influences the absorption in the silicon, is unknown. For this reason we empirically determined the optimal distance (z-axis) of the lens to the die.

In order to find the optimal focal plane, we used the effect in the BRAM of the FPGA as an indicator. We scanned a small area of the BRAM at different focal plane settings in a range from the surface to 150 µm below the surface. The optimal focal plane is corresponding to the maximum total number of generated bit-faults per scan. Since the roughly required energy in the focal plane was unknown, we started this procedure with the minimum energy output to avoid damaging the chip. As long as no faults were detected, the energy output was increased after each iteration.

It has to be noted, that this procedure may be unfeasible for actual attackers, since the observability of cells is usually not possible. Alternatively, an infrared camera can be used to adjust the focal plane. Fig. 3 depicts the results of LFIs at different z-offsets (distance from the surface) as an example for the above described procedure: Each scan position is colored with a gray value corresponding to the number of bit-faults observed at this location. In relation these figures indicate how the total number of generated bit-faults changes with the shift of the focal plane. It can be observed that from 74 µm to 79 µm (Fig. 3a and Fig. 3b) below the surface the total number of bit-faults increases, and with an additional shift to 84 µm this number decreases again. Therefore the optimal focal plane is located at around 79 µm. For the results shown in Sect. 5.2 and 5.3 implicitly the thus determined optimal focal planes were used.



(a) z-offset 74 µm (b) z-offset 79 µm (c) z-offset 84 µm

Fig. 3: Spartan-6: Fault injection results for different focal planes at 1.5 nJ pulse energy and 4 µm spot-size

4 Devices Under Test

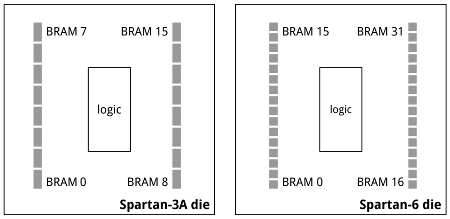


Fig. 4: Spartan-3A and Spartan-6 floorplan with location of the BRAM hard macros and placement of the logic

We chose BRAMs on FPGAs as target for our investigation for two reasons. First, the FPGA grants full control over the memory. The BRAM blocks can be exclusively used for evaluation of the LFI because they do not hold any program data, as it might be in the case of microcontrollers. Second, SRAM-based FPGAs are manufactured in a standard CMOS process, the results should therefore be comparable to ASICs. We expect that the SRAM-cells within the BRAM are designed as small as possible in the respective technologies and thus the results should provide a good base for generalization. We use two Xilinx FPGAs, the Spartan-3A with a feature size of 90 nm and the Spartan-6 with 45 nm. Those features sizes are interesting since they are similar to the ones used in contemporary security chips.

On both FPGAs all available BRAM blocks are instantiated and made accessible over a serial interface to the PC. We configure the BRAMs to be organized in 2048×9 bits in every word and include the 9^{th} bit, which is intended for the use as parity bit, while reading out the BRAM. Fig. 4 depicts the floorplans of both FPGA dies taken from the Xilinx design tools and showing the approximate locations of the BRAM blocks. To avoid errors in the logic of the design, all elements except for the BRAM hard macros are placed in the center of the FPGA.

Locating BRAM Blocks Since the actual location of the individual BRAM blocks is only roughly known by the information provided by the Xilinx design tools (compare Fig. 4), the exact location on the die had to be experimentally determined. This step is achieved by a coarse (20 µm step size) scan of a larger area on the die. The focal plane is set to the surface, since the optimal plane is unknown at this point. For the Spartan-3A, a pulse energy of about 10 nJ was required to inject faults, while for the Spartan-6, at least 35 nJ were necessary. As energies as low as 1 nJ are sufficient to inject faults in the optimal focal plane for both FPGAs (compare Sect. 5), we assume that this difference is mainly due to differences in the substrate thickness and doping.

BRAM Block Dimensions Once the locations of the BRAMs were roughly known, we determined their dimensions on the die. On the Spartan-3A the BRAM block covers an area of 300 µm×200 µm, while for the Spartan-6 the BRAM block size shrinks to 150 µm×200 µm. Thus the actual size of the BRAM shrinks only by a factor of two. Calculated from these values, the approximate size of a single SRAM cell is 3.25 µm^2 on the Spartan-3A and 1.62 µm^2 on the Spartan-6.

5 Experimental Results

For our investigation on the achievable precision of LFIs, we concentrate on a small part of the BRAM with a size of 8 µm×8 µm. The test position is varied using a step size of 200 nm. The laser spot size is set to the minimum of 4 µm with a calibrated focus level (refer to Sect. 3.1).

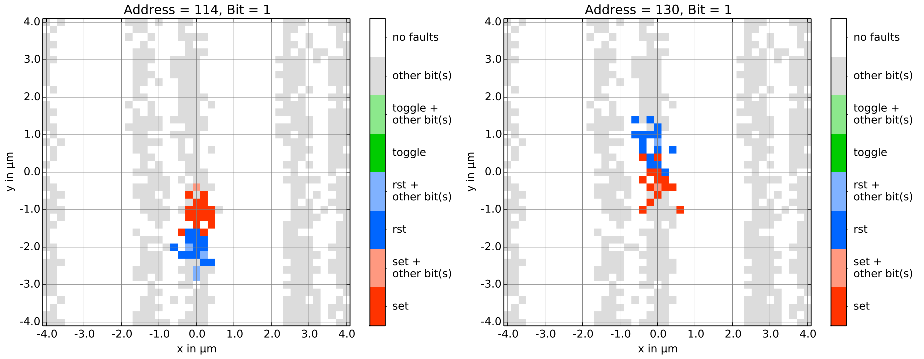
5.1 Test Procedure

For all following results, we use the below test procedure with two consecutive laser shots for each position during a scan:

1. Preload all BRAM bits with 0
2. Inject a single laser shot
3. Read back values and detect *set-faults*
4. Preload all BRAM bits with 1
5. Inject a single laser shot
6. Read back values and detect *reset-faults*

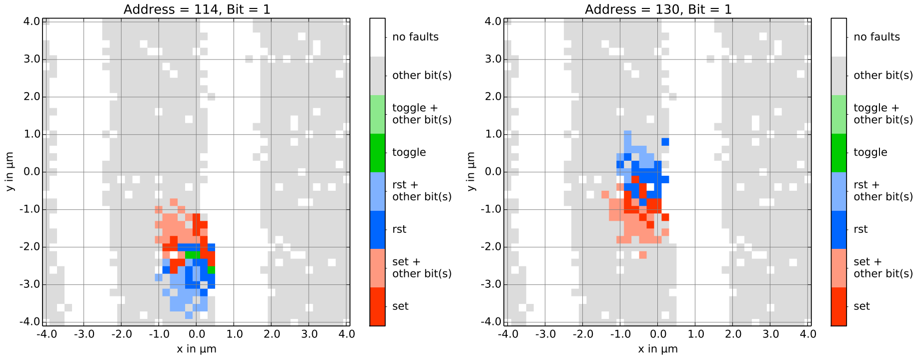
By preloading the BRAM with all 0 as well as all 1, we can detect both possible cases of bit faults: If bits can be *set* to 1, so-called *set-faults*, and if bits can be *reset* to 0, so-called *reset-faults*. At each scan position, we evaluate the results of comparing the preloaded to the read-back values. There are three general cases which we distinguish *for every bit and at every position.*

fault type	**color**	**description**
set	red	The specified bit can be set to 1 at this position
reset	blue	The specified bit can be set to 0 at this position
toggle	green	The specified bit was set to 1 in the first shot, but also to 0 in the second



(a) Result for bit 1 of address 114 (b) Result for bit 1 of address 130

Fig. 5: 90 nm Spartan-3A: LFI into single bit at 1 nJ pulse energy



(a) Result for bit 1 of address 114 (b) Result for bit 1 of address 130

Fig. 6: 90 nm Spartan-3A: LFI into single bit at 1.5 nJ pulse energy

Since we are primarily interested in the ability to precisely target specific bits exclusively, the presented figures each concentrate on single specific bits and we show maps of the scan results where the results for *one specific bit* for all scan positions are plotted. To indicate, whether bits are hit *exclusively*, or whether other bits have been affected by the shot at this position, we use pale colors instead of solid ones. Additionally, grey colored positions in the figures indicate, that another bit has been affected by the fault injection, but not the targeted bit. *If an attacker aims at injecting precise set- or reset-faults into specific bits exclusively, only the positions in the scan map which are colored in solid red and blue are eligible.*

5.2 Results on 90 nm Spartan-3A

We repeatedly carried out the test procedure described in Sect. 5.1 on the 90 nm Spartan-3A for decreasing energy outputs. In Fig. 6 and Fig. 5 the results for the energy levels of 1.0 nJ and 1.5 nJ are depicted. Thereby we evaluated the captured data for two arbitrary adjacent bits, which are located in the center of the scanned area.

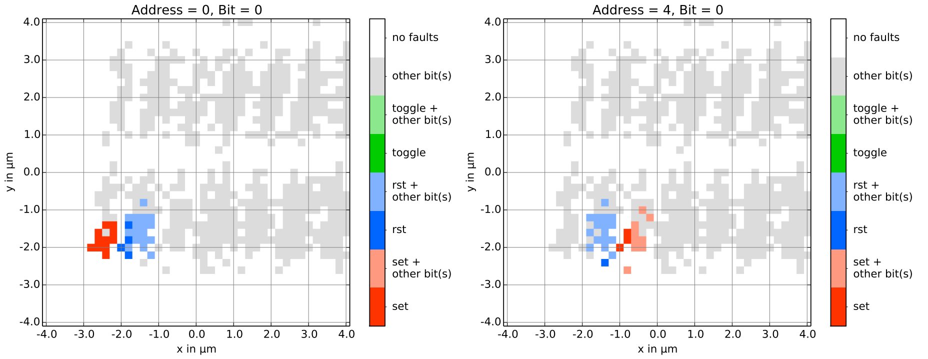
Regarding the results for energy output of 1.0 nJ depicted in Fig. 5, it is observable that the fault injection achieved a very high overall precision. Almost all test locations induced only single bit faults, as indicated by the solid red and blue colors. In addition, there are specific zones that either generate a *set-fault* or a *reset-fault*. The third fault-type, toggling the bit value, does not appear. This result is in line with the results of Roscian et al. [9]. Their model-based analysis of LFI into SRAM-cells indicates, that toggling a bit is generally unfeasible. Furthermore there are some irregularities in the distribution of the sensitive zones. By comparison of the results for both vertically adjacent bits in Fig. 5b and Fig. 5a, it can be seen that the fault sensitive zones of these bits are mirrored. Horizontally adjacent bits, by contrary, are arranged in pairs with the same orientation of sensitive zones. These pairs are separated by notably wider gaps in between to neighboring pairs. These observations are probably due to layout optimizations, i.e. the sharing of doped wells and supply lines (V_{DD}, Gnd). Against the background of the research of Sarafianos et al. [13,12,11], who showed that NMOS transistors are more sensitive to LFI than PMOS transistors, we assume that in the wide fault insensitive gaps the PMOS transistors of the SRAM-cells are located and the energy is not sufficient to trigger them.

The results obtained at an energy output of 1.5 nJ (Fig. 6) show an increased effect area of the laser spot in comparison to the results for 1.0 nJ. Unlike for the previous results, the ability to inject single-bit faults depends on the location. The sensitivity zones for vertically adjacent bits are partly overlapping, hence at most locations both bits are affected. In the results for 1.5 nJ there are some locations which induced set-faults and reset-faults (green color), however this pattern does not regularly appear. Thus we assume, the reason is a slight variation of the test position between both laser shots.

As a conclusion, we find that precision is generally higher with lower energy values as long as the energy is still sufficient for fault injection. This can be explained by the fact, that at lower energies, and if correctly focused, the effective spot-size within the active layer decreases. Regarding the Spartan-3A, it is obvious that with this setup and calibration, specific targeted bits can be set to specific values without interfering other bits.

5.3 Results on 45 nm Spartan-6

For the 45 nm Spartan-6, we carried out the same experiments with identical settings. A comparison of the results for the two different energy levels shows a similar effect as for the Spartan-3A, i.e. an improvement in precision for the lower energy of 1 nJ. Fig. 7 shows the results for the energy level of 1 nJ, evaluated



(a) Result for bit 0 of address 0

(b) Result for bit 0 of address 4

Fig. 7: 45 nm Spartan-6: LFI into single bit at 1 nJ pulse energy

for two adjacent bits. Similar to the results of the Spartan-3A, we observed areas which are either *set* or *reset* sensitive and mirrored for adjacent bits. Comparing the results of the Spartan-6 with the Spartan-3A, it can be seen that significantly less single-bit faults are achieved with identical settings, as the *set*, resp. *reset* sensitive areas of adjacent bits are still overlapping. Thereby the area that has influence on a specific bit stays approximately the same size as for the Spartan-3A. We assume that further reduction of the energy would increase the precision, but could not prove this due to the limitations of our setup regarding lower energies.

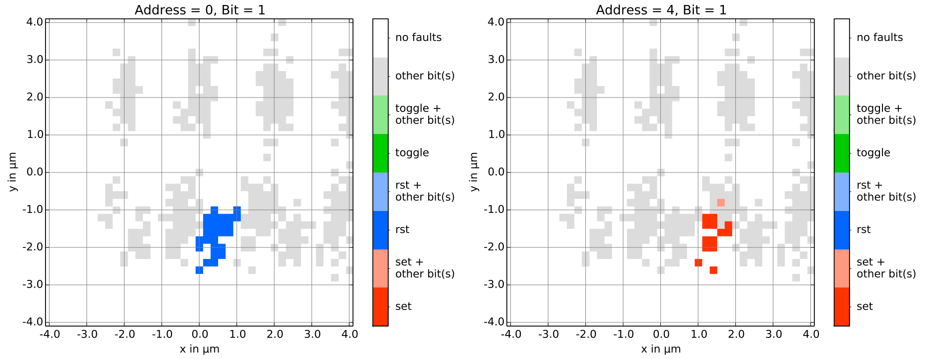
As an important observation, Fig. 7a shows that for address 0, bit 0 exclusive *set-faults* are achieved more likely. This is due to the fact that this bit is located at the boarder of the BRAM and has no adjacent bit on the left side, thus it does not share its *set* sensitive area with any other bit. Analyzing the BRAM layout revealed that such a bit is existent for every second address and will either affect index 0 or 7 (1024 bits in total).

5.4 LFI Precision Depending on Stored Values

In the previously described experiments, the memory cells have been preloaded with the same bit values, i.e. either all 0 or all 1 during the fault injection. Since adjacent bits have mirrored *set* and *reset* sensitive regions, this can be seen as a worst case scenario while trying to affect bits exclusively. Attackers can achieve a better precision if adjacent bits store complementary values.

We tested this in an additional experiment on the Spartan-6 and preloaded complementary values to adjacent bits. For the results shown in Fig. 8, all bits of address 0 are preloaded with 1, while all other bits are preloaded with 0. Therefore we can only observe reset-faults for bits of address 0 in the evaluation, and set-faults for all bits corresponding to other addresses.

Contrary to our previous results presented in Fig. 7, we can observe exclusive single-bit faults depicted in Fig. 8. Fig. 8a concentrates on the bit with index



(a) Bit 1 of address 0 is *reset* without affecting other bits

(b) Bit 1 of address 4 is *set* without affecting other bits

Fig. 8: 45 nm Spartan-6: Bits are preloaded with different values before LFI into single bits at 1 nJ pulse energy

1 at address 0 and shows that it is *exclusively reset* at many positions which are marked as solid blue. The reason for this is that the bit shares its *reset*-sensitive zone with another horizontally adjacent bit, namely the bit with index 1 at address 4, which already contains the value 0 and is therefore not affected. Fig. 8b concentrates on the bit with index 1 of address 4 and shows that it is *exclusively set* at many positions which are marked as solid red. The reason for this is that the bit shares its *set*-sensitive zone with another horizontally adjacent bit, namely the bit with index 2 at address 0, which already contains the value 1 and is therefore not affected.

As a conclusion for a feature size of 45 nm *we show that single-bit faults must still be considered feasible, although the achieved precision is lower in general. This is particularly due to the observation that feasibility is dependent on the values stored in the adjacent SRAM cells.*

6 Considerations for Secure Implementations

If an error detection or correction code is used against LFI, it should respect the specific memory layout. Cells which share common doped wells will likely be affected by faults in the same way:

- It is likely, that both cells will contain the same value after the laser injection.
- It is unlikely that both adjacent bits change their values if they had different values before.
- If adjacent cells belong to the same word, it is likely that more than one bit of a word is affected at once.

In this way, the organization of cells has a high impact on the fault model from LFI. Such information can be valuable to *design or configure efficient error* *correction codes* for secure implementations. Also simple redundancy measures in software can be made more effective with these considerations and the actual arrangement of the memory cells in mind.

Bits which are stored in SRAM cells that are located at the borders of BRAM hard macros will likely not share one of their sensitive regions. Therefore, an attacker will have a better chance to exclusively set them to either 0, or 1, depending on the location. *For a secure implementation, this means that data such as cryptographic keys, for whom there e.g. exist attacks based on exclusively setting some bits to certain values, should rather not be stored in such cells.*

7 Conclusion

In this work we have shown, how precise faults can be injected into the BRAM of two state-of-the-art FPGAs with feature sizes of 90 nm and 45 nm. Thereby we extend the state of publication with results for 45 nm. Our results indicate that the achievable precision is sufficient to enable the manipulation of specific single bits for 90 nm structures. As a result fault attacks with the most strict fault model are feasible. E.g. Safe-Error attacks successively setting individual bits to a specific value are feasible.

In case of the 45 nm chip, it is more difficult to attack a single bit without influencing an adjacent bit. Although it is definitely feasible to generate single-bit faults, this is only possible at a lower success rate, heavily depending on the state of the adjacent cells. The capability to set a specific bit to specific value is however equally to the 90 nm device.

In order to achieve such precision, the careful tuning of the system parameters is essential. For this reason, we thoroughly specified our setup to allow future comparison.

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: Technologies for Homeland Security (HST), 2010 IEEE International Conference on. pp. 113–119 (Nov 2010)
2. Agoyan, M., Dutertre, J., Mirbaha, A., Naccache, D., Ribotta, A., Tria, A.: How to flip a bit? In: 16th IEEE International On-Line Testing Symposium (IOLTS 2010), 5-7 July, 2010, Corfu, Greece. pp. 235–239 (2010), http://doi.ieeecomputersociety.org/10.1109/IOLTS.2010.5560194
3. Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., Whelan, C.: The sorcerer's apprentice guide to fault attacks. IACR Cryptology ePrint Archive 2004, 100 (2004), http://eprint.iacr.org/2004/100
4. Courbon, F., Loubet-Moundi, P., Fournier, J.J.A., Tria, A.: Adjusting laser injections for fully controlled faults. In: Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers. pp. 229–242 (2014), http://dx.doi.org/10.1007/978-3-319-10175-0_16

5. Drimer, S., Güneysu, T., Paar, C.: Dsps, brams and a pinch of logic: New recipes for AES on fpgas. In: 16th IEEE International Symposium on Field-Programmable Custom Computing Machines, FCCM 2008, 14-15 April 2008, Stanford, Palo Alto, California, USA. pp. 99–108 (2008), http://dx.doi.org/10.1109/FCCM.2008.42
6. Dutertre, J.M., Fournier, J., Mirbaha, A.P., Naccache, D., Rigaud, J.B., Robisson, B., Tria, A.: Review of fault injection mechanisms and consequences on countermeasures design. In: Design Technology of Integrated Systems in Nanoscale Era (DTIS), 2011 6th International Conference on. pp. 1–6 (April 2011)
7. Giraud, C.: DFA on AES. In: Advanced Encryption Standard - AES, 4th International Conference, AES 2004, Bonn, Germany, May 10-12, 2004, Revised Selected and Invited Papers. pp. 27–41 (2004), http://dx.doi.org/10.1007/11506447_4
8. Roscian, C., Dutertre, J., Tria, A.: Frontside laser fault injection on cryptosystems - application to the AES' last round -. In: 2013 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013, Austin, TX, USA, June 2-3, 2013. pp. 119–124 (2013), http://dx.doi.org/10.1109/HST.2013.6581576
9. Roscian, C., Sarafianos, A., Dutertre, J., Tria, A.: Fault model analysis of laser-induced faults in SRAM memory cells. In: 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography, Los Alamitos, CA, USA, August 20, 2013. pp. 89–98 (2013), http://dx.doi.org/10.1109/FDTC.2013.17
10. Saha, D., Mukhopadhyay, D., Chowdhury, D.R.: A diagonal fault attack on the advanced encryption standard. IACR Cryptology ePrint Archive 2009, 581 (2009), http://eprint.iacr.org/2009/581
11. Sarafianos, A., Gagliano, O., Lisart, M., Serradeil, V., Dutertre, J.M., Tria, A.: Building the electrical model of the pulsed photoelectric laser stimulation of a pmos transistor in 90nm technology. In: Physical and Failure Analysis of Integrated Circuits (IPFA), 2013 20th IEEE International Symposium on the. pp. 22–27 (July 2013)
12. Sarafianos, A., Gagliano, O., Serradeil, V., Lisart, M., Dutertre, J.M., Tria, A.: Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology. In: Reliability Physics Symposium (IRPS), 2013 IEEE International. pp. 5B.5.1–5B.5.9 (April 2013)
13. Sarafianos, A., Roscian, C., Dutertre, J., Lisart, M., Tria, A.: Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell. Microelectronics Reliability 53(9-11), 1300–1305 (2013), http://dx.doi.org/10.1016/j.microrel.2013.07.125