A Digital Sensor for Detecting Laser Fault Injection

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

Abstract— Laser based fault injection (LFI) is a powerful technique for fault injection in critical circuits. Since LFI creates faults by injecting high energy through photons, it can be detected in advance by a sensitive embedded sensor. In this paper, a low-cost, all-digital sensor system for detecting laser fault injection is presented. Experiments on FPGAs show a 100% detection rate, with significant power and spatial security margin, whilst maintaining extremely low hardware cost.

I. Introduction

Hostile implementation circumstances in security application demand the security-critical circuit be fortified with a strong protection against various attack threats. Fault injection attacks (FIA) are a popular threat which retrieves confidential information by analyzing the faulty behavior of security-critical ICs. The injection methods can be global – power/clock system glitch disturbance, or more fine-grained – laser/EM based fault injection (LFI/EMFI [1]). Among those, LFI is a powerful technique as it is capable of making precise faults. In this work, we develop an all digital LFI sensor.

Sensor based countermeasures can be used to detect the fault injection on-the-fly [2]. It is a plug-in circuit which can be easily combined with a sensitive circuit. The sensor should have a high sensitivity against the disturbance (in this case laser), such that it triggers the logic (`alarm`) signal before the sensitive circuit is violated. More precisely, the injected disturbance should have more significant impact on the sensor, thus triggering the alarm signal. Moreover, the detection coverage of fault types should also be high. In the following, we discuss the design of the proposed LFI sensor.

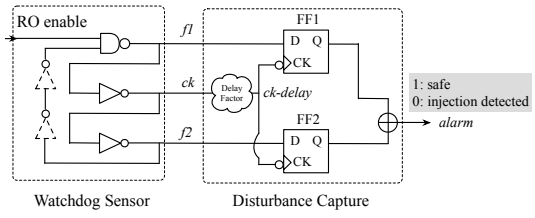


Fig. 1. Topology of the schemed fault injection sensor system.

TABLE I
Area Report of the All-Digital LFI Sensor

Component	LUT	DFF
Watchdog Sensor	3	0
Disturbance Capture	1	2
Delay	1	0

II. A Design of High-Sensitivity LFI Detector

A. Digital LFI Sensor

Fig. 1 shows the presented sensor system which consists of a multi-inverter RO serving as the frequency disturbance `Watchdog Sensor`, and a `Disturbance Capture` logic comprised by two flip-flops and a 1-bit XOR gate. The frequencies from two points on this RO loop are fetched to be sampled by two flip-flops, being clocked by a frequency from another point. The two-bit vector from the two flip-flops manifests whether an abnormality occurred in the RO. The function of the entire detection system is detailed in Fig. 2. The area report is given in Tab. I. The delay can also be configured by appropriate routing only.

The outputs of three consecutive inverters in `Watchdog Sensor` RO are used as the inputs for the `Disturbance Capture` part, named as *f1*, *ck*, *f2* by signal propagation sequence. Given a stable electrical environment, the three signals will have the same frequency with a fixed phase shift, and an opposite polarity to signal *ck*, w.r.t. *f1* and *f2*. FF1 and FF2 are both triggered by the `falling edge` of *ck*, as seen in Fig. 2(a). In absence of a signal delay from RO to flip-flops, the sampled values for FF1 and FF2 are respectively `'1'` and `'0'`, as indicated by the blue dotted arrow lines in Fig. 2(a). **Noticeably**, the ripples in this RO will identically affect three frequencies, which cannot incur sampling changes in the two flip-flops.

In order to generate abnormal samplings, a `delay factor` is intentionally inserted into the clock inputs of FF1 and FF2, which is used for introducing a propagation delay of *ck* signal by several clock cycles. In a sequel, each flip-flop is actually clocked by the falling-edge of an earlier *ck* cycle, as highlighted by the red dotted arrow lines in Fig. 2(a). The significant merit here is that the

ripple in RO only affects the *f1* and *f2* at the injection moment, without immediately affecting the sampling frequency (*ck-delay*) on `Disturbance Capture`. In this way, this system is able to capture bidirectional abnormalities in RO frequency ripples.

B. Timing Violation

Delayed Propagation: In case the signal propagation is delayed by the LFI, the frequency of RO can be reduced shortly, as indicated by Fig. 2(b). In this situation, the duty cycle of *f1* and *f2* are temporarily extended. As discussed before, both FF1 and FF2 are clocked by the delayed clock signal *ck-delay*, hence the sampling time in flip-flops at the injection moment is not impacted by the RO disturbance, which is very likely to result in the set-up time violation at *f2*. As seen in Fig. 2(a), the sampled value vector from FF1 and FF2 is `'10'`. Hence, the sampled vector in presence of timing violation from delayed signal propagation is `'11'`, as highlighted in Fig. 2(b).

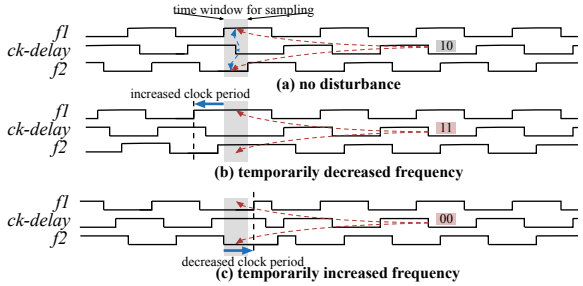
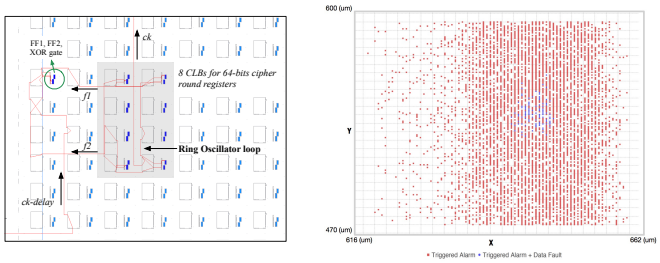


Fig. 2. Timing violation under low/high-frequency ripple.

Accelerated Propagation: As aforementioned, the frequency can also be transiently increased by LFI. In this way, the duty cycles of both *f1* and *f2* can be reduced when the injection affects the RO. Comparatively, the timing will be violated in FF1, rather than FF2, *cf.* preceding situation. As explained in Fig. 2(c), the sampled value vector from FF1 and FF2 becomes `'11'` from the normal `'10'`.

III. Experimental Evaluation

To evaluate the detection capability of this system against LFI, a Xilinx 65*nm* Virtex-5 FPGA (VLX50T) was used as the target. The basic architecture includes a massive Configurable Logic Block (CLB) array for implementing the main logic. The *ISO/IEC* standardized `PRESENT-80` block cipher [3] is selected as the protection target, and the watchdog RO is implemented as a circuit to encompass the 64-bit `round registers`, as seen in Fig. 3(a). A region surface scan to a single CLB where 4-bit round registers are deployed, is conduced relying on a controllable 2D stepper stage where the FPGA is fixed on. The magnification of objective lens is 5×, and the scan matrix is 150 × 150 with laser pulse length ranging from 200*ns* to 300*ns*. Fig. 3(b) shows the plot of the scan result, where the blue spots represent the injected cipher faults that triggered the alarm, and red spots denote the triggered alarm without cipher faults. Tab. II summarizes the experimental results, where the `Detection Rate` is used to quantify the quality of countermeasure against LFI. As seen, all the incurred cipher faults (99) have been successfully detected, which shows 100% detection rate. Moreover, the alarm is triggered from a much bigger number of injection (4461) without injected cipher faults. This means that the on-going injection campaign can be sensed in advance, which offers significant spatial margin to alert the system to respond to the LFI threats. The lowest laser power to induce the cipher faults is 63% of its full strength, and the lowest power to trigger the alarm is 42%, which certifies that the sensor is more sensitive to the LFI, i.e., the power security margin is 19%.



(a) (b)

Fig. 3. (a) FPGA implementation of the proposed sensor and the protected 64-bit round data registers of PRESENT; (b) Laser fault injection scan to a single CLB inside watchdog RO loop.

TABLE II
LFI scan result to single CLB with 4-bit cipher registers

	Only Alarm Case_(1)	Fault+Alarm Case_(2)	Only Fault Case_(3)	Scan Points	RO freq. (MHz)
No.	4461	99	0	22,500	163
min.Power	42%	63%	*n/a*		
Detection	Successful		Failed		
Detection Rate	$\frac{Case\_(2)}{Case\_(2)+Case\_(3)} = 100\%$				

IV. Concluding Remark

In this paper, a sensor system for detecting a malicious laser fault injection into integrated circuit is described. Experimental evaluation on a Virtex-5 FPGA proves its high sensitivity against malicious laser fault injection. Owing to its pure digital and simple architecture, this system can be easily transplanted into any security-critical ICs, particularly for applications with restricted power and hardware resources.

References

[1] A. Barenghi et al. , "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, pp. 3056–3076.

[2] N. Miura et al. ,"Pll to the rescue: A novel em fault countermeasure," in *Proceedings of the 53rd ACM Design Automation Conference*, 2016.

[3] A. Bogdanov et al. , "Present: An ultra-lightweight block cipher," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2007, pp. 450–466.