Extended Abstracts of the 2020 International Conference on Solid State Devices and Materials, VIRTUAL conference, 2020, pp791-792

An Inductive Impulse Self-Destructor in Sense-and-React Countermeasure Against Physical Attacks

Sho Tada[1], Yuki Yamashita[1], Kohei Matsuda[1], Makoto Nagata[1], Kazuo Sakiyama[2] and Noriyuki Miura[3]

[1] Kobe University, [2] The University of Electro-Communications, [3] Osaka University, Japan

Abstract

This paper presents an inductive impulse self-destructor for a sense-and-react countermeasure against physical attacks on a cryptographic processor. Upon attack detection, the destructor generates >10V impulse and permanently destructs the processor to avoid repetitive attack. A fully standard CMOS compatible, compact circuit solution with only single inductor and transistor significantly saves fabrication cost. A prototype implemented in both discrete components and 0.18μm CMOS successfully demonstrated the-proof-of-concept.

1. Introduction

Physical attacks on a cryptographic processor are realistic security threats today. An attacker exploits recent technology advancement in computation and instrumentation to develop powerful yet low-cost attack schemes, such as a micro-EM probing [1], a direct probing [2], and a laser fault injection attack [3] for secret key disclosure (Fig. 1).

Various IC-level countermeasures were presented to tackle these attacks. A logic-level countermeasure can enhance the resiliency however the hardware overhead is huge [4]. One solution is a sense-and-react countermeasure (Fig. 1). An integrated attack sensor detects the attacks and then reacts for protection [5, 6]. One typical counter reaction is system halt. A flush code eraser [6] shuts the core supply down immediately after the detection and erases both internal data and key (Fig. 1(a)). The area penalty of this sense-and react countermeasure was only +28% of the unprotected core.

This paper proposes a compact and low-cost self-destruction circuit as an alternative counter reaction (Fig. 1(b)). This, namely impulse self-destructor, instantaneously generates high-voltage impulse to destruct the cryptographic processor. The state of the processor turns into permanent halt brutally after the first attack detection to disable repetitive attacks. Unlike technology-dependent schemes [7, 8], a complete circuit solution fully compatible with standard CMOS is proposed. No additional process steps are needed and hence this work is free from the fabrication cost penalty.

2. Circuit Design

In CMOS, transistor gate breakdown is one most typical defect mechanism. By utilizing this phenomenon, the processor can be destructed. The breakdown voltage of 0.18μm CMOS transistor is ~10V. To generate such high voltage far beyond the supply V_{DD} (=1.8V), a boost converter circuit could be a primary option (Fig. 2(a)). Our impulse self-destructor is modified specifically for the instantaneous self-destruction (Fig. 2(b)). Since the boost voltage is not needed to be DC stable, an area-consuming rectification unit is removed for ~3x area saving. The destructor mainly consists of only a single inductor and transistor (a pulse generator consists of only few small logic gates). Triggered at *Alarm* signal assertion, the pulse generator produces an impulse *Pls* to temporary turns ON the transistor. A large short current I_M is drawn from V_{DD} through the inductor L. A large magnetic-field energy $E_M=LI_M^2/2$ is thus accumulated. By *Pls* negation, the large E_M energy rushes into the target processor (data/key registers) and inertially generates the >10V high-voltage V_{BST}. It quickly reaches the breakdown voltage within few ns which is ~1000x faster than the conventional boost converter. The proposed destructor was first prototyped by discrete components for the-proof-of-concept. Fig. 3 depicts its test setup and the operation waveform snapshot. The boost impulse V_{BST} successfully reaches >13V within 3ns. This compact prototype of ~5mm x 8mm can be used as a package- and board-level countermeasure against the physical attacks.

3. IC Implementation

Co-integration of the destructor into the processor IC enhances its security level. The in-situ operation with the sensor reduces the reaction latency for instantaneous self-destruction. It also reinforces the difficulty of the attack on the destructor itself. In this paper, the self-destructor was co-designed with 128bit AES processor in 0.18μm logic CMOS (Fig. 4). The processor macro was designed by using a standard EDA toolchain. The processor layout was drawn without using the top metal (M6 here) to save metal resources for the inductor. The layout footprint of the AES macro was ~480μm x 480μm. The on-chip inductor is drawn over the macro. Although the inductor footprint is as large as the macro size, no area penalty is burdened with this complete overlap scheme. This top-metal inductor also acts as a metal shield against a front-side laser attack (back-side attack is detected by [6]). For electrical characterization of the inductor, an EM-field solver was used to derive an equivalent circuit [9], which is imported and combined with the transistor circuits in a post-layout circuit simulator to evaluate the overall operation. The physical dimensions of the inductor are adjusted through the two-step simulations in the field solver and the circuit simulator through few-times iteration.

Fig. 5 depicts the final evaluation setup in the post-layout simulation. V_{BST} is applied to the reset pins *Resetb* of 128bit key registers in AES for permanent halt. The intermediate key values are also immediately erased. The load capacitance is equivalent to ~1.3pF for the destructor. The design parameters were optimized under the nominal V_{DD} of 1.8V. The inductor was designed to be 9 turns and 20μm line width and the equivalent circuit is derived as in Fig. 5. The line space should be the minimum allowed in the process rule for

the metal shield coverage. The parasitic capacitance has no impact on V_{BST} because of the large loading. The switch transistor was design as 512µm channel width to draw the peak current of 250mA. The accumulated magnetic energy E_M in the inductor is ~0.4nJ. This large energy is inertially supplied to the key register by the sudden transistor switching OFF. The waveform in Fig. 5 successfully demonstrated 14V-peak impulse. The co-integration further reduces the reaction latency by 10x. The single transistor circuit occupies only <1400µm^2 area including the buffer and periphery (Fig. 4). The area overhead is only +0.6% of unprotected AES. This destructor circuit is placed under the inductor for self-protection (Fig. 4). Fig. 6 shows the die photo. Compared to the flush code eraser [6], the destructor occupies 1/4 smaller area. Also tamper resiliency is higher in 4 standard metrics [10] (Table I). The tamper resistance is high due to its self-protection property against the attack on the countermeasure itself. The tamper evidence is equipped with permanent halting nature. These advantages make the destructor to be suitable for the high-level security requirement.

Acknowledgements

This work is supported by JSPS Grants-in-Aid for Scientific Research under Grant 18H05289.

References

[1] T. Sugawara, *et al*., "On Measurable Side-Channel Leaks Inside ASIC Design Primitives," *CHES*, vol. 8086, pp. 159-178, Sep. 2013.

[2] R. Schlangen, *et al*., "Functional IC Analysis Through Chip Backside with Nano Scale Resolution - E-Beam Probing in FIB Trenches to STI Level," *IPFA*, pp. 35-38, July, 2007.

[3] S. P. Skorobogatov and R. J. Anderson, "Optical Fault Induction Attacks," *CHES*, vol. 2523, pp. 2-12, Aug. 2002.

[4] M. Doulcier-Verdier, *et al*., "A Side-Channel and Fault-Attack Resistant AES Circuit Working on Duplicated Complemented Values," *ISSCC*, pp. 274-275, Feb. 2011.

[5] N. Miura, *et al*., "A Local EM-Analysis Attack Resistant Cryptographic Engine with Fully-Digital Oscillator-Based Tamper-Access Sensor," *VLSI*, pp. 172-173, June 2014.

[6] K. 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," *JSSC*, Vol. 53, No. 11, pp. 3174-3182, Sep. 2018.

[7] S. Borel, *et al*., "A Novel Structure for Backside Protection against Physical Attack on Secure Chips or SiP," *ECTC*, pp. 515-520, May 2018.

[8] A. R. Desai, *et al*., "Anti-Counterfeit Integrated Circuits Using Fuse and Tamper-Resistant Time-stamp Circuitry," *HST*, pp. 480-485, Nov. 2013.

[9] N. Miura, *et al*., "Analysis and Design of Inductive Coupling and Transceiver Circuit for Inductive Inter-Chip Wireless Superconnect," *JSSC*, vol. 40, no.4, pp. 829-837, Apr. 2005.

[10] S. H. Weingart, "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses," *CHES*, vol. 1965, pp. 302-317, Jan. 2002.

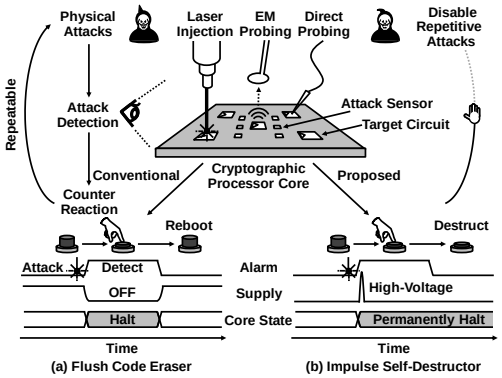

Fig. 1 Operation concept of sense-and-react countermeasure with (a) conventional flush code eraser and (b) proposed impulse self-destructor.

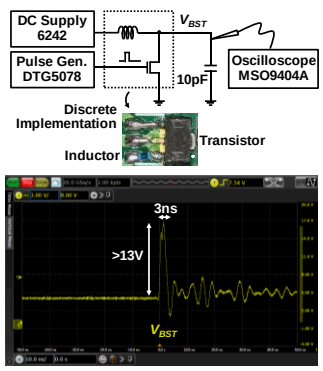

Fig. 3 Prototype setup and waveform snapshot of boost voltage V_{BST} in discrete destructor prototype.

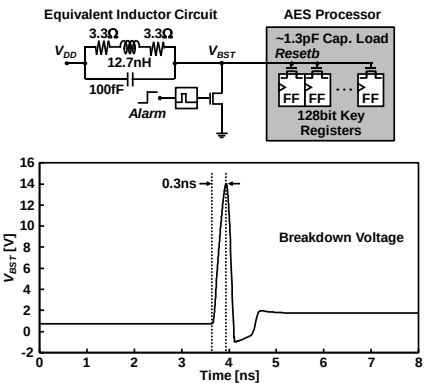

Fig. 5 Simulated circuit and its waveform of self-destructor with AES processor.

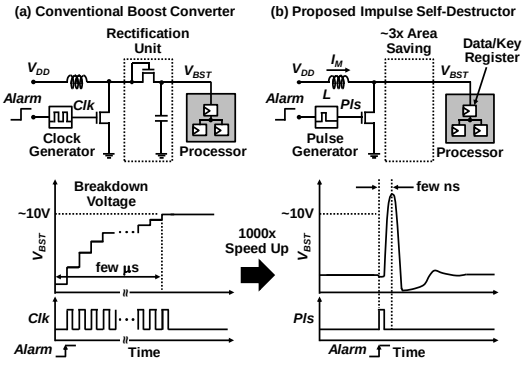

Fig. 2 Circuit schematics and operating waveforms of (a) conventional boost converter and (b) proposed impulse self-destructor.

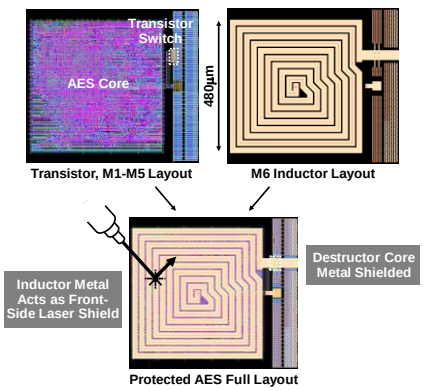

Fig. 4 Physical layout view and die photo of protected AES processor with self-destructor.

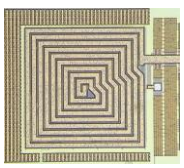

Fig. 6 Die photo of test chip.

TABLE I
TAMPER RESILIENCY COMPARISON

	Flush Code Eraser (Conventional)	Impulse Self-Destructor (Proposed)
Tamper Resistance	-	+
Tamper Evidence	-	+
Tamper Detection	+	+
Tamper Response	+	+