IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2022, No. 4, pp. 862–885. DOI:10.46586/tches.v2022.i4.862-885

On the application of Two-Photon Absorption for Laser Fault Injection attacks

Pushing the physical boundaries for Laser-based Fault Injection

Bodo Selmke[1] *, Maximilian Pollanka[2] *, Andreas Duensing[2],

Emanuele Strieder[1], Hayden Wen[2], Michael Mittermair[2],

Reinhard Kienberger[2] and Georg Sigl[1,3]

[1] Fraunhofer Institute for Applied and Integrated Security (AISEC), Munich, Germany
firstname.lastname@aisec.fraunhofer.de
[2] Technical University of Munich (TUM), Chair for Laser and X-ray Physics, Munich, Germany
firstname.lastname@tum.de
[3] Technical University of Munich (TUM), Chair of Security in Information Technology, Munich, Germany firstname.lastname@tum.de

Abstract. Laser Fault Injection (LFI) is considered to be the most powerful semi-invasive fault injection method for implementation attacks on security devices. In this work we discuss for the first time the application of the nonlinear Two-Photon Absorption (TPA) effect for the purpose of LFI. Though TPA is an established technique in other areas, e.g. fluorescence microscopy, so far it did not receive any attention in the field of physical attack methods on integrated circuits. We show that TPA has several superior properties over the regular linear LFI method. The TPA effect allows to work on non-thinned devices without increasing the induced energy and hence the stress on the device. In contrast to regular LFI, the nonlinearity of the TPA effect leads to increased precision due to the steeper descent in intensity and also a vertically restricted photoelectric effect. By practical experiments, we demonstrate the general applicability of the method for a specific device and that unlike a regular LFI setup, TPA-LFI is capable to inject faults without triggering a latch-up effect. In addition we discuss the possible implications of TPA-LFI on various sensor-based countermeasures.

Keywords: Laser Fault Injection · Countermeasures · Single-Photon Absorption · Two-Photon Absorption · Fault Attacks

1 Introduction

Physical attacks on embedded systems are relevant in scenarios where cryptographic keys are used on devices to which an attacker has direct access. In general, two main classes of attack methods can be distinguished in the area of physical attack methods: Side Channel Attacks (SCAs) and Fault Attacks. SCA is classified as a *passive* attack method, since it relies on the observation of environmental parameters of a device during its operation. Most prominent methods are the measurement of the power consumption or the dissipated electromagnetic field. Fault Attacks are *active* attacks, since they aim at tampering the normal operation of a device by altering processed data or instructions. These faults can

*Both authors contributed equally

Received: 2022-04-15 Accepted: 2022-06-15 Published: 2022-08-31

be exploited in various ways by an attacker. Skipping of instructions can allow to bypass security mechanisms, like a certificate check or the setting of a device configuration value. Fault attacks on cryptographic algorithms were invented in the late '90s [BDL97] and allow to determine the device internal secret by observing the reaction of the device to the fault injection. E.g. Differential Fault Attacks (DFA) allow to compute the key from the differential in the output of the same encryption (or decryption) with and without fault injection (cf. [TMA11]). Statistical Fault Attacks (cf. [Fuh+13; Dob+18]) allow to determine the used key by a statistical analysis of the output.

For the injection of faults a multitude of methods were established, differing in precision and cost of the required equipment. The most inexpensive method are glitching attacks, where the attacker manipulates the core voltage or the clock frequency. However this approach has some disadvantages: The attacker cannot restrict the attack to specific parts of a device, hence he might trigger unintended side-effects. Also this means it is relatively easy to design countermeasures which block this attack vector. A more localized effect can be achieved with Electromagnetic Fault Injection (EMFI). This method utilizes a small coil to generate a short electromagnetic pulse which induces currents in the device under test (DUT). Interestingly, in comparison to glitching attacks this technique is also much easier to use in practice, since it only requires the placement of the injection coil, but no modifications of the device are necessary. The most precise method for fault injection is the use of focused Laser beams. Originally, this technique was developed to simulate radiation effects in Integrated Circuits (ICs) [Hab65], since the usage of Laser systems is more viable and cost effective than usage of a particle accelerator. In 2002 Skorobogatov et al. [SA02] showed, that LFI is well suited for Fault attacks. Since then, LFI has marked the benchmark for Fault Injection, as it allows to inject faults with maximum feasible precision in both timing and location on the chip. In the hardware security community, LFI was for now always restricted to the usage of the linear photoelectric effect, which is based on the absorption of a single photon. By the use of single-mode Lasers and objectives with high numeric apertures, this already allowed very precise fault injections, e.g. single bit manipulations in SRAMs or registers (cf. [Sel+15; SHS16]). With regard to state-of-the-art technology nodes, conventional LFI is however reaching its limits. Fault injection using the two-photon absorption effect is able to push this boundary, but did not receive any attention in the scientific hardware security community so far. Hence, in this work we want to introduce the topic of LFI using two-photon absorption and discuss its impact for the field of hardware security.

Contribution. We analyze for the first time the TPA effect in the context of LFI attacks.

Firstly, we provide a thorough explanation of the underlying non-linear physical effects. The properties of the effects are compared to the characteristics of a state-of-the-art linear Single-Photon Absorption (SPA)-LFI setup.

Secondly, we solidify the results by examining the theoretically appealing properties of TPA using two ARM Cortex-M0 microcontrollers. We provide, for the first time in the cryptographic context, results which prove the feasibility of an injection using TPA. Practical results are provided, showing the effect of transparency of the TPA effect when applied to silicon. Moreover, we show that TPA can be seen as an alternative injection method to circumvent the triggering of unintended latch-up effects.

Finally, we reiterate state-of-the-art countermeasures which promise to mitigate SPA-LFI. We provide notion about the possible impact of TPA on these countermeasures and discuss limitations of the technique. Based on our results, we conclude that TPA-LFI is a viable alternative to commonly used laser sources, and has to be investigated further, especially with respect to circumvention of countermeasures.

Outline. The remainder of this work is structured as follows: In Section 2 we discuss the physical theory behind the nonlinear two-photon absorption process. Section 3 describes the setup built to investigate this effect on two exemplary microcontrollers. The results from these experiments are presented in Section 4. Subsequently we discuss the impact of fault injection by TPA in Section 5. In Section 6 we discuss practical limitations of TPA for LFI. Section 7 concludes the paper.

2 Theory

In this section we will discuss the physics behind LFI and the TPA process and give a short overview of the electrical effects in silicon.

2.1 Laser silicon interaction

In general one can distinguish between single-photon absorption and two-photon absorption as two mechanisms for the excitation of an electron from the valence band (VB) into the conduction band (CB) by photons, depending on their energy, as described theoretically in the next sections [F G07]. The photon energy of monochromatic laser light is governed by Planck's equation and can be generalized as follows:

$$E = h\nu = \frac{hc}{\lambda}, \tag{1}$$

where E represents the energy of a photon, h the Planck's constant, ν the laser frequency, λ the laser wavelength and $c = \lambda\nu$ the speed of light [F G07].

For photon energies being equal or greater than the direct bandgap of an illuminated semiconductor, the photon can transfer its energy to an electron in the VB, excites it into the CB and an electron-hole pair is formed. In the case of silicon, the bandgap energy at room temperature is about 1.12 eV [Mei+07], which corresponds to a wavelength of about 1110 nm. According to Planck's equation (cf. Eq. (1)), wavelength and energy are inverse proportional and therefore the process of SPA is forbidden for wavelengths above 1110 nm (cf. Fig. 1a). In detail, crystalline silicon has an indirect bandgap, i.e. if the gap between the valence and conduction band is regarded in the momentum space, the local maximum and minimum of both (and hence the transition with the least energy required) have a different momentum. Hence excitation of an electron with minimal energy additionally requires always the involvement of a *phonon* to transfer this momentum to the crystalline lattice and thus satisfy the conversation of momentum. A phonon is a *quasiparticle* representing a quantum mechanical quantization of a mode of vibration in the lattice. However, this aspect can be neglected in this context, since at room temperature there is a sufficient amount of phonons for the inner photoelectric effect to occur, though it is less likely compared to direct bandgap semiconductors.

If the sum over the photon's energies surpasses the bandgap, there is a possibility of the simultaneous absorption of two photons. In this case, the electron will be elevated from the valence band to a virtual intermediate state within the bandgap by the first photon and after the absorption of a second photon the electron will be further elevated into the conduction band to its final energy level [She00]. The existence of such virtual intermediate states between stationary ones was postulated by Heisenberg's energy-time uncertainty principle, which claims the lifetime of the virtual intermediate state is equal to

$$\Delta t \geq \frac{h}{4\pi\Delta E}, \tag{2}$$

where ΔE is the energy difference between the virtual and the nearest stationary state. In the case of silicon, the maximum virtual state lifetime lies around the order of femtoseconds

[Bel+00]. During this lifetime, the bandgap bears the possibility to simultaneously absorb a second photon with half the bandgap energy as well. With the combined energy of both photons it is possible for the electron to overcome the bandgap and an electron-hole pair is generated. This mechanism is called TPA and is schematically depicted in Fig. 1b. The very low probability for TPA to happen compared to SPA can be increased by using higher peak laser intensities and therefore increasing the amount of photons available for the process in a nonlinear way (cf. Section 2.3) [Göp31; She00].

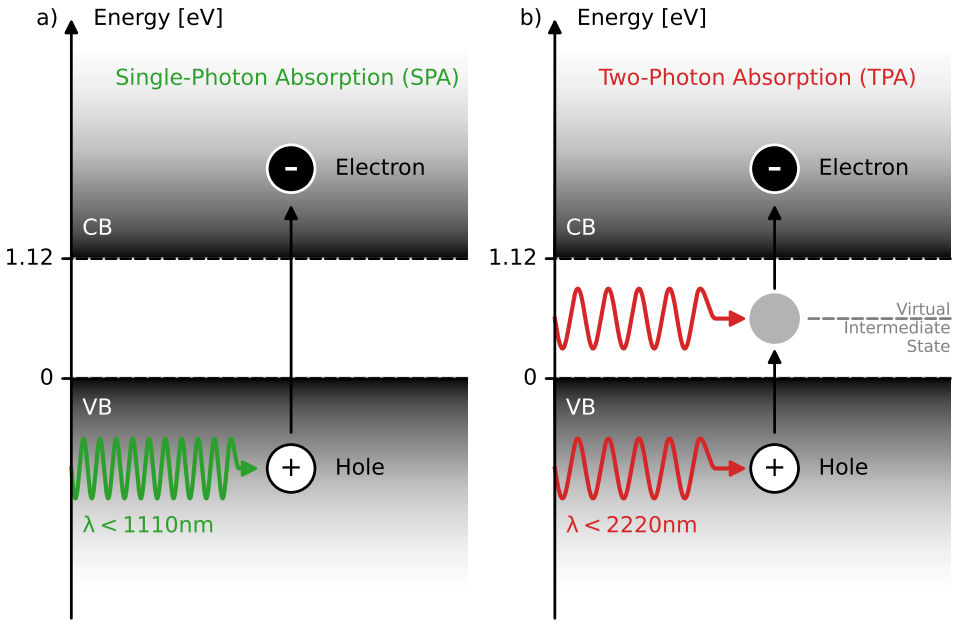


Figure 1: Bandgap diagram of silicon: a) Single-photon absorption with wavelengths shorter than 1110 nm creates a hole in the VB and directly excites an electron into the CB. b) Two-photon absorption with wavelengths containing half the energy of the bandgap. Excitation of the electron into an virtual intermediate state within the bandgap before the electron is elevated into the CB by a second photon.

2.2 Single-Photon Absorption (SPA)

The possibility for common electron-hole pair generation via SPA is primarily governed by Beer's law described with an exponential decay of the laser intensity with penetration depth into the material [Kai+10]. Using laser pulse intensities below $1 \times 10^6\,\mathrm{W\,cm^{-2}}$, nonlinear effects can be neglected and the path-dependent intensity is described by

$$\frac{dI(z)}{dz} = -\alpha_\lambda I(z) \tag{3}$$

respectively

$$I(z) = I_0 e^{-\alpha_\lambda z}. \tag{4}$$

$I(z)$ denotes the laser intensity as a function of penetration depth z, I_0 is the laser intensity at the materials surface and α_λ the material dependant linear absorption coefficient. Eq. (3) shows that the attenuation rate is linearly proportional to α_λ, which is also strongly

dependent on the laser's wavelength (cf. Fig. 3) [McM+02; NS04]. Eq. (4) describes the wavelength dependent exponential decay of intensity during the propagation of the laser light trough the material. This behavior will be discussed later in terms of a simulation of the generated charge carrier density N in Section 2.3 in detail.

Because of the behavior of the wavelength-dependent absorption in silicon, a trade-off between charge carrier generation (absorption) and penetration depth has to be made as can be seen in Fig. 3.

2.3 Two-Photon Absorption

Theoretical background. As it comes to high peak intensities above $1 \times 10^6\,\mathrm{W\,cm^{-2}}$, generated by e.g. femtosecond laser pulses at sub-bandgap optical wavelengths, this simple linear relation between absorption rate and laser intensity does not hold any longer. As a result, the materials response is not linear but can rather be estimated by higher-order terms [NS06]. The important effect in this context is two-photon absorption (TPA) and can be described as follows:

$$\frac{dI(z)}{dz} = -\beta I(z)^2 \tag{5}$$

respectively

$$I(z) = \frac{I_0}{1 + I_0 \beta z}, \tag{6}$$

where β is the two-photon absorption coefficient that characterizes the non-linear response of the system due to third-order susceptibility, a fundamental property of nonlinear optics [Hor86]. The absorption rate is proportional to the square of the laser intensity (cf. Eq. (5)) unlike the linear dependency in single-photon absorption and its solution expresses the intensity dependence of the position z inside the material (cf. Eq. (6)).
The combination of Eq. (3) for SPA and Eq. (5) for TPA results in the expression for the total absorption in the material [McM+02]

$$\frac{dI(z)}{dz} = \underbrace{-\alpha I(z)}_{\text{SPA}} \underbrace{-\beta I(z)^2}_{\text{TPA}}. \tag{7}$$

Having in mind that the absorbed photon energy creates electron-hole pairs under excitation trough the inner photoelectric effect and the photon energy itself can be modelled by Planck's equation (cf. Eq. (1)) one can set an equation that represents the generation rate $G(z)$ of electron-hole pairs as a function of laser penetration depth z into the material [NS06]:

$$G(z) = \frac{dN(z)}{dt} = \underbrace{\frac{\alpha I(z)}{h\nu}}_{\text{SPA}} + \underbrace{\frac{\beta I(z)^2}{2h\nu}}_{\text{TPA}}. \tag{8}$$

The left and right terms represent SPA and TPA respectively and the factor of two in the denominator of the TPA term marks the fact that the energy of two photons is absorbed to create one electron-hole pair. By using wavelengths longer than that at the band gap ($\lambda > 1150\,\mathrm{nm}$) in silicon, the left term can be neglected due to the small value of α (cf. Fig. 3a) and an insufficient photon energy for SPA in this sub-bandgap wavelength regime. Therefore, TPA then becomes the dominant mechanism for electron-hole pair generation in silicon [McM+02]. In this case, the solution of Eq. (8) results in

$$N_{2P}(z) = \frac{\beta}{2h\nu} \int_{-\infty}^{\infty} I(z,t)^2 \, dt, \tag{9}$$

which is used in the simulation in Section 2.3 and is essentially a time integral over the square of the intensity development trough the material [McM+02].

Beam properties. The nonlinear model for absorption is only valid for high intensities, which can be achieved by using ultrashort laser pulses (i.e. $1 \times 10^{-12}\,\mathrm{s} - 1 \times 10^{-15}\,\mathrm{s}$) without exceeding the damage threshold of silicon [Cow06; Hal+14]. These pulses are described by a beam shape on the basis of a Gaussian intensity distribution I(r, z) over z and the radial axis r [Li+; Sal03]

$$I(r, z) = \frac{2P}{\pi w^2} e^{-\frac{2r^2}{w^2}}, \tag{10}$$

where P is the laser pulse peak power [Kai+10] and w describes the beam radius as

$$w(z) = w_0 \sqrt{1 + \left(\frac{\lambda z}{\pi w_0^2 n}\right)^2}. \tag{11}$$

The longitudinal position relative to the waist with beam radius $w(z = 0) = w_0$ is denoted with z and n is the linear index of refraction. The distance between $z = \pm z_R$ is called the confocal parameter [Bro88] respectively the depth of the beam's focus, with Rayleigh length z_R, and is given by:

$$z_R = \pm \frac{\pi n {w_0}^2}{\lambda}. \tag{12}$$

At $z = \pm z_R$ the beam radius w is by a factor of $\sqrt{2}$ larger with respect to the focal plane, where $w = w_0$ and the on-axis intensity at $r = 0$ is one half of the peak intensity at $z = 0$ [F G07; McM+02].

Fig. 2 depicts the schematic representation of a Gaussian beam including the intensity profile $I(r, z)$ in red and the beam waist $w(z)$ parameters in black.

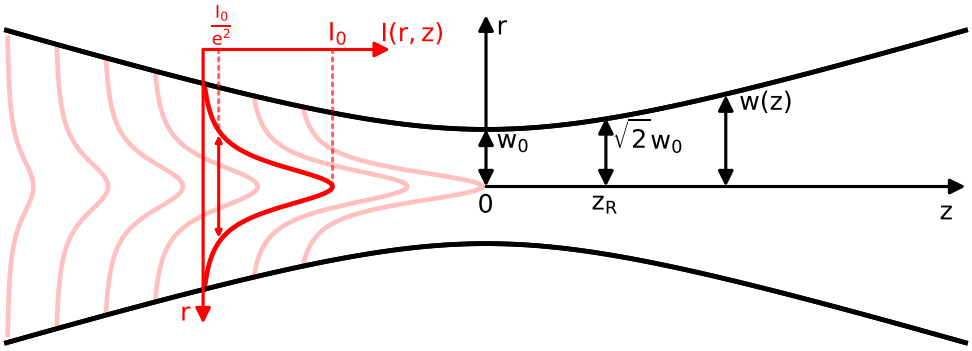


Figure 2: Schematical representation of the Gaussian beam shape. Red: Intensity profile $I(r, z)$. Black: beam radius $w(z)$, beam radius $\sqrt{2}w$ at z_R and beam radius w_0 at the waist.

Application and Advantages. The application of two-photon absorption on laser fault injection bears some great benefits compared to single-photon absorption. The resulting properties of the transparency of silicon within the wavelength region for TPA, a focal width respectively nonlinear response of the material even below the Abbe diffraction limit and a selective excitation referred to the depth of the material.

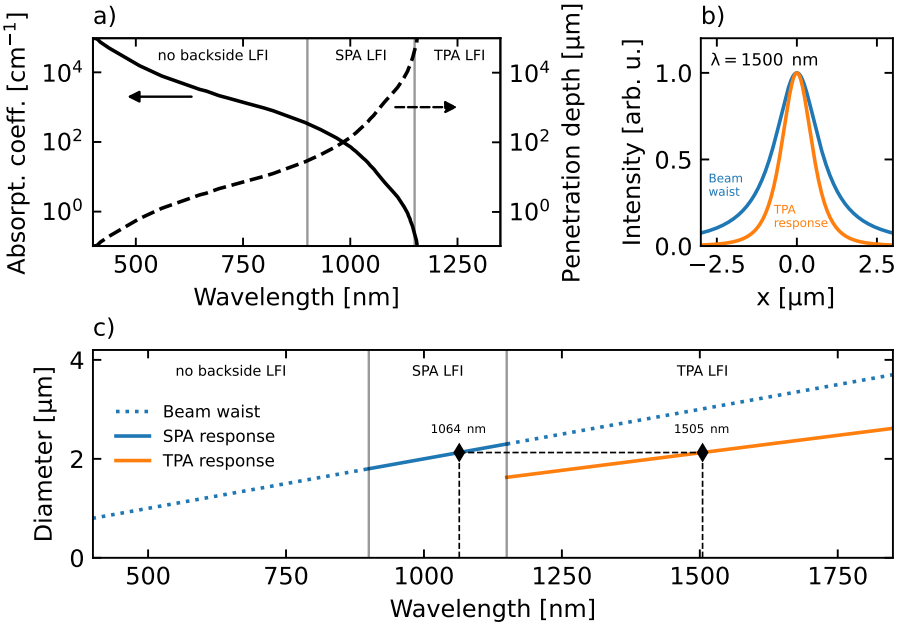


Figure 3: a) Absorption coefficient respectively penetration depth of silicon dependent on the wavelength. The three central regimes are indicated, containing Two-Photon Absorption Laser Fault Injection (TPA-LFI), Single-Photon Absorption Laser Fault Injection (SPA-LFI) and the range where no backside LFI is possible. In the case of wavelengths suitable for two-photon absorption laser fault injection the absorption coefficient is almost zero and the penetration depth is $\gg 1 \times 10^5$ µm [McM+02]. b) Comparison between the Abbe limited theoretical radial focal width (blue) for $\lambda = 1500$ nm and the theoretical two-photon absorption response (orange). c) Comparison between the Abbe limited theoretical radial focal width (blue) and the theoretical two-photon absorption response (orange) within the three wavelength ranges. Conducting TPA at wavelengths of about $\lambda \leq 1500$ nm, the nonlinear response bears the possibility of an even smaller focal width than conducting SPA-LFI using the commonly used wavelength of $\lambda = 1064$ nm.

The reason for the transparency is the low absorption coefficient of silicon in the range of the typical wavelengths for two-photon absorption (cf. Fig. 3a). The resulting penetration depth of laser light of wavelengths above $\lambda = 1150$ nm (sub-bandgap) allows a precise excitation inside the material with nearly no loss of intensity and therefore there is no need for substrate thinning on the backside of the DUT. Also the risk of loss or damage of the device caused by either laser induced thermal damage due to optical absorption or thinning can be minimized. The difference between SPA and TPA regarding optical absorption inside silicon is compared in a simulation of the generated electron-hole density N for three different wavelengths (cf. Fig. 4). Most clearly the difference becomes evident by comparing SPA using $\lambda = 800$ nm (cf. Fig. 4b) and TPA at $\lambda = 2000$ nm (cf. Fig. 4c). The focal plane is set inside the material at a depth of $z = 70$ µm for all cases and also the focal parameters for SPA and TPA are chosen equally for the charge carrier density simulation. The result for TPA shows a perfectly located spot and therefore a maximum electron-hole density centred around the aimed depth inside silicon. For SPA this depth is not even reached by the laser light due to the high absorption coefficient at $\lambda = 800$ nm. Therefore, almost all laser intensity is lost near the air-silicon interface.

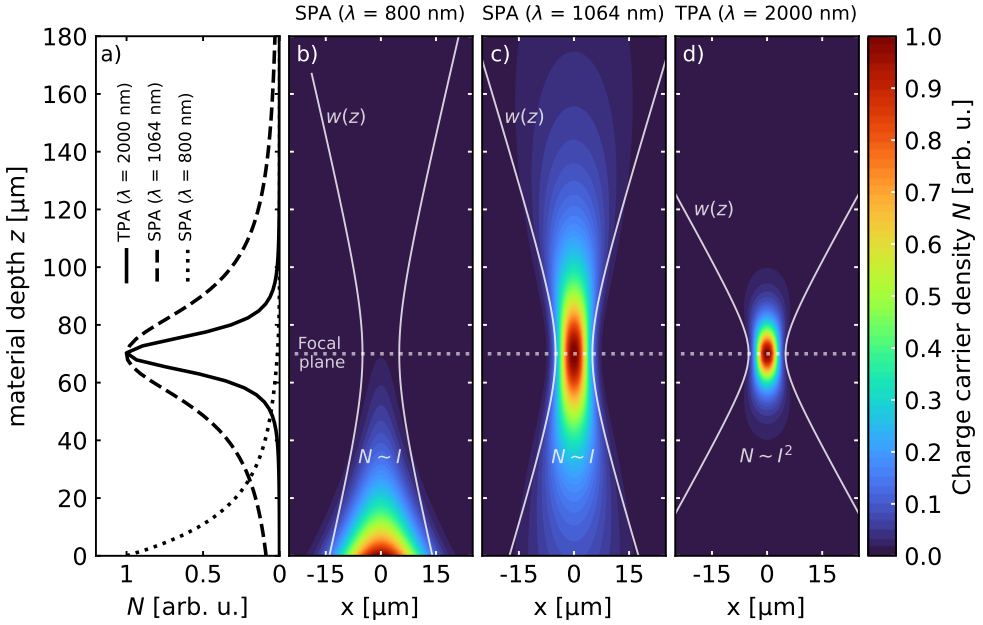


Figure 4: a) Generated charge carrier density as a function of the material depth z for SPA and TPA at $x = 0$. Charge carrier density N simulation for 800 nm (b) and 1064 nm (c) single-photon absorption (SPA) and 2000 nm (d) two-photon absorption (TPA). For comparability N is normalized to one. Compared to the TPA case, the generated electron-hole density is a factor ~ 6 (1064 nm) respectively ~ 2.3 (800 nm) higher.

Beside the advantage of the transparency of silicon a precise and sharp excitation in z and x direction is possible. On the basis of the geometrical focus conditions for TPA, reliable fault injection only in the focal spot of the laser is possible. This becomes evident by comparing the generated electron-hole density for $\lambda = 1064$ nm nm SPA and $\lambda = 2000$ nm TPA (cf. Fig. 4c-d). Assuming same laser power for both SPA and TPA, the overall generated N in silicon with SPA is a factor of ~ 6 higher than for TPA, leading to negative effects like latch-up or other unwanted electronic damage and misbehavior inside the DUT. Fig. 3 compares the wavelength dependant focal beam waist in the theoretical Abbe limit with the nonlinear response of the material, in principle the focus size for SPA and TPA. Fig. 3b shows the direct comparison for $\lambda = 1500$ nm between the Abbe limited theoretical radial focal width (blue) and the theoretical two-photon absorption response (orange) and therefore a focal spot size under the theoretical resolution limit for TPA. Fig. 3c depicts the focal spot size difference within the three wavelength ranges for TPA-LFI, SPA-LFI and where no backside illumination is possible. Conducting TPA using wavelengths of about $\lambda = 1500$ nm and below, the nonlinear response bears the possibility of an even smaller focal width than conducting SPA-LFI using the standard wavelength of $\lambda = 1064$ nm.

As a further advantage of TPA, we point out the selective excitation referred to the depth of the material. Fig. 4a shows the charge carrier density distribution as a function of the material depth. The direct comparison between 1064 nm SPA and 2000 nm TPA makes the huge difference evident. In the case of TPA there is an evenly gaussian distribution in front of and behind the focal plane with a FWHM of about 15 µm for the sharp region of where charge carrier excitation is possible. For SPA the result is a by far

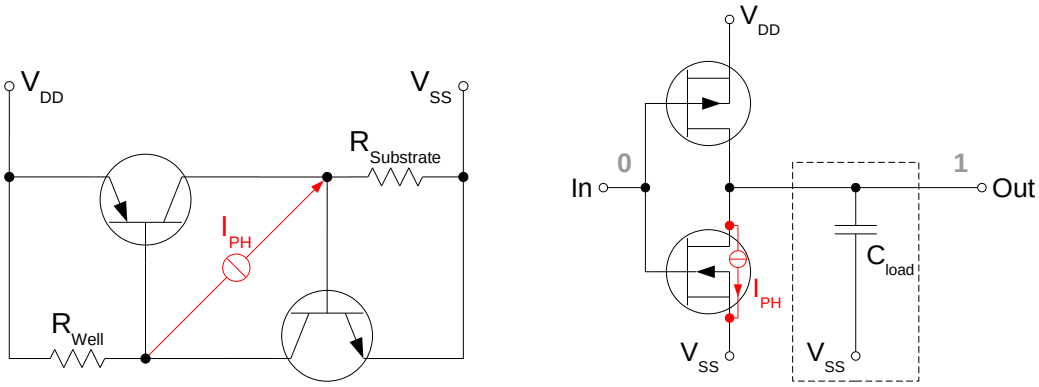
more broadened and uneven gaussian distribution with a FWHM of about 40 µm. This behavior is also visible in Fig. 4c as the contour lines of the plot are compressed in front of, and stretched behind the focal plane. The reason therefore is again on the one hand the greater transparency of silicon at $\lambda = 2000\,\text{nm}$ compared to $\lambda = 1064\,\text{nm}$ and on the other hand the I^2 dependency of TPA and therefore a smaller region in z-direction, where the intensity requirement for this nonlinear process is fulfilled.

Executing the simulation shown in Fig. 4 assuming Abbe limited conditions and using a solid immersion lens for optimized focussing, shows that the generated charge carrier density can be further reduced and therefore greater fault precision could theoretically be achieved. $\text{N}(\lambda = 2000\,\text{nm})$ turns out to be a factor of 24 lower compared to the initial simulation parameters, $\text{N}(\lambda = 1064\,\text{nm})$ could be even reduced by a factor of about 70. However, the practicability using an immersion lens for ultra-short laser pulses in the region of sub-10 fs seems critical because of the need for temporal and spacial dispersion compensation.

2.4 Single Event Effects induced by LFI

On a circuit level, the photoelectric effect induced by a laser can trigger various effects. Commonly these effects in semiconductors are referred to as *Single Event Effects (SEE)*, since they result from a single environmental cause, typically high-energetic cosmic particles. These generic term can be further subdivided, for LFI relevant are following effects:

Single Event Upset. The charge carries generated by the photoelectric effect recombine without any effect in the bulk silicon. In the vicinity of an reverse-biased pn-junction however, charges are separated by the electrical field before recombination. This leads to an electrical current which may affect the circuitry in forcing faulty logic levels at the output of gates, which will result in a fault if this value is sampled or latched. This effect is referred to as an Single Event Upset (SEU). Figure 5b shows the basic SEU effect in a CMOS inverter. With a logic 0 level at the input, the reverse-biased pn-junction at the drain of the n-channel MOSFET is sensitive for SEU by laser irradiation. The induced current I_{PH} may unload the capacitance of the output network and hence induce a soft error. With an logic 1 at the input, the corresponding SEU effect would be triggered at the drain of the p-channel MOSFET.



(a) Equivalent circuit formed by the parasitic transistors responsible for SEL effect

(b) SEU mechanism in a CMOS inverter

Figure 5: SEE effects in a basic CMOS inverter

Single Event Latch-Up. Besides the SEU effect, lasers can also trigger a Single Event Latch-Up (SEL) effect. This effect originates from parasitic structures in the semiconductor. Figure 6 shows exemplary how parasitic bipolar transistors are formed in the proximity of the NMOS and PMOS transistor of an CMOS inverter. If the laser induces a photo current I_{PH} (cf. Fig. 5a) in the substrate, this circuit creates a short between V_{DD} and V_{SS} with an positive feedback loop once it was triggered. I.e. this circuit behaves like an thyristor and will stay activated after laser irradiation, hence requiring a full power cycle of the device for recovery. Basically ICs are usually designed in a way to be as robust as possible against these effects. E.g. technologies like Silicon on isolator (SOI) are inherently resistant against latch-up effects, due to the full isolation of the well structures. However, SOI is significantly more expensive and therefore mostly used for large high-performance ICs.

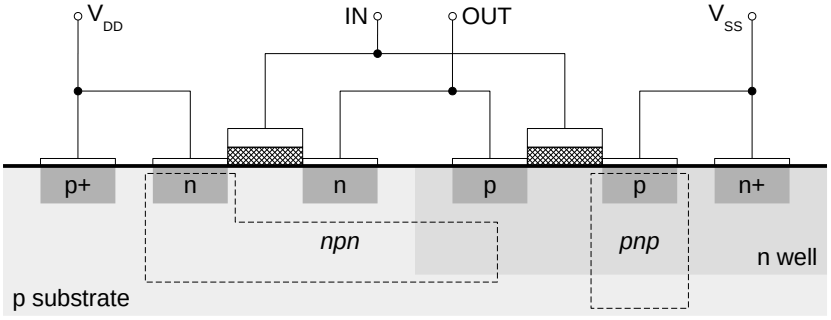


Figure 6: Cross section of an inverter with parasitic bipolar transistors

3 Experimental Setup

We used two different laser setups for our experiments, Table 1 gives a brief overview over the key features of both setups and the used energy levels. In the following we describe both setups in detail.

3.1 Single-Photon Absorption

The SPA setup contains a diode-pumped neodymium-doped yttrium aluminum garnet (Nd:YAG) solid state laser. The laser source can be configured to emit light at either 532 nm or 1064 nm. For our experiments we only used the latter. The source has a fix pulse length of 800 ps and is able to emit pulses at maximum repetition rate of 1 kHz. The beam is focused by a refractive objective lens with 20× magnification and a numerical aperture of 0.4.

3.2 Two-Photon Absorption

For the TPA effect, the setup was built by using a high power laser source and converting the wavelength to the infrared range. This optical system is generally capable of triggering the TPA effect, but not yet optimized, as we discussed in Section 2: An ideal setup would use a center wavelength of around 1300 nm. Maximum precision does also require a fine control over the energy output, in order to reduce the used laser energy to the required minimum, which in the laboratory setup is only adjustable by a manual iris. Moreover, the positioning capabilities of the system are very limited. To not further complicate the beam bath, the setup does not include a camera, which otherwise would have required an additional beam splitter introducing further dispersion. Moreover, the used xyz-table

has a resolution of approx. 1 µm with limited repeat accuracy and lack of a tilt correction, impeding very precise scans.

Front-end laser system. The commercial front-end of the used laser system is a master oscillator power amplifier (MOPA) system manufactured by the former Austrian Femtolaser Produktions GmbH. The specifications of the entire laser system are an output power of $P_0 < 12\,\mathrm{W}$, pulse energies E_{pulse} up to 3 mJ and pulse durations of $\tau_0 = 23\,\mathrm{fs}$ at a repetition rate of $f_{rep} = 4\,\mathrm{kHz}$. Subsequently to the commercial part, an tailored hollow-core fiber compressor setup, containing a 3 m noble gas filled glass capillary and two pairs of custom designed chirped mirrors to compress the laser pulses down to $\lambda < 5\,\mathrm{fs}$ with a spectral range of over an octave centred around 690 nm.

These laser pulses are now predestinated for the usual generation of high harmonics, but the laser parameters at this point are also ideal to perform nonlinear laser fault injection. Therefore, an attenuated fraction of the laser beam $\sim 50\,\mu\mathrm{J}$ is guided outside the regular experimental setup respectively laser beam path towards the LFI setup.

Nonlinear laser fault injection setup. Figure 8 shows a schematic depiction of the apparatus and associated optical components built up for two-photon laser fault injection. The first optical component of the nonlinear LFI setup is a pair of fused silica wedges (FS) for fine dispersion adjustment to keep the pulse length as short as possible and to be able to optimize the later generated IR spectrum. The following aperture (A) narrows the beam diameter and therefore allows for tuning the laser power from 0 to 200 mW, limited by the damage threshold of the device, and helps finding the power sweet spot for fault injection. The folding mirror (M) directs the beam onto a concave mirror (CM) that focuses the laser beam under a small angle into the nonlinear crystal (BBO). With the aim to conduct single-shot fault injection, a combination of a chopper wheel (CW) and a shutter (S) is used to reduce the initial repetition rate of 4 kHz to 100 Hz after the copper and subsequently being able to pick single pulses with the synchronized mechanical shutter. For the TPA experiment infrared light is generated via difference frequency generation (DFG) [Fat+13] by a nonlinear crystal (BBO: Beta-Barium Borate), which shifts the central wavelength to approx. $\lambda_c = 2000\,\mathrm{nm}$ (cf. Fig. 7) The residual visible light in the spectrum ($\lambda < 1100\,\mathrm{nm}$) is then blocked by a Germanium (Ge) filter, to avoid a superposition of both the SPA and the TPA effect. Hence all observed effects can directly be ascribed to TPA.

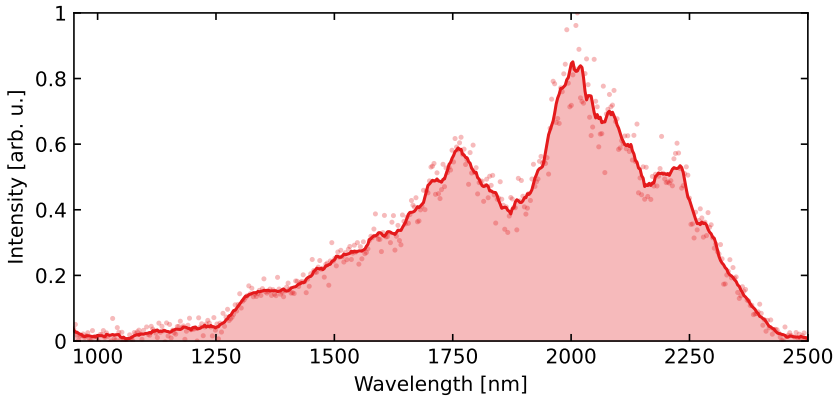


Figure 7: IR spectrum generated via difference frequency generation (DFG), solid line: smoothed spectrum, shaded: original recorded spectrum.

As Ge induces a negative dispersion to the laser pulses, a fused silica plate (FS) is used for compensation by inducing a proper amount of positive dispersion. The thickness

of the fused silica plate is chosen to even taking into account the induced dispersion of the silicon protective layer on the DUT. By considering this physical effect and with the additional used pair of fused silica wedges, nearly theoretically Fourier-limited pulses can be provided inside the DUT. For optimal focusing conditions, a Schwarzschild objective (RO: reflective objective, Newport^{TM} Microscope Objective Lens Model: 50105-02) is used to ensure tight focusing with a short focal length and without inducing further dispersion. The respective DUT is mounted on a combination of a z-translation stage together with piezo actuators for high resolution x-y-scans. Therewith, flexible alignment is guaranteed as well as optimal focusing conditions.

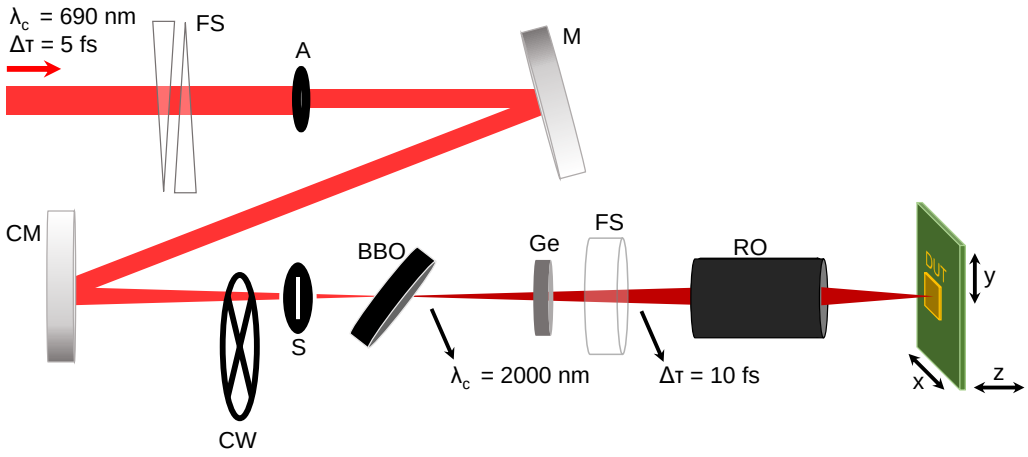


Figure 8: Schematic experimental setup for two-photon absorption laser fault injection measurements. FS: fused silica wedges, A: aperture, M: folding mirror, CM: focusing mirror, CW: chopper wheel, S: shutter, BBO: Beta-Barium Borate crystal, Ge: Germanium filter, FS: fused silica plate, RO: reflective focusing objective, DUT: device under test.

The resulting laser parameters on the DUT can be assumed as follows:

Table 1: Laser parameters on the DUT conducting LFI

Parameter	TPA Setup	SPA Setup
Center wavelength	2000 nm	1064 nm
Average Power	30 µW	1 µW
Single pulse energy	7.5 nJ	≈ 1 nJ
Focal width	10 µm	4 µm
Pulse duration	10 fs	800 ps

3.3 Comparison of the system parameters

Comparing the chosen laser parameters both for SPA and TPA, there is a quite large difference in the pulse duration. The SPA setup was specifically designed for LFI attacks and uses a 800 ps pulse duration since this always enables to limit the fault effect to a single clock cycle. The reason for the use of approx. 10 fs pulses for the TPA experiments is to achieve the necessary high pulse intensities of above $1 \times 10^6\,\mathrm{W\,cm^{-2}}$ for two-photon absorption inside the DUT. This is technically realizable only by using ultra-short pulses in the fs-range. In addition, the pulses in the femtosecond range enable to use difference frequency generation (DFG) in a nonlinear crystal, allowing to shift the wavelength into the NIR range. Therefore we combine the wavelengths on the left (around 400 nm) and

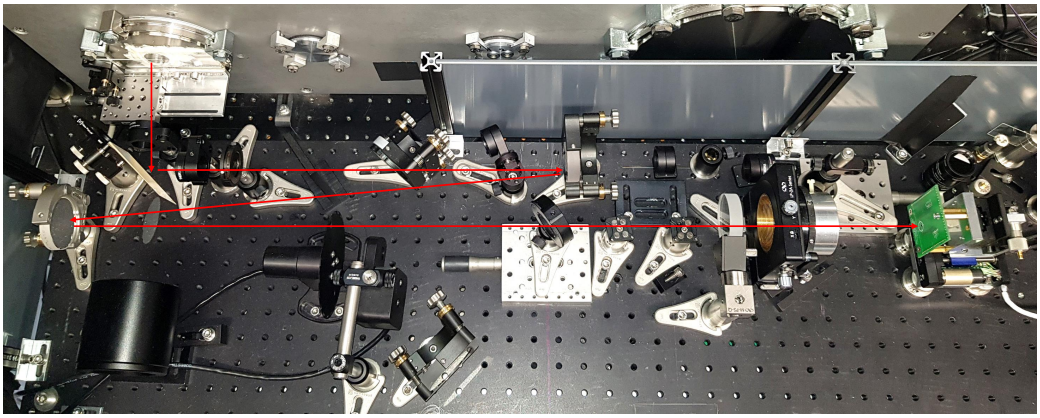


Figure 9: Picture of the two-photon laser fault injection setup in the laboratory with indicated beam path in red.

the right (around 1100 nm) side of the ultra-broad spectrum in a nonlinear crystal to generate the intended difference frequency of 2000 nm. Hence the exact parameters of the experiment originate to a certain degree from the specifications of the available laser system. Originally, the utilized laser setup is intended for performing high harmonic generation and attosecond streaking experiments where ultra-short few-cycle fs-pulses are required. Considering the time-bandwidth product, the broader the spectrum of the laser pulse is, the shorter it can be compressed in the time-domain. At the input to the TPA-LFI setup, the laser pulses have an estimated pulse duration of < 5 fs, which is well in the applicable range for the TPA-effect.

3.4 Target Devices

Table 2 lists the devices used for the LFIs experiments and details some of their physical properties.

Table 2: List of target devices used in LFI experiments

	NXP LPC11E14	**Infineon XMC1401**
Device identifier	`LPC11E14FBD64`	`XMC1401-F064F0128`
Process size	140 nm	65 nm
Memory size	8 kB + 2 kB	16 kB
Latch-up prone	Yes	No
Thinned/Unthinned	Unthinned	Both

NXP LPC11E14. The NXP LPC11E14 was used by Selmke et al. [Sel+18] during a LFI evaluation. It is fabricated using a 140 nm process size and was found to be prone to SEL hindering the injection of reliable and frequent faults. Selmke et al. have shown that when SPA was performed on the SRAM, the chip would enter a latch-up state and become unresponsive until a full power cycle was administered. We used this chip to investigate

whether TPA could produce faults in devices where the state-of-the-art method would usually trigger a latch-up.

Infineon XMC1401. The XMC1401 has a 65 nm transistor process size which is over two times smaller than the process size of the LPC11E14. Performing SPA on this chip highlighted the precision limitations of the state-of-the-art LFI setup, as it struggled to reliably produce single-bit faults in this device's SRAM area. We used this chip to determine whether TPA could address this precision limitation and more reliably produce single-bit faults than using SPA.

4 Experimental Results

We used the described setups (cf. Section 3) to verify the theoretically appealing properties of TPA-LFI in comparison to SPA-LFI. We investigated transparency of silicon, latch-up resistance and precision during a TPA-LFI.

4.1 Transparency

As discussed in Section 2.3, one property of TPA is transparency of silicon for the emitted wavelengths. Optical absorption is a major limitation of SPA because of exponential attenuation of the laser (cf. Eq. (4)). Depending on the thickness of the substrate of a chip, emitted light of a SPA setup may lose the necessary intensity, to create enough electron-hole pairs in the sensitive area. Firing a laser with too much intensity however, can destroy the chip. The state-of-the-art solution addressing this issue is mechanical and chemical thinning [BH22]. However, this has to be done in a precise process, can be expensive and risks damaging the chip.
Figure 10 shows results of a z-scan using the TPA-LFI setup. We measured the probability that any type of single-event effect takes place. For each z-position we repeated the injection multiple times and registered any single-event effect. The probability distribution indicates the size of the beam's active range along its axis, where the intensity is high enough to cause nonlinear effects to take place. Figure 10 shows the results of this z-scan and highlights the beam's small active range. The overall shape of the fault probability distributions

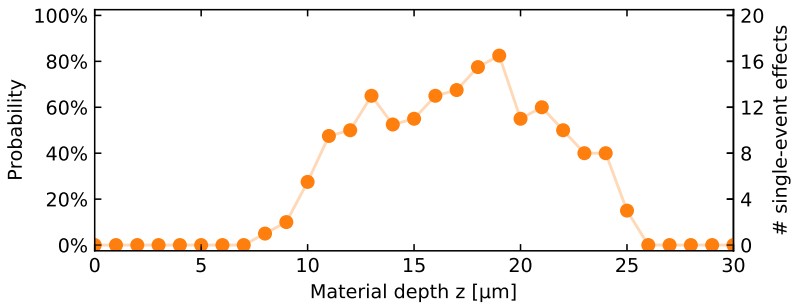


Figure 10: Probability of single-event effect from TPA-LFI at varying z-axis positions.

resembles that of a Gaussian curve and could be fitted as such. This fits the simulated results described in Fig. 4 and is indicative of the tightly focused nature of the absorption region in the TPA beam. Unlike SPA the is only located in the beam waist where the intensity is high enough for TPA to take place.

4.2 Avoidance of Latch-Up

We confirmed the results reporting the latch-up effect [Sel+18] by injecting faults using the SPA setup on the LPC11E14 target device. We performed a full x-y-scan over the chip's silicon area and determined a rough mapping of the chip's active area. Figure 11 shows the results of this scan. We could not inject a successful SRAM fault. However, we encountered multiple latch-ups indicated in green. This matches the results reported in [Sel+18] and shows that the chip is prone to latch-ups. We performed TPA-LFI on

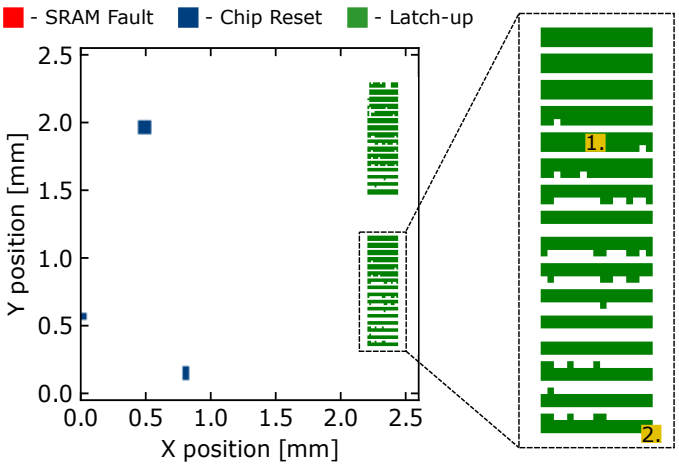


Figure 11: Full x-y-scan of NXP chip using the SPA laser system for fine scan over the SRAM area.

that same chip, however instead of scanning the full area we used the knowledge gained from the SPA-LFI experiments to direct the laser only on the latch-up prone SRAM area and performed precise x-y-scans on key areas. These areas are indicated in yellow and marked with *1.* and *2.* in Fig. 11. Fig. 12 shows the respective areas and there single-bit fault probabilities based on multiple shots using TPA-LFI. In contrast to the SPA experiments, we were successfully able to induce single-event upsets without triggering single-event latch-up. Specifically, we were able to flip individual bits in the memory at a high probability of success using TPA. Across different scan locations in the SRAM array we did not experience any latch-up at all using TPA-LFI once the correct laser settings were applied. This suggests that TPA does indeed play a significant role in reducing the likelihood of single-event latch-up in LFI and can be used to access latch-up sensitive regions of target devices.

Table 3 provides a summary of the fault performance on the areas tested during the SPA and TPA experiments. The results of the SPA experiments are denoted with L/U to indicate that they only produced latch-up. As mentioned previously, maximum precision single-bit faults were able to be induced in the SRAM of the NXP chip using TPA, however we wanted to evaluate how reliably we could induce these single-bit faults at specific addresses. As such, the metric we used to measure fault performance was given as a percentage likelihood, reflecting the probability of a single-bit flip at a given bit-address which was determined through multiple LFI repetitions at each position. We assume that this outcome is not a result of the drastically reduced pulse duration, but a better localization of the induced charge carriers due to the TPA effect. For progressively shorter pulses the circuit capacitances become dominant at which point the injected

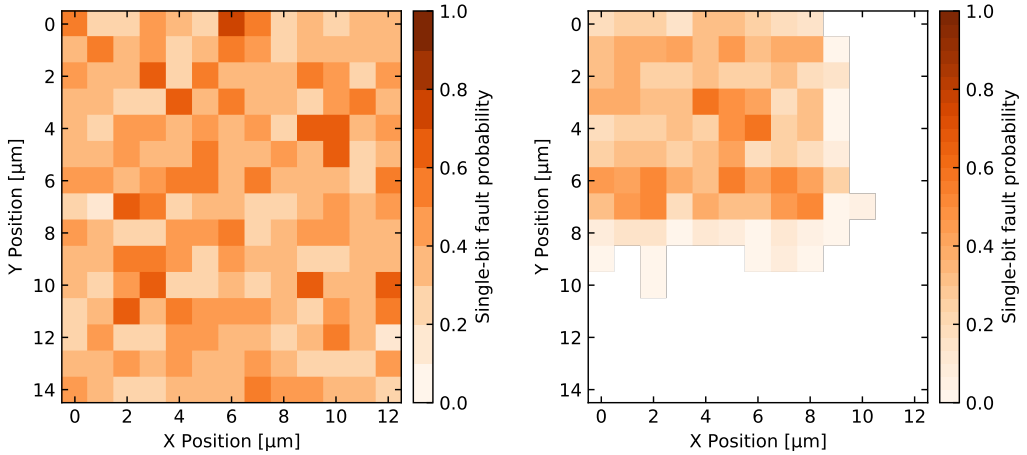


Figure 12: Precise TPA x-y-scan of middle stripe (left, cf. Fig. 11 (1.)) and corner (right, cf. Fig. 11 (2.)) of SRAM block in NXP chip.

charges become more important than the injected currents. Let us assume that the load capacitance of the gate is significantly larger than the capacitance of the parasitic thyristor that has to be charged for it to be triggered on. Then, the amount of injected charge needed to trigger the thyristor is smaller than that needed to fault the output of the gate. Hence, with short pulses of increasing energy it is likely that the thyristor is triggered before enough charge could be injected to discharge the load capacitance sufficiently to cause a fault at the output of the gate. In order to successfully inject a fault, the injected charge density has to be increased near the output MOSFET drain-bulk pn-junction and decreased near the pn-junctions associated with the parasitic thyristor, which is what the TPA setup proposed in this work was able to approach more closely than is possible with conventional SPA setups.

Table 3: Summary of single-bit fault probabilities in active area of NXP chip. L/U indicates only latch-ups.

	Corner			Middle		
	Min.	Max.	Avg.	Min.	Max.	Avg.
SPA	L/U	L/U	L/U	L/U	L/U	L/U
TPA	3.3 %	60 %	24.1 %	10 %	70 %	26.6 %

4.3 Single-bit fault precision

Table 4: Summary of overall single-bit fault probabilities XMC chip.

	Min.	Max.	Avg.
SPA	5 %	30 %	8 %
TPA	10 %	50 %	15.4 %

The following presents our findings from our experiments investigating the reliability of single-bit faults on the XMC1401 with TPA-LFI compared to SPA-LFI. Table 4 provides a comparison between the SPA and TPA results and summarizes their performances.

Once again, the same convention is used from before, where Min. represents the smallest non-zero fault probability/probability resolution, Max. represents the maximum single-bit fault probability at a single position and Avg. represents the aggregated averages of the non-zero set- and reset-fault probabilities in the scan-area. The TPA results show a significant improvement in fault performance over SPA as it yielded an average single-bit fault probability of 15.4 % compared to 8 %. The maximum (30 % vs. 50 %) as well as the minimum (5 % vs. 10 %) likelihood for a fault is better for TPA compared to SPA. This results are promising and have to be solidified by a even comparable setup where only the laser source is the separating factor. In the following we discuss the possible impact of our findings with respect to LFI countermeasures.

5 Impact on Sensor-based Countermeasures

The presented results raise the question whether state-of-the-art tamper protection mechanism could be bypassed using TPA. Countermeasures against fault injections can roughly be divided into two groups: Specialized sensors and device-level countermeasures to detect or prohibit a fault injection, and those relying on some form of redundancy in the implementation. There is a wide variety of sensor-based countermeasures described in scientific literature and patents, which usually aim at protecting against very specific attack methods. Redundancy as a countermeasure on the other hand works indifferently of the actual attack vector and relies on correcting or handling faults, so that the attacker is not able to exploit them. This can be achieved in various ways: Duplication of execution units, repetition of calculations in the time domain, or by code-based transformations. Since redundancy-based countermeasures are indifferent of the attack method, this section discusses the impact of a TPA-based LFI attack on the various sensor-based countermeasures which try to detect a fault injection process. Thereby we include concepts which are used in practice or were suggested in the scientific community.

5.1 Photodiodes / Light Detectors

Light sensors are a common countermeasure against optical attacks in state-of-the-art security IC, e.g. smartcards. These sensors are basically specially designed reverse-biased diodes placed at critical positions on the die. The diodes are designed to be very sensitive and raise a security interrupt if a certain current threshold is succeeded. Although these sensors are widely used, very little about their exact design is publicly known.

However, these sensors have certain limitations: First, an alarm can only be triggered if the sensor is directly illuminated. Since these sensors can only be placed in the vicinity of critical locations, these sensors can be actively avoided, if the attacker is able to identify them. Because of the high lateral precision this is especially true for a TPA-based fault injection. Hence, light sensors work well in cases, where the attacker uses imprecise tools like e.g. flash-lamps for fault injection, or performs large laser scans on the device, but they cannot guarantee that a fault injection is infeasible without triggering them.

5.2 Latch-Up Sensitive Design

Besides the intended fault injection, LFI is also capable of triggering short circuits by *Latch-Up effects* in an IC. In principle, these originate from thyristor-like structures which are implicitly formed by the placement of regular transistor-structures in the silicon.[Sel+18] Normally a design goal is to minimize the likelihood of this effect, however it has also been suggested as a countermeasure against LFI attacks.[Jai+21] The key idea is, to specifically design crucial parts to be sensitive for this effect, and then detect the short-circuit caused by an LFI attack.

However, the Latch-up can effectively be avoided by the use of TPA. The generation of Latch-ups rises from the deeper injection of charge carriers in the silicon. Since the vertical space in which charge carriers are generated is very limited, this drastically reduces the chances to trigger this effect compared to regular LFI. In 4 we demonstrate this for a microcontroller, whose SRAM is susceptible to Latch-up and therefore cannot be faulted with a standard LFI setup.

5.3 Bulk-builtin Current Sensors

For LFI electron-hole pairs have to be generated in the pn-junction of a reverse-biased transistor. Considering an inverter, the most basic CMOS element, depending on the state of the gate, the fault sensitive area is either the pn-junction at the drain of the NMOS or PMOS transistor. In the case of a logic high on the output, the drain of the reverse-biased NMOS transistor is sensitive for fault injection. Induced charge carriers at this location will then lead to a bulk current unloading the effective capacitance against ground behind the inverter output. In regular operation these bulk currents are minimal, but laser (or particle) induced currents lead to comparatively much higher currents [Net+06]. The concept of Bulk-builtin Current Sensors (BBCS) is to directly measure these irregular bulk currents. Generally, this requires taps to V_{DD} (p-well) or Gnd (n-well) connecting to the measuring circuit of the BBCS. For a complete picture of BBCS refer to [Mat+18; Mat+19; NMM21]. BBCS sensors are able to trigger at induced photocurrents lower than the level required to inject a fault [Net+06]. However, very few BBCS concepts have been actually tested. Champeix et al. [Cha+15] reported test results of a BBCS protected test chip manufactured in a 90 nm process, where only half of the well taps were BBCS protected. Though the countermeasure was generally working in the vicinity of the BBCS protected gates, their test showed a reduced sensitivity for shorter laser pulse lengths. Also the sensitivity dropped, with increased distance to the protected well taps. Unlike conventional LFI or a particle strike, TPA will not generate free charge carriers along the beam path. Since BBCSs are directly measuring the induced photocurrent, it is questionable if TPA is able to bypass this sensor-based countermeasure.

5.4 Ring Oscillator (RO) based countermeasures

Detectors which detect voltage glitches are common countermeasure. Usually, aside security concerns, there is a Brown-Out detection which is responsible for monitoring the input voltage to be in the specified range. If the input voltage drops below the specified threshold, the device will perform a hard reset. The idea behind this technique is to rather cope with a reset event, than having faulty behavior of the device. Hence, this method is directly applicable against voltage glitching attacks, with the restriction that the detector has to be fast enough to detect any form of glitch an attacker might try to induce. LFI also induces a voltage drop, even without triggering a latch-up effect (cf. Section 5.2). However, this voltage drop is smaller and localized and therefore harder to detect. With regard to modern technology nodes below 90 nm a laser spot always illuminates multiple cells and can not be limited to a single transistor anymore. Therefore, there are besides the current in the reverse-biased pn-junction responsible for the fault injection, other induced currents. Charge carriers injected in the pn boundary of the n-well to the p-substrate, lead to bulk currents resulting in a voltage drop (cf. Viera et al. [Vie+17; Vie+19]). Hence, a countermeasure can be constructed, by detecting these voltage drops.

Recently various countermeasures have been proposed, which exploit this effect by using on-chip Ring Oscillators (ROs) as an fault injection detector. This concept was first evaluated as a countermeasure against EMFI attacks [Miu+16], but has been demonstrated to be effective against LFI attaks [He+16; HBB16; He+17; Yao+21] as well. A RO consists of an odd number of inverter stages aligned in a ring, which will oscillate with a specific

frequency. The exact oscillation frequency largely depends on local manufacturing variations (e.g. doping levels) of the IC. This behavior is an often studied and used property in the context of Physical Unclonable Functions (PUFs). However, not only the manufacturing variations have influence on the frequency, but also external disturbances like temperature or a fault injection. In general, this problem of environmental parameters is known in the context of PUFs and countered by error correction. Yet, it can also be utilized as a sensor to detect LFI attacks. When designing a security IC, the natural influences have to be taken into account when integrating such a countermeasure. A certain level of tolerance has to be defined, to avoid false alarms. Since the total number of generated charge carriers is significantly less for TPA, it can be assumed that the disturbance measured by this countermeasure is drastically reduced and might be low enough to be undetectable.

5.5 Backside preparation countermeasures

Besides sensors that detect a fault injection attempt, there are various concepts to counter the required device preparation for most backside attacks. One common countermeasure against invasive attacks is shielding the die. Typically these shields protect against frontside attacks by using the top metal layer of the IC to cover the areas to be protected with signal lines, which can be tested for continuity. Since LFI is usually conducted from the backside to avoid reflection at the metal layers, frontside metal shields are not an effective countermeasure. Therefore Miki et al. [Mik+19] recently demonstrated a concept for backside shielding. Their concept is based on a copper wire in a meander shape, which covers the backside of the chip, but is connected by through-silicon vias to the chip. Compared to frontside shields, this method requires additional manufacturing steps (etching, copper filling) and hence would increase the production costs. Moreover, if the effort for an LFI attack is taken into consideration, bypassing metal shields which test for signal continuity should be principally feasible: The stated wire width is 15 µm, which can be contacted by microprobing needles or bridged by a bonding wire.

Another approach is to prevent or detect a thinning of the silicon substrate. Depending on the substrate thickness and the doping level, thinning of the silicon substrate can be required for regular LFI attacks to work. Borel et al. [Bor+18] suggested a countermeasure based on holes and vias in the silicon substrate, which shall break the silicon into pieces if the substrate is thinned. Manich et al. [Man+15] proposed a detector for the reduction of the substrate thickness based on measuring capacities between Through Silicon Via (TSV). Since LFI based on TPA works independently from the substrate thickness, countermeasures against die thinning are not applicable.

Another concept which aims at denying access to the IC backside based on optical coating was proposed by Amini et al. [Ami+17; Ami+18b; Ami+18a; Ami+20]. The latest iteration of their concept suggests coating the silicon backside with thin layers of titanium dioxide (TiO_2) and titanium (Ti). The principle of this countermeasure is to implement light emitters and sensors distributed over the die, to measure the reflection from the backside coating through the silicon substrate. At the same time this coating shall be opaque to light coming from the outside of the chip. The reflectivity of the coating is angular dependent, hence this concept should not on only detect a manipulation of the coating, but also a possible reapplication after substrate thinning. With regard to TPA the effectiveness of this countermeasures is based on the opacity of the coating. This mainly relies on the titanium layer, however this thin layer would not block the light completely but around 10 % of the energy should pass the coating. Hence, with sufficient initial energy, LFI might be feasible. Amini also tested a combination with an indium tin oxide (ITO) and silver (Ag) based coating, with the silver layer being significantly more opaque. However, we found no data for the reflectivity of silver coatings beyond 1500 nm, but we assume that high opacity continues for this spectral range.

6 Discussion and limitations of proposed LFI setup

As discussed in Section 5 and Section 2, TPA has advantages over conventional LFI in several cases. However, the usage of TPA also comes with technical disadvantages. First, the cost of a femtosecond laser source is significantly higher, over 50,000 $ only for the laser source. These laser sources are also not directly applicable for LFI since they do not come with a triggering mechanism which allows to emit a single precisely timed pulse, but constantly emit laser pulses pulses at a given rate. Hence, to receive single pulses at specific points in time, as required for LFI attacks, an additional pulse picking module must be used after the laser source, e.g. an *acousto optical modulator*, with an additional cost of approx. 25,000 $. Also these laser sources typically oscillate with an internal frequency of approx. 80 MHz. Since it is only possible to select the next available pulse to be emitted, this means that there is a variable timing delay between 0 ns to 12.5 ns. This is slightly worse, compared to the conventional 1064 nm laser system we used in our experiment, which has a triggering jitter of below 1 ns.

Moreover, retro-fitting a TPA capable laser source to an existing setup can be challenging. Since the effective pulse-length in the DUT is crucial, this means that a dispersion correction is mandatory. Every refractive optical element in the laser setup will temporally broaden the laser pulse. In our experimental setup, we therefore used a reflective objective, which is not typical for regular LFI setups, but in most cases can be installed. However, the beam path of a laser microscope system consists of several more optical elements, which usually cannot be easily modified. Hence, the pulse dispersion has to be appropriately over-compensated at the input of the system.

With regard to laser scans of larger areas, the TPA setup requires a better aligned DUT. Since charges are only generated in the focal point, this means that a small tilt of the DUT will result ineffective fault injections attempts, when the focal point is to far off. This affects the regular LFI much less, since charges are created in a larger area and the charge density drops only linearly.

7 Conclusion

In this work, we demonstrated the applicability of the TPA effect for LFI attacks. This variant of the photoelectric effect generally requires the usage of a longer laser wavelength of around 2000 nm and very short pulses in the femtosecond range. Due to the nonlinear absorption process, the TPA can be tuned to only reach the required critical intensity in the near vicinity of the focal spot of the Laser. In comparison to the regular linear inner photoelectric effect, this enables to not only restrict the generated charges by the laser beam in diameter size, but also their vertical extent. Since the energy of laser light beyond 1200 nm is not sufficient to excite electrons in the silicon, this means that the thickness of the chip substrate is almost irrelevant for the TPA process.

The overall decreased area of effect of this method should allow to inject faults with very high precision. At the same time TPA allows to circumvent undesired side-effects of the conventional single photon absorption: We were able to demonstrate, that a TPA setup was able to inject faults into an device, which otherwise shows a very high probability to generate Latch-up effects, rendering fault injections impossible. However, as we discussed in this paper, this reduced area of effect, should be able to circumvent several possible hardware countermeasures, which aim at detecting the fault injection directly. This is an important realization, as it should directly affect the security measures of modern high-security devices. As a result, manufactures of security ICs should not solely rely on such countermeasures, but also implement some level of redundancy in their circuit design, to cope with this kind of optical fault attacks.

References

[Ami+17] Elham Amini et al. "Backside protection structure for security sensitive ics". In: *Proceedings from the 43rd international symposium for testing and failure analysis*. 2017, pp. 279–284.

[Ami+18a] Elham Amini et al. "Assessment of a chip backside protection". In: *Journal of Hardware and Systems Security* 2.4 (2018), pp. 345–352.

[Ami+18b] Elham Amini et al. "IC security and quality improvement by protection of chip backside against hardware attacks". In: *Microelectronics Reliability* 88 (2018), pp. 22–25.

[Ami+20] Elham Amini et al. "Second generation of optical IC-backside protection structure". In: *2020 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. IEEE. 2020, pp. 1–5.

[BDL97] Dan Boneh, Richard A DeMillo, and Richard J Lipton. "On the importance of checking cryptographic protocols for faults". In: *International conference on the theory and applications of cryptographic techniques*. Springer. 1997, pp. 37–51.

[Bel+00] Kevin D. Belfield et al. "Multiphoton-absorbing organic materials for microfabrication, emerging optical applications and non-destructive three-dimensional imaging". In: *Journal of Physical Organic Chemistry* 13.12 (2000), pp. 837–849. ISSN: 0894-3230. DOI: 10.1002/1099-1395(200012)13:12{\textless}837::AID-POC315{\textgreater}3.0.CO;2-5.

[BH22] Jakub Breier and Xiaolu Hou. "How Practical are Fault Injection Attacks, Really?" In: *IACR Cryptol. ePrint Arch.* (2022), p. 301. URL: https://eprint.iacr.org/2022/301.

[Bor+18] Stephan Borel et al. "A novel structure for backside protection against physical attacks on secure chips or sip". In: *2018 IEEE 68th Electronic Components and Technology Conference (ECTC)*. IEEE. 2018, pp. 515–520.

[Bro88] S. D. Brorson. "What is the confocal parameter?" In: *IEEE Journal of Quantum Electronics* 24.3 (1988), pp. 512–515. ISSN: 00189197. DOI: 10.1109/3.155.

[Cha+15] Clément Champeix et al. "Experimental validation of a Bulk Built-In Current Sensor for detecting laser-induced currents". In: *2015 IEEE 21st International On-Line Testing Symposium (IOLTS)*. IEEE. 2015, pp. 150–155.

[Cow06] B. Cowan. "Optical Damage Threshold of Silicon for Ultrafast Infrared Pulses". In: *AIP Conference Proceedings*. AIP, 2006, pp. 837–843. DOI: 10.1063/1.2409223.

[Dob+18] Christoph Dobraunig et al. "Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures". In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part II*. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11273. Lecture Notes in Computer Science. Springer, 2018, pp. 315–342. DOI: 10.1007/978-3-030-03329-3_11. URL: https://doi.org/10.1007/978-3-030-03329-3%5C_11.

[F G07] F Graham Smith, Terry A King, and Dan Wilkins, ed. *Optics and Photonics: An Introduction*. Second Edition. John Wiley & Sons, 2007.

[Fat+13] Hanieh Fattahi et al. “Efficient, octave-spanning difference-frequency generation using few-cycle pulses in simple collinear geometry”. In: *Optics letters* 38.20 (2013), pp. 4216–4219. DOI: 10.1364/OL.38.004216.

[Fuh+13] Thomas Fuhr et al. “Fault attacks on AES with faulty ciphertexts only”. In: *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE. 2013, pp. 108–118.

[Göp31] Maria Göppert-Mayer. “Über Elementarakte mit zwei Quantensprüngen”. In: *Annalen der Physik* 401.3 (1931), pp. 273–294. ISSN: 00033804. DOI: 10.1002/andp.19314010303.

[Hab65] Donald H Habing. “The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits”. In: *IEEE Transactions on Nuclear Science* 12.5 (1965), pp. 91–100.

[Hal+14] Joel M. Hales et al. “Simulation of Light-Matter Interaction and Two-Photon Absorption Induced Charge Deposition by Ultrashort Optical Pulses in Silicon”. In: *IEEE Transactions on Nuclear Science* 61.6 (2014), pp. 3504–3511. ISSN: 0018-9499. DOI: 10.1109/TNS.2014.2368569.

[HBB16] Wei He, Jakub Breier, and Shivam Bhasin. “Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks”. In: *International Conference on Security, Privacy, and Applied Cryptography Engineering*. Springer. 2016, pp. 27–46.

[He+16] Wei He et al. “Ring oscillator under laser: potential of pll-based countermeasure against laser fault injection”. In: *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE. 2016, pp. 102–113.

[He+17] Wei He et al. “An FPGA-compatible PLL-based sensor against fault injection attack”. In: *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE. 2017, pp. 39–40.

[Hor86] H. Hora. “Y. R. Shen, The Principles of Nonlinear Optics, John Wiley & Sons, New York, 1984, 576 pages”. In: *Laser and Particle Beams* 4.2 (1986), pp. 318–319. ISSN: 0263-0346. DOI: 10.1017/S0263034600001889.

[Jai+21] Vibhor Jain et al. *Active attack prevention for secure integrated circuits using latchup sensitive diode circuit*. US Patent 11,171,095. Nov. 2021.

[Kai+10] Tian Kai et al. “Comparison study of the charge density distribution induced by heavy ions and pulsed lasers in silicon”. In: *Chinese Physics C* 34.1 (2010), pp. 148–151. ISSN: 1674-1137. DOI: 10.1088/1674-1137/34/1/028.

[Li+] Z. Y. Li et al. “Nonlinear absorption in single-photon detector and ultrafast mode-locked laser pulse characterization”. In: *Optical Fiber Communication Conference*. Washington, D.C.: OSA, W2A.6. ISBN: 978-1-943580-38-5. DOI: 10.1364/OFC.2018.W2A.6.

[Man+15] Salvador Manich Bou et al. “Backside polishing detector: a new protection against backside attacks”. In: *DCIS’15-XXX Conference on Design of Circuits and Integrated Systems*. 2015.

[Mat+18] Kohei Matsuda et al. “A 286 f 2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack on cryptographic processor”. In: *IEEE Journal of Solid-State Circuits* 53.11 (2018), pp. 3174–3182.

[Mat+19] K Matsuda et al. “An information leakage sensor based on measurement of laser-induced opto-electric bulk current density”. In: *Int. Conf. on Solid State Devices and Materials (SSDM) Extended Abstracts, 2019*. 2019, p. 501.

[McM+02] D. McMorrow et al. “Subbandgap laser-induced single event effects: carrier generation via two-photon absorption”. In: *IEEE Transactions on Nuclear Science* 49.6 (2002), pp. 3002–3008. ISSN: 0018-9499. DOI: 10.1109/TNS.2002.805337.

[Mei+07] Cedrik Meier et al. “Silicon nanoparticles: Absorption, emission, and the nature of the electronic bandgap”. In: *Journal of Applied Physics* 101.10 (2007), p. 103112. ISSN: 0021-8979. DOI: 10.1063/1.2720095.

[Mik+19] Takuji Miki et al. “A Si-backside protection circuits against physical security attacks on flip-chip devices”. In: *2019 IEEE Asian Solid-State Circuits Conference (A-SSCC)*. IEEE. 2019, pp. 25–28.

[Miu+16] Noriyuki Miura et al. “Pll to the rescue: a novel em fault countermeasure”. In: *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE. 2016, pp. 1–6.

[Net+06] Egas Henes Neto et al. “Using bulk built-in current sensors to detect soft errors”. In: *Ieee Micro* 26.5 (2006), pp. 10–18.

[NMM21] Makoto Nagata, Takuji Miki, and Noriyuki Miura. “Physical Attack Protection Techniques for IC Chip Level Hardware Security”. In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2021).

[NS04] A. Y. Nikiforov and P. K. Skorobogatov. “Physical Principles of Laser Simulation for the Transient Radiation Response of Semiconductor Structures, Active Circuit Elements, and Circuits: A Linear Model”. In: *Russian Microelectronics* 33.2 (2004), pp. 68–79. ISSN: 1063-7397. DOI: 10.1023/B:RUMI.0000018711.96346.1d.

[NS06] A. Y. Nikiforov and P. K. Skorobogatov. “Physical principles of laser simulation for the transient radiation response of semiconductor structures, active circuit elements, and circuits: A nonlinear model”. In: *Russian Microelectronics* 35.3 (2006), pp. 138–149. ISSN: 1063-7397. DOI: 10.1134/S1063739706030024.

[SA02] Sergei P Skorobogatov and Ross J Anderson. “Optical fault induction attacks”. In: *International workshop on cryptographic hardware and embedded systems*. Springer. 2002, pp. 2–12.

[Sal03] Reza Salem. “Characterization of Two-photon Absorption Detectors for Application in High-speed Optical Systems: PhD Thesis, University of Maryland, College Park”. In: (2003).

[Sel+15] Bodo Selmke et al. “Precise Laser Fault Injections into 90 nm and 45 nm SRAM-cells”. In: *Smart Card Research and Advanced Applications - 14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Revised Selected Papers*. 2015, pp. 193–205. DOI: 10.1007/978-3-319-31271-2_12. URL: https://doi.org/10.1007/978-3-319-31271-2%5C_12.

[Sel+18] Bodo Selmke et al. “Locked out by Latch-up? An Empirical Study on Laser Fault Injection into Arm Cortex-M Processors”. In: *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2018, Amsterdam, The Netherlands, September 13, 2018*. 2018, pp. 7–14. DOI: 10.1109/FDTC.2018.00010. URL: https://doi.org/10.1109/FDTC.2018.00010.

[She00] Sheik-Bahae, Mansoor and Hasselbeck, Michael P. “OSA handbook of optics IV”. In: *Third Order Optical Nonlinearities* (2000).

[SHS16] Bodo Selmke, Johann Heyszl, and Georg Sigl. "Attack on a DFA Protected AES by Simultaneous Laser Fault Injections". In: *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016, Santa Barbara, CA, USA, August 16, 2016*. 2016, pp. 36–46. DOI: 10.1109/FDTC.2016.16. URL: https://doi.org/10.1109/FDTC.2016.16.

[TMA11] Michael Tunstall, Debdeep Mukhopadhyay, and Subidh Ali. "Differential fault analysis of the advanced encryption standard using a single fault". In: *IFIP international workshop on information security theory and practices*. Springer. 2011, pp. 224–233.

[Vie+17] Raphael Andreoni Camponogara Viera et al. "Role of Laser-Induced IR Drops in the Occurrence of Faults: Assessment and Simulation". In: *Euromicro Conference on Digital System Design, DSD 2017, Vienna, Austria, August 30 - Sept. 1, 2017*. 2017, pp. 252–259. DOI: 10.1109/DSD.2017.43. URL: https://doi.org/10.1109/DSD.2017.43.

[Vie+19] Raphael A Camponogara Viera et al. "Simulation and experimental demonstration of the importance of IR-drops during laser fault injection". In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 39.6 (2019), pp. 1231–1244.

[Yao+21] Yuan Yao et al. "Programmable RO (PRO): A Multipurpose Countermeasure against Side-channel and Fault Injection Attack". In: *arXiv preprint arXiv:2106.13784* (2021).