Extended Abstracts of the 2019 International Conference on Solid State Devices and Materials, Nagoya, 2019, pp501-502

An Information Leakage Sensor Based on Measurement of Laser-Induced Opto-Electric Bulk Current Density

Kohei Matsuda[1], Sho Tada[1], Makoto Nagata[1], Yang Li[2], Takeshi Sugawara[2], Mitsugu Iwamoto[2], Kazuo Ohta[2], Kazuo Sakiyama[2], and Noriyuki Miura[1]

[1] Kobe University
1-1, Rokkodai-cho, Nada-ku, Kobe, Hyogo 657-8501, Japan
Phone: +81-78-803-6221 E-mail: k_matsuda@cs26.scitec.kobe-u.ac.jp
[2] The University of Electro-Communications
1-5-1, Chofugaoka, Chofu, Tokyo 182-8585, Japan

Abstract

This paper presents an information leakage sensor against a Laser Fault Injection (LFI) attack as one of the most powerful physical security threats on cryptographic processors. Distributed sensors built in a cryptographic processor measure laser-induced opto-electric bulk current density. A time-interleaved operation of the distributed sensors array together with the sensor sensitivity tuning provides information on position and strength of the injected laser beam. A partial bit information at a risk of secret disclosure can be thus detected. Test chip measurement in 0.18μm CMOS successfully demonstrated the proposed sensor operation.

1. Introduction

In the era of Internet-of-Things (IoT), information security is critical. A well-known serious security threat is a physical attack on a cryptographic processor. Especially, a Laser Fault Injection (LFI) attack is one of the most powerful physical attack [1-2] where a secret key can be disclosed by analyzing fault operation induced by the laser irradiation (Fig. 1(a)). This fault operation is originally caused by a bit flip in intermediate data register FFs (Fig. 1(b)) due to opto-electric current discharge generated at a PN junction of CMOS device (Fig. 1(c)), similar as a soft error mechanism in SRAM. A reactive sensor approach has been proposed as a circuit-level countermeasure against the LFI attack [3]. However, the original sensor only detects whether the cryptographic processor is under the attack or not. The possible reaction is just disabling the cryptographic operation to protect the key, which significantly degrades its availability in the practical IoT services. This paper presents a modified sensor detecting a partial bit information at a risk of disclosure, namely information leakage sensor. By utilizing this high-resolution physical information in an advanced cryptographic algorithm [4], a high-availability resilient security module can be realized.

2. Information Leakage Sensor

Figure 2 depicts the proposed information leakage sensor. The core circuit is based on a legacy Bulk Built-in Current Sensor (BBICS) applied to soft error detection [5]. In our modified sensor, enabling switches are newly added in the sensor front-end for a time-interleaving operation (Fig. 3) to measure a laser induced spot. In the sensor back-end, sensitivity control by tail bias V_{SN} and V_{SP} is incorporated for measuring the laser-induced opto-electric current density, and hence injected laser source energy to turn *Alarm* signal ON.

3. Experimental Setup

A test chip was designed and fabricated in 0.18μm CMOS (Fig. 4). An AES cryptographic processor was integrated with the proposed information leakage sensor with 56x5 front-ends and 56 back-ends to cover the entire processor core. For bypassing a metal shield on top of the core, the laser was injected through the cavity formed backside of the test board. To inject light energy through the Si substrate, IR laser was employed and IR LED was used for transmissive image capturing for laser injection targeting (Fig. 5).

4. Measurement Results

For preliminary characterization of the opto-electric device reaction, a laser energy for bit flip in a 0.18μm CMOS FF was measured [6]. This bit flip produces a fault cipher code for the LFI attack (Fig. 6). Figure 7 presents measured distribution of the laser source energy turning ON *Alarm*. The time-interleaved sensor operation with sensitivity control successfully provided information of partial bits at the leakage risk.

Acknowledgements

This work is supported by JSPS Grants-in-Aid for Scientific Research under Grant 18H05289. The authors are grateful to IPA for the laser test setup and technical assistance.

References

[1] S. P. Skorobogatov, and R. J. Anderson, “Optical Fault Induction At tacks,” *CHES*, vol. 2523, pp. 2-12, Aug. 2002.
[2] K. Sakiyama, *et al.*, "Information-Theoretic Approach to Optimal Differential Fault Analysis," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 1, pp. 109-120, Feb. 2012.
[3] K. Matsuda, *et al.*, “A 286F^2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack on Cryptographic Processor,” *IEEE JSSC*, vol. 53, no. 11, pp. 3174-3182, Nov. 2018.
[4] S. Micali and L. Reyzin, “Physically Observable Cryptography,” *TCC*, vol. 2951, pp. 278-296, Jan. 2004.
[5] E. H. Neto, *et al.*, “Using Bulk Built-in Current Sensors to Detect Soft Errors” *IEEE Micro*, vol. 26, no. 4, pp. 10-18, Sep. 2006.
[6] K. Matsuda, *et al*., "On-Chip Substrate-Bounce Monitoring for Laser-Fault Countermeasure," *AsianHOST*, pp. 1-6, Dec. 2016.

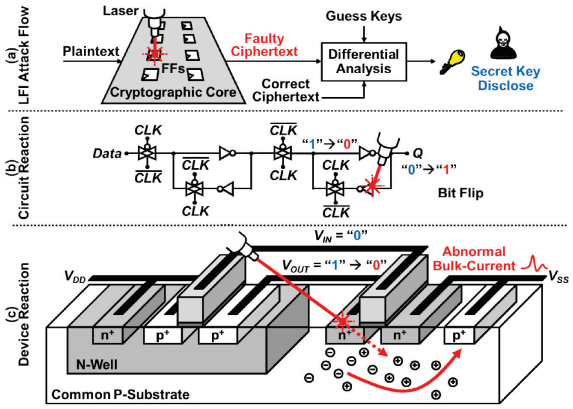

Fig. 1 Conceptual sketch of (a) Laser Fault Injection (LFI) attack flow, (b) circuit, and (c) device reaction against LFI.

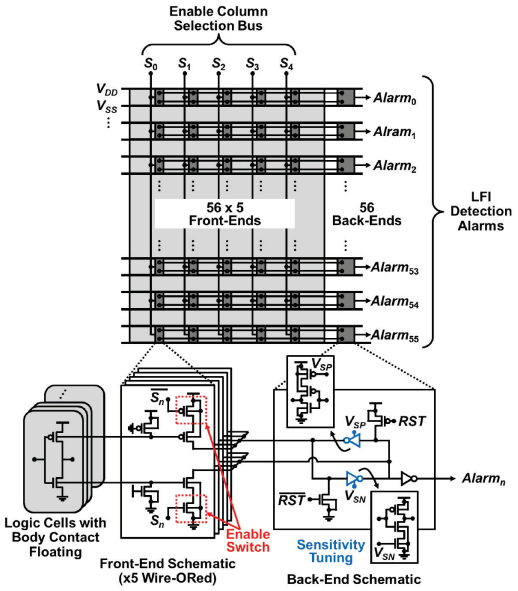

Fig. 2 Block and circuit schematic of information leakage sensor.

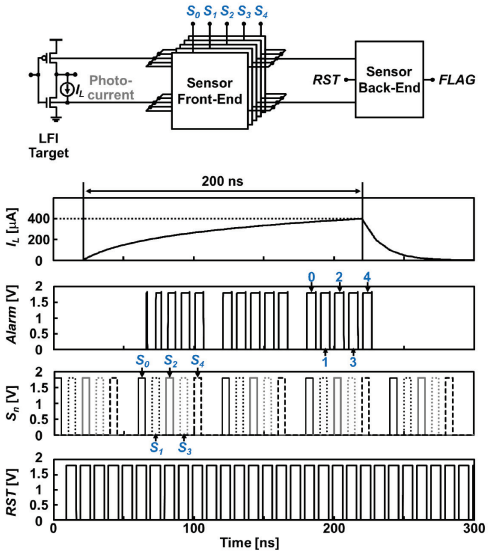

Fig. 3 Simulated waveforms of sensor operation.

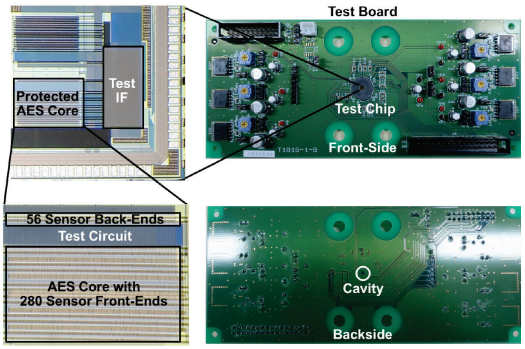

Fig. 4 Test chip die photo and test board setup.

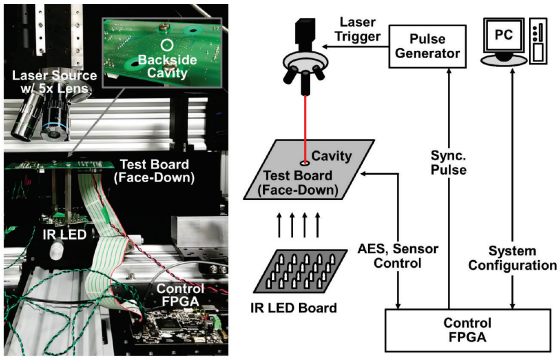

Fig. 5 LFI test system setup.

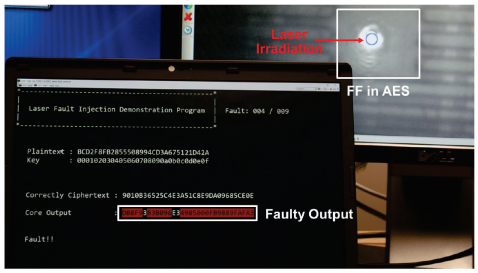

Fig. 6 Measured faulty AES operation.

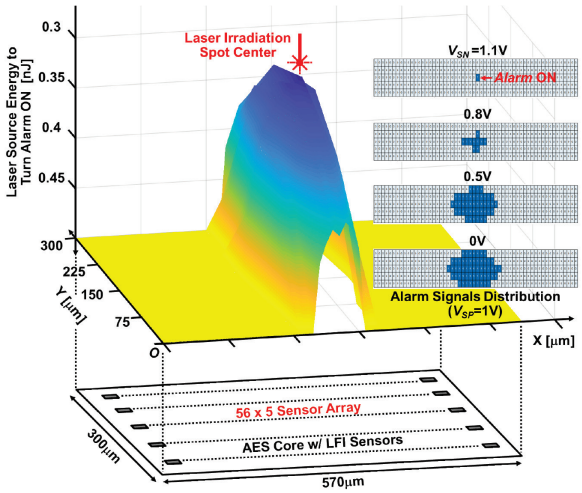

Fig. 7 Measured distribution of required laser source energy to turn Alarm signal ON and Alarm signals distributions depending on sensor sensitivity.