# Ring Oscillator under Laser: Potential of PLL based Countermeasure against Laser Fault Injection

Wei He, Jakub Breier, Shivam Bhasin
Physical Analysis and Cryptographic Engineering
Nanyang Technological University, Singapore
{he.wei, jbreier, sbhasin}@ntu.edu.sg

Noriyuki Miura, Makoto Nagata
Graduate School of System Informatics
Kobe University, Kobe, Japan
{miura, nagata}@cs.kobe-u.ac.jp

***Abstract*—As a typical semi-invasive attack against cryptographic primitives, laser fault injection (LFI) has emerged as a serious threat for security ICs. However, very few countermeasures against LFI have been proposed in previous literature. In this paper, a logic-level countermeasure for sensing the malicious laser injection on FPGA is presented. The implemented logic consists of a digital inverter ring oscillator (RO) for detecting the frequency disturbance by laser, and a Phase Locked Loop (PLL) to monitor the frequency ripple in RO, for generating an 'alarm' signal. The effectiveness of this countermeasure is validated by a series of laser scan on Xilinx Virtex-5 FPGA. The experimental results show that the detection rate reaches up to 92.82% for protecting the registers in slice, and the countermeasure offers a significant security margin against LFIs.**

***Index Terms*—Cryptography, Laser Fault Injection, Countermeasure, Ring Oscillator, Phase Locked Loop, FPGA**

## I. Introduction

Cryptographic security has gained paramount importance during the past decade owing to the prevailing usages of embedded devices in our daily life. Confidential and critical information have to be encrypted and securely transmitted, stored and processed for ensuring the data security. Security in this domain basically consists of two metrics: (a) security of algorithm, where modern cryptography has provided sufficient security grade against pure mathematical cryptanalysis; (b) security of implementation, which normally concerns the implementation itself. The latter can have several source of vulnerabilities e.g., network, operating system, hardware etc. The threats targeting hardware are popularly known as physical attacks and can be widely classified into side-channel attack (SCA), and the fault injection attacks (FIA). FIA mainly purposely injects computation faults into the device, and exploit the induced faulty behaviors for extracting the secrets.

To inject a fault into a cryptographic hardware, several techniques can be deployed which differ in precision and cost. Some fault injection techniques induce random fault in the system by perturbating electrical disturbance into a global variable. Such systems can be fairly inexpensive with limited precision at hand. The solutions which fall under this category are glitch on clock system or power supply, or deploying out of specification clock (overclocking) or power (underpowering) to the system till faults occur. When using global injection techniques, the adversary might need to collect a large number of faulty outputs to identify the useful ones.

When higher precision is needed, the adversary must resort to local fault injection techniques. These technique can even precisely inject the faults into the desirable data bits. However, the precision comes at the high cost of equipment and expertise to identify precise point of interests (POIs). The typically used local injection techniques are laser based fault injection (LFI) and electromagnetic fault injection (EMI).

The defense against fault attacks can be classified under detection and prevention. While detection methods try to sense attack attempts and raise an alarm, prevention techniques aim for fault resilience. Resilience signifies the ability to either bypass the faults or detect and correct/infect the sensitive data simultaneously. In general, resilience relies on error correction code. An implementation of duplication code in terms of dual-rail logic was presented [1].

To detect fault injection, one can detect either at data level or circuit level. There are also other package level solutions like tamper-resistant cover, or light detectors which stay out of scope of the paper.

- Data-level detection uses error detection code like parity to detect any modification of the data. A prominent example is `parity predictor` [2], implemented in parallel with the cryptographic

computation. The predictor pre-computes the parity of the output of a cipher operation, by knowledge of the input. If the parity of final output does not matches the original prediction, an alarm is raised. The predictor part is generally merged with the cipher logic and cost almost as much as the cipher operation itself. **Importantly**, the alarm is only triggered when a valid fault has been injected into the protected cipher, e.g., it has no security margin to predict an on-going injection campaign in advance. Moreover, the protection is only valid on specific fault models.

- Circuit-level detection uses deployed sensors, on top of the cryptography to detect faulty environmental parameters, and thus fault model agnostic. These sensors can be analog, digital or mixed in nature. An instance is the `glitch detector` proposed in [3]. This logic functions to detect the glitch that is induced by the global or local means, and subsequently triggers an 'alarm' signal. However, it does not prevent fault injection into the cipher. So a security margin is required for effective protection.

This paper explores protection techniques against laser fault injection. The essential prerequisite of a valid countermeasure should have the following merits: (a) `strength`: the minimum laser strength of triggering the 'alarm' is lower than the minimum laser strength of injecting valid cipher faults, and (b) `spatial`: the area of protection coverage must be larger than the area wherein the fault can inject cipher fault.

A ring oscillator (RO) based countermeasure against EMI was proposed by Miura et al. in [4], which relies on a commonly used frequency-modulation component: phase locked loop (PLL) that can be easily found in a wide spectrum of high-performance ICs. An inverter based high-frequency Ring Oscillator (RO) is deployed as a watchdog, which senses an EM pulse injection leading to PLL triggering an alarm. The proposed countermeasure reports excellent spatial and strength parameters.

This paper thoroughly explores the application of PLL/RO based detectors against LFI. Since the physical property of LFI is significantly different from EMI, the constraints on design of watchdog RO are different. These constraints involve specific routing constraints, and the security grade is evaluated relying on a series of laser injection scan on a Xilinx exemplary FPGA.

The remainder of this paper is organized as follows: Section II presents the relevant background about LFI and the detection countermeasures. Section III discusses about the technical details of RO based detection system against LFI. Section IV details countermeasure implementation and experimental setup. The experimental results and some further discussions are elaborated in Section V. Section VI draws work conclusion and perspectives of future work.

## II. Technical Background

This section provides basic background on architecture of modern FPGA (target platform), lightweight cryptographic algorithm PRESENT (sensitive core) and laser fault injection (attack technique).

### A. FPGA Architecture

As the major FPGA vendor, Xilinx provides series of products that have been widely used in academia and industry. Even with technology upgrading and function enhancement, the basic architecture is generally consistent for different series of devices. Fig. 1 illustrates a brief view of the architecture of Virtex-5 FPGA, which is composed of an array of configurable logic blocks (CLBs) in a mesh fashion. As the most fundamental logic cell, CLB basically consists of two slices, and each slice has 4 6-input look-up-tables (LUTs), 4 multiplexors, 4 flip-flops and a carry chain. LUT is intrinsically a 64-bit SRAM which can be configured to implement any single 6-input Boolean function, or 2 Boolean functions with no more than 5 shared inputs, or 2 Boolean functions with no more than total 5 different inputs. Each CLB has a switch-box, providing interconnects to the local or global routing channels over the entire FPGA matrix, as illustrated in Fig. 2. To enlarge the usage of FPGA, rich digital or analog functional modules are provided on-chip, as the clock managing elements: phase locked loop (PLL), digital clock manager (DCM), embedded temperature and voltage sensors (System Monitor), Block RAM, and digital signal processor (DSP), etc.

### B. PRESENT Block Cipher

The target of this case study is lightweight block cipher **PRESENT** which is standardized under `ISO/IEC 29192-2:2012`. As a low-cost and substitution-permutation network (SPN) based cipher, PRESENT is particularly compact in hardware implementation for being used in devices where low-power consumption and high chip efficiency is desired. These devices are attractive targets for malicious physical attacks, such as side-channel attacks and fault attacks, since expensive countermeasures would be unaffordable in consideration of costs. The block size of PRESENT is 64 bits and the

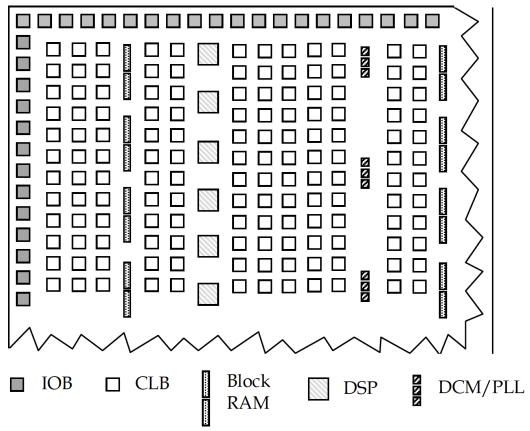



Fig. 1: Virtex-5 architecture overview.

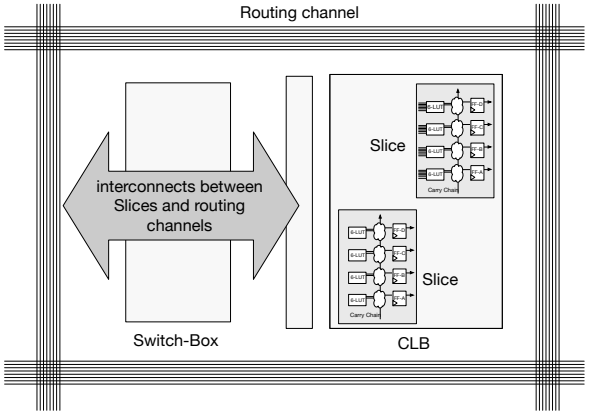



Fig. 2: CLB logic cluster and routing resources.

key size can be either 80 or 128 bits. For PRESENT-80, the 64-bit plaintext is encrypted using 80-bit key with 11 computation rounds. A group of 64-bit round data registers are used in each round for storing the data bits. The structure of the implemented PRESENT-80 is depicted in Fig. 3. As the typical targets, registers are vulnerable against laser fault injection, which hence needs to be specially protected. Without loss of generality, **round data registers** are considered as the primary target for protection. However, the countermeasure shields the entire algorithm including the combinatorial logic parts.

### *C. Laser Fault Injection*

Ionization effect on transistors is a well-known phenomenon. The first observation of such effect was described in 1975, when flip-flop circuits of communication satellites were triggered by cosmic rays [5]. More specifically, the mechanism for the cosmic ray interaction was the charging of the base-emitter capacitance of a transistor to the turn-on voltage.

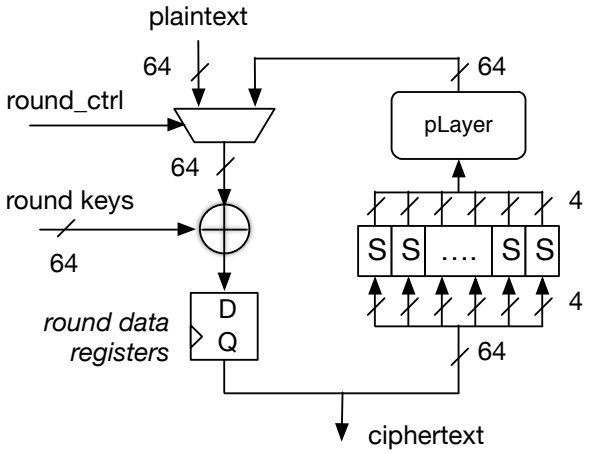



Fig. 3: Structure of PRESENT-80 block cipher.

Since then, a single-event upset (SEU) simulation by lasers has become a standard methodology for testing integrated circuits, providing an inexpensive and fast alternative to the accelerated ion beam technique [6]. Because of the increasing number of the frontside metal layers, it was shown that the most effective way to disturb the circuits by the laser is by focusing the beam through the backside substrate [7]. When using this method, it is still necessary to focus the beam so that it affects the frontside of the chip where the components are positioned, as seen in Fig. 4. This figure also shows that it is important to have a constant thickness of the substrate, because any variation in wafer thickness results in different Z-position of the focal point with respect to sensitive components one wants to target. Also, the backside should be polished so that the beam quality would not be affected by silicon absorption and refraction.

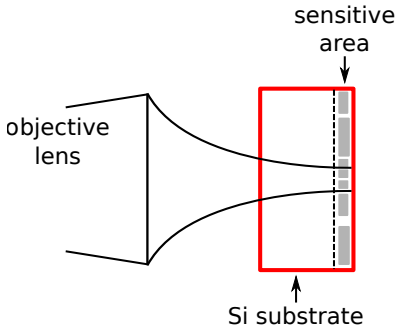



Fig. 4: Backside laser targeting.

As the beam passes through the surface, it converges. The angle of incidence varies across the beam from 0 degree to its maximum ($sin^{-1}(r_1/l)$), where $r_1$ is the

lens radius and $l$ is the distance of the lens from the surface [8]. This is also illustrated in Fig. 5. By changing the distance from the surface, the resulting spot size of the laser varies. First, the laser is focused on the surface (a), then it moves by distance $\Delta z$ so that it is focused on sensitive components (b). This value can be calculated by the following equation:

$$\Delta z = \frac{t_{sub}}{\eta_{Si}} \tag{1}$$

where $t_{sub}$ is the substrate thickness, and $\eta_{Si}$ is the refractive index for silicon. For example, for near-infrared laser used for backside laser irradiation, the value is $\eta_{Si}$ (1064 nm) = 3.5.

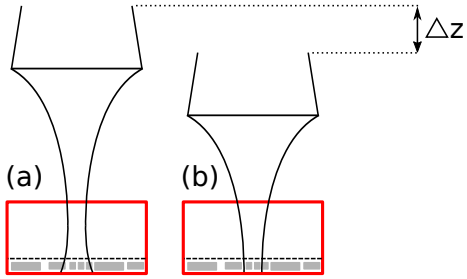



Fig. 5: Focusing on the sensitive spot – in case of (a), laser is focused on the backside surface of the chip, in case of (b), it is focused on sensitive components. In both cases, the effective laser spot will be different.

In order to determine the most effective wavelength for triggering SEU, the following formula gives the first-order approximation of the electron-hole pairs generation:

$$\frac{dN}{dt}(d) = \frac{\alpha\lambda}{hc} I(d) \tag{2}$$

where $d$ is the substrate thickness, $\alpha$ is the absorption coefficient, $\lambda$ is the wavelength, $h$ is the Planc constant, and $I$ is the laser intensity. Experimental measurements show that the following expression approximates the absorption in silicon [9]:

$$\alpha = \left(\frac{84.732}{\lambda} - 76417\right)^2 \tag{3}$$

It means, for a substrate thickness $d = 400\mu m$, the maximum generation rate is obtained for a wavelength of 1.04 $\mu m$ [7]. For thinner substrates, optimum wavelength is lower. Therefore, lasers with near-infrared wavelengths are suitable candidates for the backside testing.

Fig. 6 shows the situation when the NMOS drain of the OFF transistor is irradiated by a pulse laser [10]. Photo-generated holes (grey dots) flow to the ground line via the NMOS body and the photo-generated electrons (black dots) flow to the power line, via the PMOS transistor. However, if the laser is focused on the drain of the ON transistor, there will be no photocurrent generated and the transient voltage will not propagate to the gates on its output.

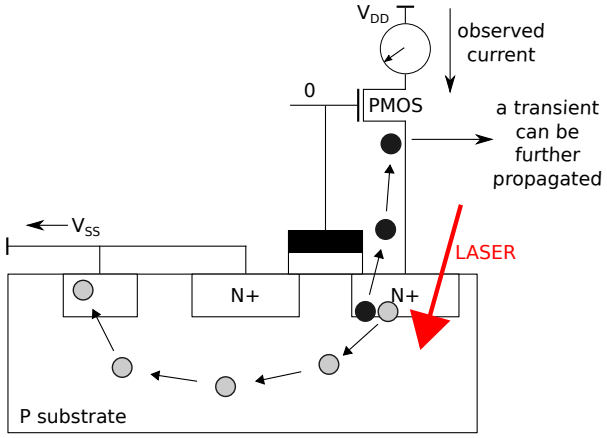



Fig. 6: Effect of laser when focused on the OFF transistor.

The effective spot size is another important parameter when targeting sub-micron components. It is mostly determined by the optics and the wavelength. If the laser spot is smaller than the component size, it is possible to determine the amount of charge deposited in the component by converting the laser energy to a linear energy transfer (LET) equivalent by the following formula [8]:

$$LET = (1 - R(\lambda)) \cdot \frac{E_0 \cdot E_p}{E_\gamma} \cdot \frac{1 - e^{\alpha(\lambda)d}}{\rho d} \tag{4}$$

where $R(\lambda)$ is the reflection coefficient, $E_p$ is the electron-hole creation energy (3.6 eV/pair in Si), $E_\gamma$ and $E_0$ are the photon and incident energies, respectively. $\rho$ is the material density, $\alpha(\lambda)$ is the absorption coefficient, and $d$ is the charge collection depth.

When it comes to hardware-level countermeasures, there are several full custom approaches focusing on creating a fault tolerant design. There are designs of single-event tolerant flip-flops [11], redundancy approaches using back-up transistors [12], [13], or even special transistor designs that can resist radiation [14]. Recently, Lacruche et al. [15] evaluated the effects of forward body biasing on the sensitivity of registers of a microcontroller under the laser fault injection. They are able to decrease

repeatability of the faults. Note that the countermeasure proposed was not preventing laser injection, it was affecting the repeatability only.

## III. Laser Fault Injection Countermeasure

The mechanism of laser fault injection is described in the previous section. To recall the main principle, a laser injection on a semiconductor circuit induces a localized but very high-energy disturbance on the point of impact or focus. The high energy leads to photocurrent thus causing a SEU. However, with the shrinking technology, it is hard to focus on a single transistor, which leads to event upset in several neighbouring transistors. A laser injection countermeasure would detect such photocurrent before a SEU and raise an 'alarm'. A straightforward approach to design a countermeasure would be to use photodetectors or equivalent full custom design. However, it is not always possible to deploy such custom sensors. The PLL based fault countermeasure was initially proposed in [4] to detect EMI. In the rest of the section, the principle of this countermeasure is elaborated, followed by its potential application for laser fault detection in sub-nanometer technology nodes.

### A. Fault Injection Sensor

The schemed countermeasure is composed of two principle components: a PLL and a watchdog RO. PLL is a widely used for analog component for modulating clock of digital circuit. It detects phase and frequency difference between clock source and a feedback to keep the phase synchronization. This functionality is established with three basic components i.e., Phase-Frequency Detector (PFD), Low Pass Filter (LF), and Voltage-Controlled Oscillator (VCO). The PFD compares the timing of the input clock with the feedback clock. The polarity and magnitude of the difference are converted into *UP* and *DOWN* pulses. These pulses are then converted into a control voltage by LF which drives the VCO to adjust the phase and frequency and bring the two frequencies in synchronization. This phenomenon is depicted in Fig. 7.

One of the main function of PLL is to monitor the stability of internal clock. When a fault injection attempt is made using local injection techniques, the circuit experiences intentional induction of instantaneous abnormal energy or charge to disturb or overwrite normal operations. In order to detect such abnormal injection, a watchdog RO was proposed as a clock generator. This watchdog clock is continuously monitored by the PLL. Under normal conditions, the RO clock is stable

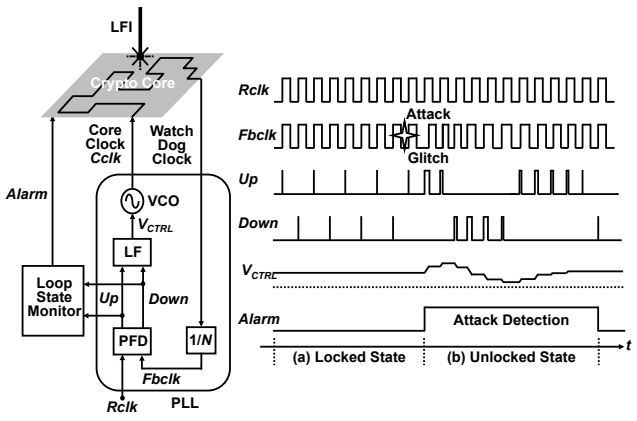



Fig. 7: Block diagram of PLL-based FI countermeasure. The waveforms depicts (a) lock and (b) unlock state.

in phase and frequency, which leads PLL into a locked state as shown in Fig. 7(a). An instantaneous injection can disturb the phase of the RO watchdog clock, which forces the PLL into unlock state as in Fig. 7(b). The lock signal from the PLL serves as the 'alarm' in this case, which is triggered by laser injection.

In [4], authors proposed to place the RO over the sensitive core in order to detect EMI campaign. This configuration proved efficient with a significant security margin and spatial coverage. However, the injection mechanism of EMI is different from LFI. LFI injections are more local and the fault is caused by induction of high energy as compared to interfering field in EMI. Therefore the countermeasure proposed in [4] cannot be directly used. In the following, the proposed modifications are described in order to make the countermeasure effective against LFI.

### B. Laser Detection using RO

Photodetectors and equivalent custom cells were previously used to detect laser injection. The intention of this work is to use readily available components and cell library to design a countermeasure, specially for FPGA. Whenever a laser is injected in a semiconductor device, a high energy is induced. If the laser is well focused to a particular cell, this energy can cause SEU (see Fig. 6).

RO, in principle, is a low-cost running oscillator which is a closed loop chained by **odd** number of inverters, as sketched in Fig. 8. RO has been widely applied in security circuit domain, particularly as the RO physical unclonable function (RO PUF) and random number generator (RNG), etc. Upon start-up, the RO undergoes a 'warm-up' phase to find a locking state with stable

frequency $f_{RO}$ i.e., inverse time period $t_{RO}$ of the RO path delay. The frequency of RO is sensitive to process, voltage and temperature (PVT) variation.

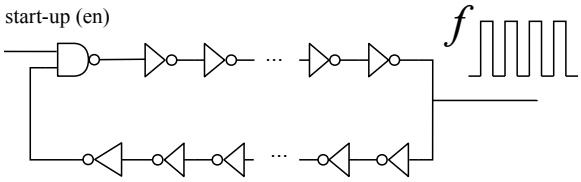



Fig. 8: Digital inverter based ring-oscillator.

In the event of laser injection, the instantaneously induced energy modifies the PVT parameters near POI region. As RO is sensitive to PVT variation, the injection should impact the phase and frequency of output clock. A single inverter RO was implemented covering 9 adjacent CLB to generate a clock. The RO generated a clock of 210 MHz which is shown in Fig 9 (top). In the event of laser injection in the region of RO placement, it can be observed in Fig. 9 (bottom), that the instantaneously induced energy by laser modifies the phase, frequency and amplitude of the RO output frequency. After the injection, the RO eventually settles to its natural oscillating frequency.

Since the laser injection modifies the phase of RO, this modification of phase can be easily detected by a PLL as shown in [4]. However, as stated earlier, the energy injection in laser stays very localized. Therefore, the RO must be placed close to POI, otherwise the energy might fail to diffuse to the RO sensor. If the placement of RO is not precise, the RO might have low or even zero detection rate. The constraint is different from EMI, where a RO over the sensitive circuit proved secure enough, as EMI injects disturbance using EM field. This motivates deployment of small and local RO protecting very small POIs. In the following section, an empirical characterization for appropriate size and placement for RO is provided.

Apart from LFI and EMI, the attacker can exploit the external clock to crypto-core to perform an FSA [16]. As in the original EMI countermeasure, by carefully designing the maximum operating frequency of the crypto core to be higher than the tuning range of PLL, FSA can be avoided.

## IV. System Implementation and Experimental Setup

Two scenarios are considered to evaluate the security margin of proposed countermeasure in terms of

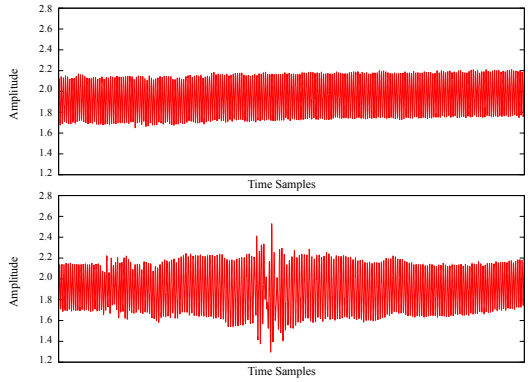



Fig. 9: RO generated clock (top) under impact of laser injection (bottom).

`strength` and `spatial`. In the first scenario, the protection target is the security-critical registers of the implemented cryptography, which requires high detection rate in locations where register data faults are injected, e.g., security margin of laser `strength` is considered. In the second scenario, the `spatial` security margin is evaluated by computing all the locations where either countermeasure or data faults are triggered. This assumption is more reasonable in practice since the adversaries typically need to launch a scan campaign for a larger chip region for finding the POIs where the security-critical logic is deployed. In case the countermeasure can sense the laser injection when the scanning has not yet reached the POIs, the protection mechanism can react in advance against the LFI.

### A. FPGA Implementation

To validate the effectiveness against LFI, the countermeasure is implemented in a Xilinx Virtex-5 (VLX50T) FPGA, manufactured on 65 nm SRAM technology.

*1) Implementation 1:* For testing the `spatial` security margin, we implemented a RO which covers 9 CLBs. Only 1 LUT from a slice is used to implement the single inverter of this RO, and the routing path is intentionally handled as a rectangle. Since routing in FPGA is not controllable directly using the router in commercial EDA toolkit, a router is instantiated from the customized APIs constructed upon Rapidsmith [17], [18], to enforce the routing path of the RO through three corners, but without using the LUTs in the corners, as indicated in Fig. 10. The full signal delay of this RO is $4.762\ nS$, yielding an oscillation frequency of $\approx 210MHz$. A PLL is instantiated into this design and the RO output is connected to PLL's `clkin` input. The `elocked` output of PLL is connected to the cipher

`reset` pin, in order to reset the whole cipher in case the frequency disturbance induced by the laser is detected. The PLL is tuned properly to the frequency range of the implemented RO. Here, 40 out of the 64 round data register bits of PRESENT-80 have been deployed into 5 CLBs, as indicated by the dotted line region of Fig. 10. This special implementation is for demonstrating the influence of laser impacts on the RO and data registers that are not closely situated in the same CLBs.

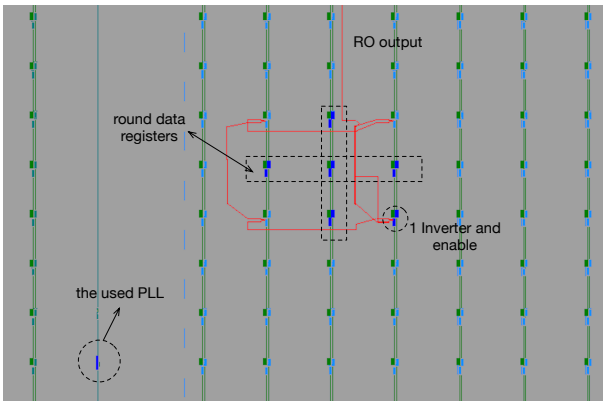



Fig. 10: Schematic view of routing controlled RO loop, covering 9 CLBs.

*2) Implementation 2:* For testing the `strength` security margin, we exclusively investigate the detection rate for each individual slice, as shown in Fig. 2. The RO is implemented by a single inverter using an LUT, while the other 3 LUTs inside this slice have been chained in this loop but only implementing a transparent gate. This helps to increase the routing density inside this slice. Since the routing is passing only through this slice, the summed up routing delay of this 1-inverter RO is only 3.846 $nS$, which yields an output frequency $\approx$ $260MHz$. The 4 flip-flops in this slice are used to implement 4 out of the 64 **round data register** bits of PRESENT-80 cipher. The neighbouring slice is used to generate the enable signal of this RO. The connection and configuration of PLL are the same with implementation 1. The schematic view of the single slice implemented 1-inverter RO is shown in Fig. 11.

### *B. Experimental Setup*

All the components of our setup are depicted in Fig. 12, where the connections between them are illustrated by dashed lines. The main component is the *Risure* diode pulse laser station [19], controlled by a triggering device connected to the computer. DUT and positioning table are directly controlled from the computer. Oscilloscope is used in order to check the critical signals from the DUT.

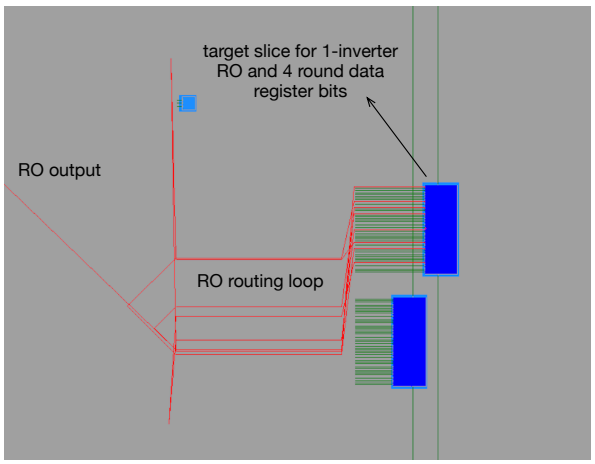



Fig. 11: Schematic view of single slice RO.

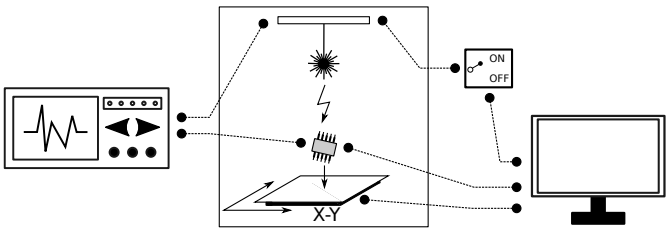



Fig. 12: Schematic of components involved in the experimental setup.

The diode pulse laser source used for experimental validation has the following properties:

- Pulse power: 20 W (reduced to 10 W and 8 W with 5$\times$ and 20$\times$ objective lens, due to the optical property of the used lens)
- Pulse repetition: 10 MHz
- Spot size: 60$\times$14 $\mu$m$^2$ (5$\times$ objective lens), 15$\times$3.5 $\mu$m$^2$ (20$\times$ objective lens)
- Response to trigger pulse: $\leq$ 60 ns
- Pulse length adjustable by: 1 ns

The experimental target is the *Genesys* board from Digilent which has a Virtex-5 FPGA that is chosen to implement the PRESENT-80 cipher and the countermeasure system. The trigger signal for activating the laser injection from glitch generator is intentionally generated from cipher. The trigger time is set to the last encryption round, hence the affected data bits can be directly observed by a comparison between the faulty ciphertext and the corresponding right ciphertext. As aforementioned, the diode pulse laser with 5$\times$ and 20$\times$ objective lens are

employed for performing laser injection. X-Y positioning table was used for scanning the entire region of the chip. This table has a step precision of 0.05 $\mu$m. Fig. 13 shows the main part of the setup for our experiments.

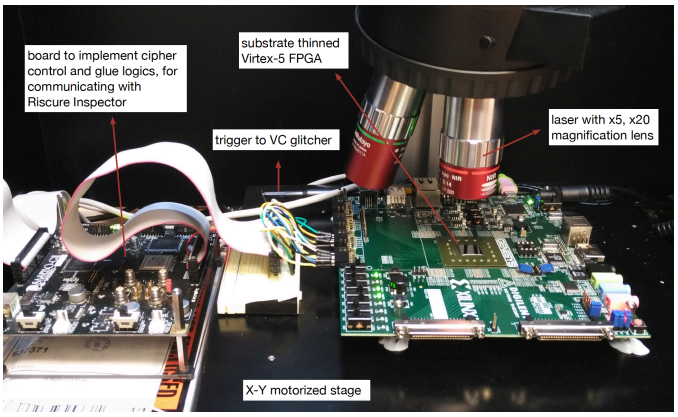



Fig. 13: Experimental setup for laser injection campaign.

### C. Chip Preparation of Virtex-5

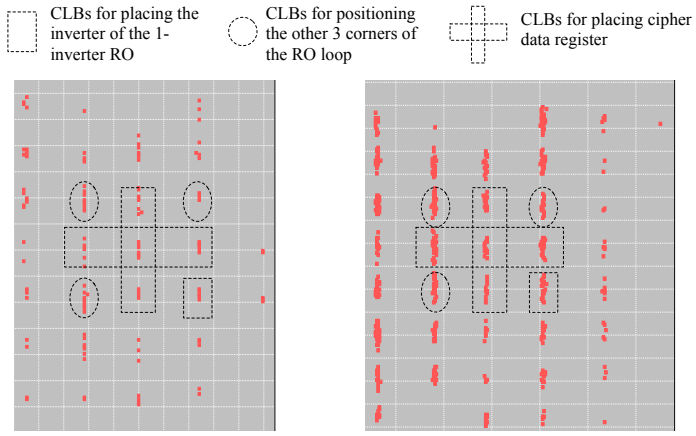
The target 65nm Virtex-5 FPGA comes with flip-chip package. To enable laser injection, firstly the heat-sink metal lid over the FPGA was removed, which exposes the chip substrate. However, the substrate on the die is $\approx$ 300 $\mu m$, which absorbs a majority of induced energy/charges, thus preventing efficient fault injection. So the chip substrate was further thinned down to $\approx$ 100 $\mu m$ by specialized backside polishing equipment. After this operation, it was possible to inject faults in slice registers using our laser.

## V. Experimental Evaluation

This section describes the methods for validating the countermeasure described in Section III, together with experimental results using the LFI test bench.

### A. Countermeasure Sensitivity

The countermeasure from implementation 1 is tested for observing its detection sensitivity against laser impact. In this experiment, we employed the diode pulse laser with $20\times$ and $5\times$ objective lens respectively. Fig. 14 demonstrates the results by scanning the region where the cipher data registers and RO sensor are deployed. Each red dot represents a successful LFI detection. The scan matrix is $240 \times 200$, which results in 48,000 points to be scanned for each test. Note that the round data registers are only implemented inside the 5 CLBs, highlighted by the dotted rectangle region, and the rest part of the PRESENT cipher are placed in remote FPGA fabric, to keep it intact from this scan. The scan result shows very regular distribution of the POIs, which exactly matches the CLB array of the target FPGA, as seen in Fig. 10.




(a) with 20x objective lens (b) with 5x objective lens

Fig. 14: Laser injection scan to countermeasure deployed region using different objective lenses.

The scan results are summarized as follows:

- The frequency disturbance induced by LFI using both $20\times$ and $5\times$ objective lens could trigger the 'unlock' of PLL, while injection using $5\times$ lens have higher probability to be detected. This is because of the higher energy transmitted from the larger laser spot by the smaller objective lens.
- No data fault was successfully injected into any bit of the 40 implemented registers in this region, using $20\times$ lens, while data faults were injected using laser with $5\times$ lens. It is also because the energy transmitted by the smaller laser spot from $20\times$ lens is not sufficient to upset the data registers.
- **Importantly**, both results clearly show that despite the neighbouring CLBs are unused (see Fig. 10), when the laser was injected into the those CLBs, the alarm can still be triggered with high probability. Meanwhile the cipher was working normally, except for the flipped bits in the scanned slices.

Due to the unrevealed information from the bottom layer of commercial FPGA, we cannot directly clarify this phenomenon. However, some useful information can still be extracted by deducing the disclosed knowledge of device architecture. For Xilinx FPGAs, each CLB has a switch-box for providing interconnects from the internal slice pins to external routing channel (refer to Fig. 2). Since the frequency or phase shift of the RO is introduced to the routing part of RO, it is very likely

that the switch-box, impacted by the laser, potentially propagates the signal disturbance to other neighbouring local switch-boxes, which as well are able to incur the 'unlocking' of the PLL. This property is particularly helpful for constructing effective detection system, since it greatly enlarges the detection area, even using a small RO loop.

### *B. Power Threshold for Proposed Countermeasure*

Further analysis are performed to check the power threshold for triggering the alarm signal and the data fault, in order to find the power strength related security margin against LFI. As discussed before, only the laser injection using $5\times$ objective lens has created register faults, hence we just focus on the experimental results shown in Fig. 14(b) for this analysis. Fig. 15 shows the scan of the bigger area around the RO. The scanned area is $\approx 300\times400$ $\mu$m$^2$ large, and the RO is implemented in the middle $3\times3$ matrix, using 4 corner CLBs to handle the routing, as explained in Subsection IV-A. Fig. 15(a) shows the lowest power necessary to trigger the alarm signal of the countermeasure, while Fig. 15(b) shows the lowest power to induce data faults into the implemented cipher **without** triggering alarm. Several important observations are briefed as follows:

- The lowest laser strength to trigger alarm of the countermeasure is 64% of its full power. Comparatively, except two outliers between 75% to 90%, faults into data registers start at 91% and mostly are over 98%. This result shows good `strength` security margin of this LFI detection system.
- The RO/PLL based countermeasure is significantly more sensitive than the valid data registers against LFI, and the alarm can be triggered not just from the RO covered CLBs, but also from the neighbouring CLBs. This result shows better `spatial` security margin of this countermeasure.

### *C. Security Analysis on Single-CLB RO*

The second LFI scan targets implementation 2, where the RO and 4 cipher data registers are embedded inside a single slice from a CLB, as shown in Fig. 11, with an area of $\approx 3\times7$ $\mu$m$^2$. We enforced the RO routing through the other 3 LUTs for (a) increasing the routing density, to have higher sensitivity to laser, and (b) reducing the yielded RO frequency from $> 500MHz$ to $260MHz$, in order to drop into the allowed frequency range of PLL clk input, as specified in [20].

Different from the previous test, we repeated the LFIs in each location for 50 times by increasing laser strength from 51% to 100% with 1% as the step. In this way, the scan result related to the laser strength can be observed. Fig. 16 plots the LFI scan results of this region, where $X$ and $Y$ axes represent the coordinates of the plane of the active transistor layer, and the $Y$ axis demonstrates the laser power level. Points in Fig. 16(a) represent the LFIs that unlocked the PLL, i.e., triggered the alarm signal of countermeasure, and points in Fig. 16(b) shows LFIs that generated single or multiple bit faults from the 4 data registers inside this slice, while **bypassing** the countermeasure. The comparison shows that it is extremely difficult to inject cipher faults without triggering the countermeasure. As well, countermeasure can be triggered from a very low laser strength (from 64%), and the cipher faults require much higher laser strength (from 91%).

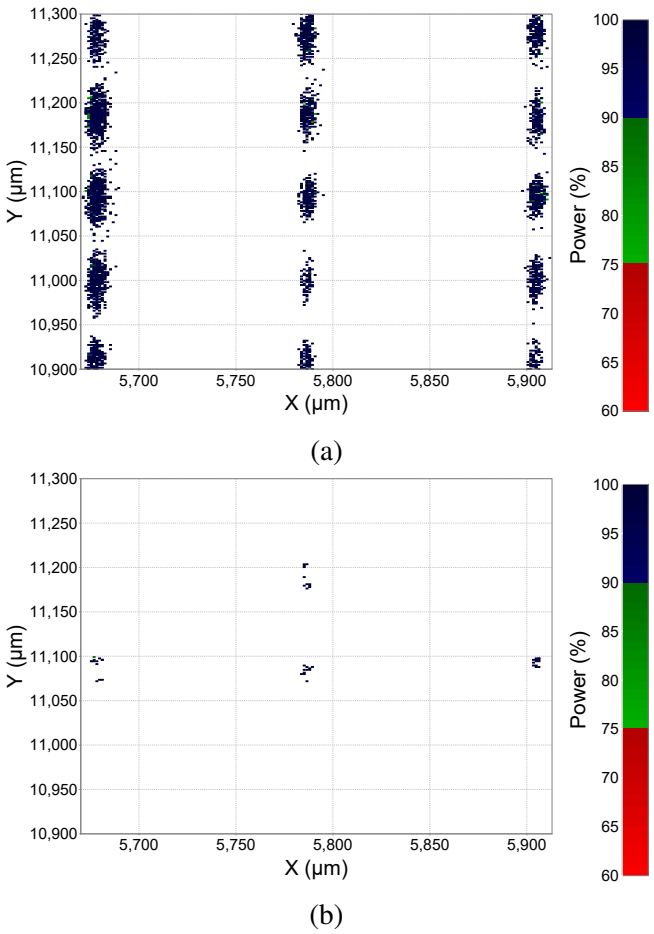
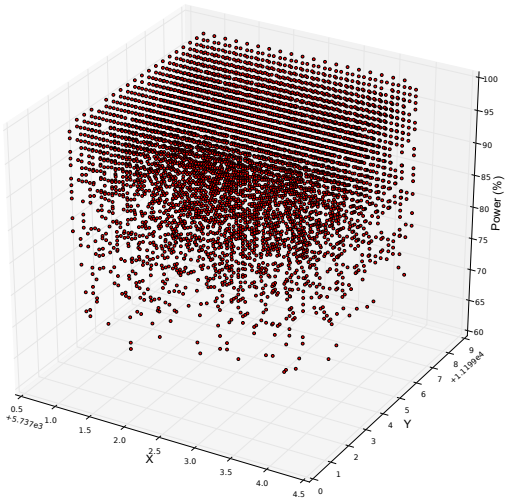
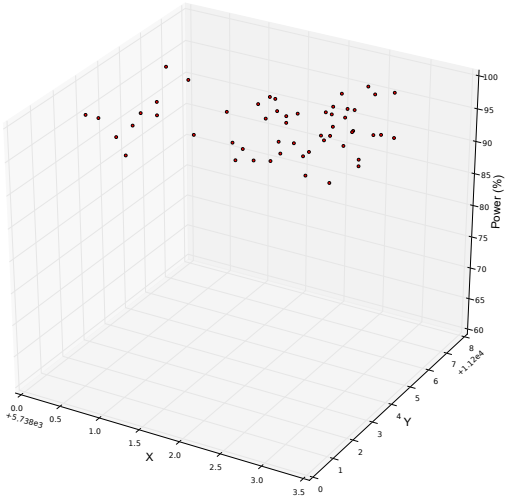



Fig. 15: Area of 15 CLBs sensitive to laser fault injection. Each point of (a) represents the lowest power necessary to trigger the countermeasure, points in (b) shows the lowest power required to cause data faults without triggering the countermeasure.




(a)




(b)

Fig. 16: Area covering one slice, showing the corresponding laser power required to trigger (a) the countermeasure, and (b) data faults.

The power comparison between the detected and undetected cipher faults are given in Fig. 17. It can be seen that both start from around 90% of the full laser power, and the number of detected faults rises quickly following the increasing laser power, with sharp difference to the number of the undetected faults. This result concludes that the countermeasure is easier to be triggered by LFIs than the cipher faults, and the difference is more significant with stronger laser power.

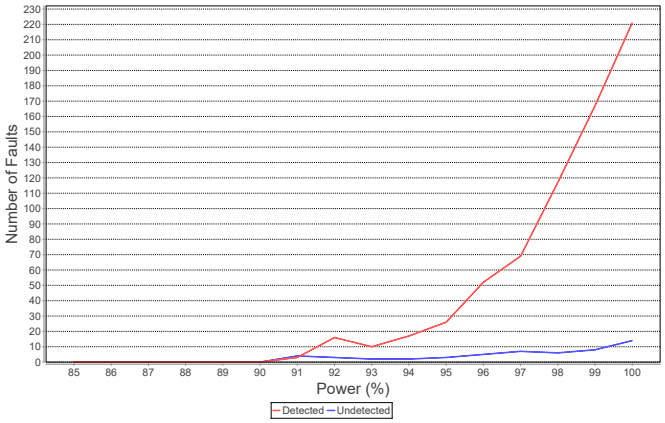



Fig. 17: Total number of detected and undetected faults w.r.t. laser power.

Moreover, Equation 5 is used to compute the detection rate $R_{data}$, which only considers the data fault injection. $N_{injected}$ denotes the times that faults are injected into single or multiple bits of the cipher. $N_{undetected}$ represents the times that faults are injected, but alarm is not triggered (In our case, $N_{injected} = 752$, and $N_{undetected} = 54$). The detection rate in this case is $\approx$ 92.82%, only considering the fault injected LFIs.

$$R_{data} = \frac{N_{injected} - N_{undetected}}{N_{injected}} \tag{5}$$

If we include all the injections that triggered the countermeasure, Equation 6 can be used to compute the ratio between the undetected cipher faults and the detected injection, where $N_{countermeasure} = 5759$ refers to the total times of injections that triggered alarm, which gives a ratio of $R_{undeteced/countermeasure} \approx 0.94\%$. This equation is more suitable to describe the situation that adversary does not know the exact location to perform LFIs. In this case, the inevitable profiling scan risk triggering the alarm of the RO countermeasure, and the chance to inject faults without triggering countermeasure is as low as $0.94\%$, according to the experimental result.

$$R_{undeteced/countermeasure} = \frac{N_{undetected}}{N_{countermeasure}} \tag{6}$$

### D. Further Discussions

*1) Protection Coverage:* The experiments shown above demonstrated the effectiveness of the proposed LFI detection system against the laser attacks, which relies on the PLL to monitor the frequency disturbance into high-frequency ROs induced by laser impacts. In principle, the PLL locked on high-frequency oscillation

is easier to be unlocked by a minor frequency/phase shift induced by laser. Therefore, the RO frequency cannot be too low in order to maintain acceptable detection sensitivity. However, as elaborated in Subsection V-A, the countermeasure can as well detect the LFIs targeting to the neighbouring CLB regions, which actually offers a much larger protected area using special routing shape, like the *zigzag* path applied in [4]. Beside, using long-wire in FPGA routing channels is recommended to construct the RO loop, since it has smaller routing delay compared to the short-wire (due to the fewer interconnects in long-wire routing path). In addition, multiple PLLs are available in modern FPGA devices, so several RO can be deployed in parallel to enlarge the coverage of the protection.

*2) Comparison to Glitch Detector:* Another popular circuit level countermeasure proposed is the glitch detector [3]. This countermeasure is ideally designed to detect global fault injection. It was also shown to work against EM injection when deployed in a sensor network manner. However, its applicability against laser injection is not obvious. First of all, the detector contains flip-flops which can potentially detect LFI. However, if a precise laser is targeting flip-flop of detector, it might not be able to affect flip-flops carrying sensitive data and vice-versa. Moreover, the delay element in the detector is comprised of several LUTs. In event of LFI, the delay of affected element can increase or decrease, depending on the injection source. In this case, the countermeasure sensitivity can be improved (when delay increased) or deteriorated (when delay decreased), which reduces overall reliability.

*3) Accidental Unlock by PVT Variation:* As discussed before, the RO frequency can be affected by the variations of intrinsic electrical properties, as power, voltage and temperature (PVT). It is emphasized that natural PVT parameters are floating by nature in real-world devices, even without the presence of LFIs. However, unlike the sudden and significant impact caused by LFIs, these natural and gradual PVT changes are slight which cannot cause sharp frequency change in RO. The gradual changes in frequency are tolerable by the PLL, since the feedback loop can recalibrate itself, maintaining its locked state if the frequency change is not significant. Therefore, the chance of accidental unlock by natural PVT floating is very low, and in our experiments we did not find any unlocking case without performing LFIs.

## VI. Conclusions and Future Work

In this paper, a frequency based LFI detection system is proposed, which relies on the PLL block, available on modern FPGAs, to sense the frequency disturbance on RO induced by malicious laser injection. In presence of laser impacts, the locked PLL can be unlocked in a short time, which triggers an 'alarm' signal to activate defence responses, like temporary cipher hibernation. To validate the security of this system, we implemented the system on Xilinx Virtex-5 FPGA for protecting a lightweight PRESENT-80 cryptographic primitive. Extensive experimental results show that the proposed countermeasure can detect LFIs in advance of valid cipher faults in data registers, in terms of both *power* and *spatial*, which provides high detection rate and security margin against laser attacks. In addition, some practical recommendations are given for better implementing the countermeasure in real-world applications.

The following work will focus on the protection evaluation for on-chip BRAM that is another major target for LFIs. Another interesting extension can be deploying a network of multiple ROs for enlarging protection coverage without losing sensitivity. The technique of combining several ROs is the key requirement.

## Acknowledgment

The part of the work conducted at Kobe University is partly supported by JSPS KAKENHI No. 26240005.

## References

[1] N. Selmane, S. Bhasin, S. Guilley, T. Graba, and J.-L. Danger, "WDDL is protected against setup time violation attacks," in *FDTC*, 2009, pp. 73–83.

[2] K. Wu, R. Karri, G. Kuznetsov, and M. Goessel, "Low Cost Concurrent Error Detection for the Advanced Encryption Standard," in *In Proceedings of the IEEE International Test Conference (ITC 2004)*, 2004, pp. 1242–1248.

[3] L. Zussa, A. Dehbaoui, K. Tobich, J. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clédière, and A. Tria, "Efficiency of a glitch detector against electromagnetic fault injection," in *Design, Automation & Test in Europe Conference & Exhibition, DATE'14, Dresden, Germany, March 24-28, 2014*, 2014, pp. 1–6.

[4] N. Miura, Z. Najm, W. He, S. Bhasin, X.-T. Ngo, M. Nagata, and J.-L. Danger, "Pll to the rescue: A novel em fault countermeasure," in *To Appear in Proceedings of the 53rd ACM Design Automation Conference*, Austin, TX, USA, 2016.

[5] D. Binder, E. C. Smith, and A. B. Holman, "Satellite anomalies from galactic cosmic rays," *IEEE Transactions on Nuclear Science*, vol. 22, no. 6, pp. 2675–2680, Dec 1975.

[6] S. P. Buchner, D. Wilson, K. Kang, D. Gill, J. A. Mazer, W. D. Raburn, A. B. Campbell, and A. R. Knudson, "Laser simulation of single event upsets," *IEEE Transactions on Nuclear Science*, vol. 34, no. 6, pp. 1227–1233, Dec 1987.

[7] D. Lewis, V. Pouget, F. Beaudoin, P. Perdu, H. Lapuyade, P. Fouillat, and A. Touboul, "Backside laser testing of ics for set sensitivity evaluation," *IEEE Transactions on Nuclear Science*, vol. 48, no. 6, pp. 2193–2201, Dec 2001.

[8] S. P. Buchner, F. Miller, V. Pouget, and D. P. McMorrow, "Pulsed-laser testing for single-event effects investigations," *IEEE Transactions on Nuclear Science*, vol. 60, no. 3, pp. 1852–1875, June 2013.

[9] M. Saritas and H. D. McKell, "Absorption coefficient of si in the wavelength region between 0.8-1.16 $\mu$m," *Journal of Applied Physics*, vol. 61, p. 4923, 1987.

[10] P. Fouillat, V. Pouget, D. McMorrow, F. Darracq, S. Buchner, and D. LEWIS, *Radiation Effects on Embedded Systems*. Dordrecht: Springer Netherlands, 2007, ch. Fundamentals of the Pulsed Laser Technique for Single-Event Upset Testing, pp. 121–141.

[11] S. Jagannathan, T. D. Loveless, B. L. Bhuva, S. J. Wen, R. Wong, M. Sachdev, D. Rennie, and L. W. Massengill, "Single-event tolerant flip-flop design in 40-nm bulk cmos technology," *IEEE Transactions on Nuclear Science*, vol. 58, no. 6, pp. 3033–3037, Dec 2011.

[12] J. Han, E. Leung, L. Liu, and F. Lombardi, "A fault-tolerant technique using quadded logic and quadded transistors," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 8, pp. 1562–1566, Aug 2015.

[13] P. Schiefer, R. McWilliam, and A. Purvis, "Fault tolerant quadded logic cell structure with built-in adaptive time redundancy," *Procedia* {*CIRP*}, vol. 22, pp. 127 – 131, 2014, proceedings of the 3rd International Conference in Through-life Engineering Services. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2212827114009287

[14] B. Dierickx, "Radiation hard design in CMOS image sensors," Sep 2014, presented at CPIX'14 Workshop, Bonn, Germany.

[15] M. Lacruche, J.-B. Rigaud, J.-M. Dutertre, and E. Kussener, "On the use of forward body biasing to decrease the repeatability of laser-induced faults," in *To Appear in Proceedings of the 19th Conference on Design, Automation and Test in Europe (DATE'16)*, Dressden, Germany, 2016, pp. 1–7.

[16] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault Sensitivity Analysis," in *CHES*, ser. Lecture Notes in Computer Science, vol. 6225. Springer, August 17-20 2010, pp. 320–334, Santa Barbara, CA, USA.

[17] C. Lavin, M. Padilla, P. Lundrigan, B. Nelson, and B. Hutchings, "Rapid prototyping tools for fpga designs: Rapidsmith," in *Field-Programmable Technology (FPT), 2010 International Conference on*. IEEE, 2010, pp. 353–356.

[18] W. He, A. Otero, E. de la Torre, and T. Riesgo, "Customized and automated routing repair toolset towards side-channel analysis resistant dual rail logic," *Microprocessors and Microsystems*, vol. 38, no. 8, pp. 899–910, 2014.

[19] Riscure, "Diode laser station - inspector data sheet," 2011.

[20] Xilinx, "Phase Locked Loop (PLL) Module (v2.00a), DS622; available at http://www.xilinx.com/," June 24 2009.