On-Chip Physical Attack Protection Circuits for Hardware Security

Invited Paper

Makoto Nagata*, Takuji Miki* and Noriyuki Miura
*Graduate School of Science, Technology and Innovation, Graduate School of System Informatics
Kobe University
1-1 Rokkodai, Nada, Kobe 657-8501, Japan
nagata@cs.kobe-u.ac.jp

***Abstract*—Hardware security, application of modern digital cryptography and authentication technologies for protecting information in electronics, involves analog functionality to avoid physical threats in operation fields. This paper introduces semiconductor integrated circuits designed for on-chip detection and disablement of malicious attempts on cryptographic devices through side-channel and fault attacks. The protection against local electromagnetic attack (LEMA) and laser fault injection attack (LFIA) are demonstrated with Silicon measurements.**

Keywords—Side-channel attack. Fault attack, Electromagnetic emanations, Laser fault injection, Cryptographic processor

I. Introduction

Proliferation of cryptographic devices emerges among internet-of-things (IoT) applications [1]. Symmetric ciphers are chosen for encryption/decryption of data and control code protection in the communication between small scale nodes and centralized servers. Public-key ciphers realize the higher order security functionality like message authentication with digital signature [2]. Continuous efforts have been devoted to implement ciphers in semiconductor integrated circuit (IC) chips with low-power and small footprint features [3], [4] or even in field programmable gate array (FPGA) devices [5], [6]. The adoption of cipher algorithms will be extended among general electronics toward the security and safety of autonomous driving vehicles, machine learning facilities, medical and healthcare devices, and many other applications.

However, there have also been a variety of attempts to derive secret information of "key" from cryptographic devices during their actual operation in fields. The attempts explore transistor-level vulnerabilities of a cryptographic device actualizing cipher algorithm, and are therefore classified as a physical attack or an implementation attack. Passive attacks observe side-channel information leakage, as in a side-channel attack (SCA) [7], [8], [9] while active attacks analyze the difference between erroneous outputs after an intentional fault injection with originally correct outputs, as in a fault attack (FA) [10], [11], [12]. As one of the most efficient active attacks, the fault sensitivity attack (FSA) directly relates the minimum power of intentional fault injection with secret information [13], [14]. Emerging threats of Hardware Trojans need to be considered in the design of modern electronics systems [15], [16].

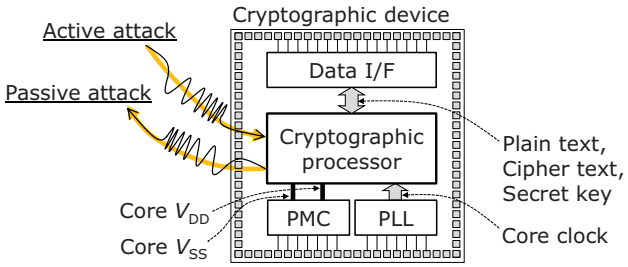


Figure 1: IC chip with cryptographic processor.

Operation environment of ICs in a packaged chip can be in-place evaluated by on-chip power supply and signal waveform monitoring techniques [17], [18]. On-chip power noise measurements have promoted the design and analysis of very large scale IC chips for power integrity, signal integrity and electromagnetic compatibility [19].

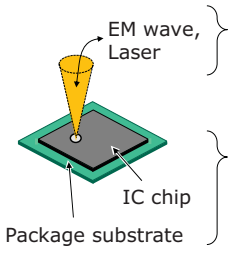
This paper discusses the evolvement of on-chip monitoring capability of an IC chip toward physical attack protection. Sections II and III classify physical attacks and associated on-chip characterizations, respectively. Section IV demonstrates on-chip protection circuits and examples. Section V summarizes the paper.

II. Physical Attacks

An IC chip as a cryptographic device generally includes a cryptographic processor in its part of digital system, as shown in Fig. 1. Plain and cypher texts are communicated through digital interface (I/F) with other processing elements. Power supply (V_{DD}) and ground (V_{SS}) are provided by power management circuits (PMC) involving dc-dc converters and reference voltage generators. Also, a phase-locked loop (PLL) regulates the core operating frequency. From an ideal viewpoint, the crypto processor is therefore isolated from the off chip in signaling as well as powering [20], [21], [22], [23]. However, physical attacks still potentially jeopardize hardware level security by breaking isolation walls [24], [25], [26].

The power current at the core V_{DD} varies with the progress of processing steps according to a cipher algorithm. An external observer has a chance to deduce secret key bytes from power

* 978-1-5386-9395-7/19/$31.00 ©2019 IEEE



Physical media

Passive attacks	Side channel attack (SCA)	EM, Photon, Volt., Current
Active attacks	Fault attack (FA)	EM, Laser, ESD, Glitch

Assembly structure

ASIC	Wire bonding, Flip chip	Plastic mold, CoB, etc.
FPGA	3D stacking, Fan out	Si interposer, MCM, etc.

Figure 2: IC chip under attacks.

current waveforms, as is known as side-channel information leakage. The waveforms on the core V_{DD} can be captured by measuring electromagnetic (EM) emanations with micro antennas closely positioned to an IC chip [27], even if the power current is separated by PMC from a power source assembled off-chip on PCB.

The crypto processor produces erroneous output bits once an observer intentionally injects faults to flip internal values of memory macros or register files, likewise soft errors spontaneously induced by cosmic rays. The observer can assume that the specific fault bit is processed by a cipher algorithm as in a normal way and then reduce the search space of secret key bytes. The EM irradiation can be straightforwardly focused on the area of storage nodes within the die. This is more efficient than other intentional disturbances like voltage surges and clock glitches, which can be prevented by the PMC and PLL, respectively.

Physical attacks are classified in Fig. 2 with associated physical medias and packaging options. An attacker has the choice of tool suites for either optics or microwaves. The former is advantageous in localizing attacks in space and time with the resolution of 1 μm and 10 ns, respectively, while needing decapsulation. The latter is more flexible in selecting locations, angles as well as frequencies of interest, while spread over 100 μm or more in space. The attack efficiencies are also dependent on the orientation of IC chips in either face up or flip chip assembly, with the difference of access distance or penetration to the transistors as the source of vulnerability. The challenge of attacks has been reported not only on custom IC chips while also on cryptographic functionality on FPGA devices.

III. On-Chip Characterization

A. Side-Channel Information Leakage

An on-chip waveform monitor (OCM) of Fig. 3 realizes in-place characterization of side-channel information leakage [17]. The voltage variation is measured at the probe points of interest, on the core V_{DD}, core V_{SS} and even Silicon substrate. The OCM can only provide in-place measurement capability on those on-chip voltage domains, which are expected to be isolated from on-board ones, even with frequency dependency due to parasitic impedances on power delivery networks.

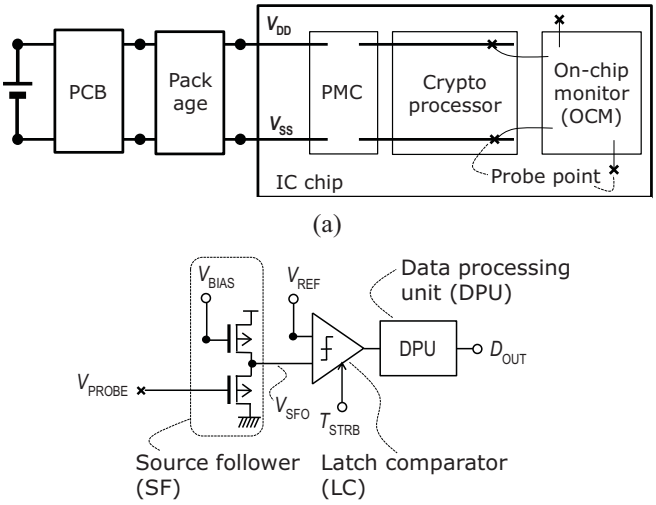


Figure 3: (a) Inclusion of OCM and (b) detailed structure.

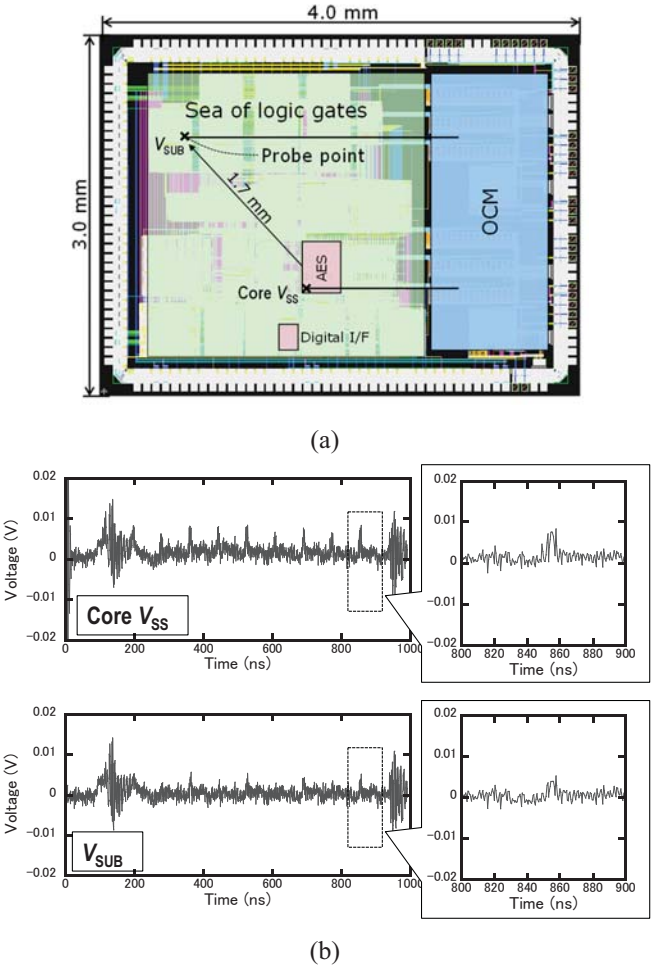


Figure 4: (a) AES test chip and (b) captured waveforms.

The probed voltage, V_{PROBE}, is sensed by a source follower (SF) at the input of OCM (Fig. 3(b)). The voltage at the output of SF (V_{SFO}) is compared to the stepped reference voltage (V_{REF}) by a latch comparator (LC) at its strobe timing (T_{STRB}). The most proximate voltage of V_{SFO} at T_{STRB} is determined and output as the digital code of V_{REF}. The code is determined one after another for successive strobe timings through iterative operation of the whole IC chip. The resolutions of voltage (ΔV_{REF}) and timing (ΔT_{STRB}) are typically set at 100 μV and 100 ps, respectively.

A cryptographic device of Fig. 4 is equipped with an Advanced Encryption Standard (AES) processor and a full-function multi-channel OCM macro [28]. The on-chip captured voltage waveforms at the node of AES core V_{SS} and on the p-type substrate node V_{SUB} are also given. It is observed that there is a regular peak at every 100 ns, equivalent to the period of operating frequency at 10 MHz. The waveforms exhibit the similarity among those two probing points, while V_{SUB} is slightly attenuated due to the distance of 1.7 mm away from the AES core. The core V_{SS} is resistively connected to a p-type Si substrate in each logic cell as is often the case with a standard CMOS technology.

The SCA analysis on the on-chip captured V_{SUB} waveforms was based on a correlated power analysis (CPA) technique and provided that the set of V_{SUB} waveforms collected for 1,000 different plain texts (with the same secret key) was sufficient to determine at least a single key byte of a 128-bit secret key for this particular design. Another waveform set for more than 4,000 plain texts revealed 14 bytes.

The characterization of side-channel information leakage by OCM implies that the waveforms at any locations within a sea of logic gates in system-level integration could be attacked, even from the backside of an IC chip in flip-chip packaging. In the other way, the OCM measurements could check the potentiality of side-channel information leakage by analyzing the waveforms in the background of cryptographic processing.

B. *Fault Injection*

On-chip characterization using the OCM is applied when a laser is irradiated to transistors in ICs under operation, as depicted in Fig. 5 [29]. When the laser is irradiated pin-point at the junction node of a transistor, electron-hole pairs are induced due to the energy translation with photons. Since the transistor is biased by power supply and ground voltages given to ICs, the electrons and holes are immediately separated to the respective electrodes. This creates the flow of substrate current and associated voltage bounce nearby the location of irradiation.

The near infrared (NIR) laser module is synchronized to OCM macro and also to 16-bit shift register (SR) circuits on a device under test (DUT). The OCM captures V_{SUB} waveforms during and after the irradiation of NIR laser, with the laser power large enough to induce a single-bit failure. The in-place measured waveform is given in Fig. 6(a), where the maximum voltage increase of 180 mV is found when the LSB of SR flips (0xF0FF) from the originally stored value (0xF0FE). The dependency of substrate voltage variation (ΔV_{SUB}) on the distance along the SR from the point of laser irradiation is

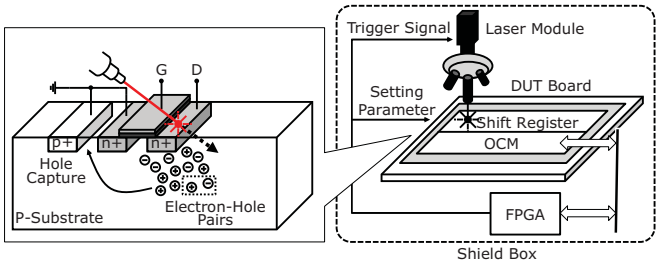


Figure 5: Laser fault injection principle and setup.

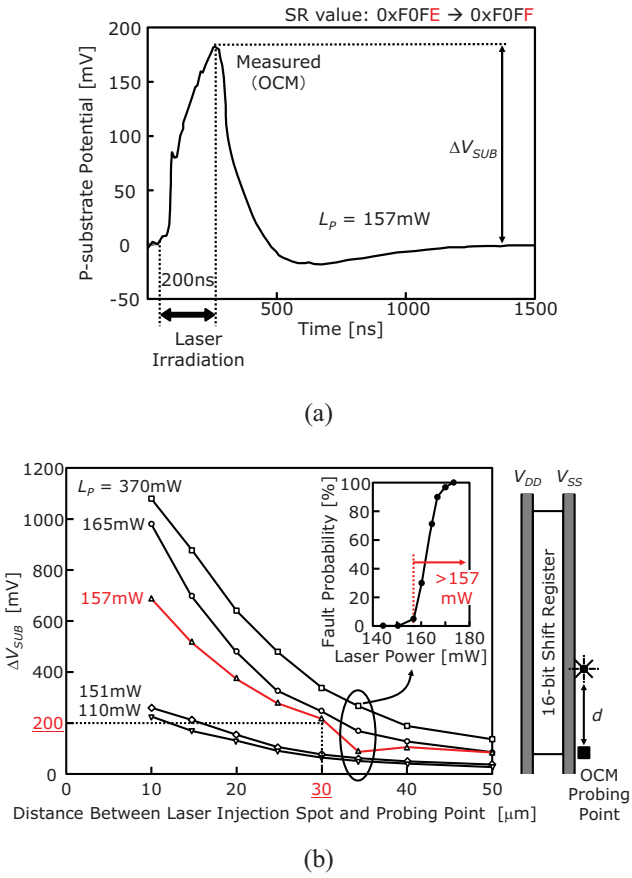


Figure 6: (a) Measured V_{SUB} waveforms after laser irradiation. (b) Measured V_{SUB} versus distance.

characterized for different laser powers as in Fig. 6(b), using the OCM with multiple probing points. It is seen from the chart that the faulty bits are seen with the laser power higher than 157 mW, which is sensed as the ΔV_{SUB} of larger than 200 mV at the distance of 30 μm.

The characterization of fault injection by OCM implies that the IC chip can recognize the attack by measuring voltage bounce inside or surrounding positions to a cryptographic processor.

IV. On-Chip Attack Prevention

A. Side-Channel Attack

Attackers may use a miniaturized micro antenna (μEM probe) to search the location of the highest level of side-channel leakage from a cryptographic processor over an IC chip, in the local electromagnetic side-channel attack (LEMA) [27]. The dynamic movement or even static placement of an antenna creates the change in the electromagnetic field nearby an IC chip. This invisible reaction is inevitable in accordance with a physical law, even though the LEMA search itself is considered physically nonintrusive to an IC chip. An on-chip inductor (sensor coil) of Fig. 7 can detect the advent of adversary through magnetic coupling to its antenna (μEM probe), with the higher sensitivity for the more proximate positioning. As the prevention mechanism against LEMA, the cryptographic processor will be immediately halted or even changed into a dummy state, once the attack is detected.

An actual embodiment of LEMA sensor is given in Fig. 8 [30], where two inductors (coils) with different shapes (e.g. the number of turns) to each other overlay the respective part of a cryptographic core. Each inductor belongs to an LC oscillator. The dual LC oscillators provide the sensitivity to the micro antenna with different coupling coefficients. The sensor is calibrated beforehand by matching the pair of LC oscillators about its self-oscillating frequency. Another pair of inverter-based ring oscillator regulates the frequency to compensate for process-voltage-temperature (PVT) variation.

The test chip fabricated in a 0.18 μm standard CMOS technology used the 5th and 6th layers of metal to form the coils. The cost of LEMA sensors was measured to be 2% increase of Si area [31].

Once the frequency is regulated, the change in oscillation frequencies among the pair of LC oscillators detects the approach of a μEM probe , as demonstrate in Fig. 9. It is noticed that this dual coil scheme precludes attacks using multiple antennas or even stealthy antennas at stationary positions.

B. Fault Attack

Once an IC chip is decapsulated, one of the most powerful attacks uses the laser injection, as addressed in Sec. III. On-chip detection contributes to a prevention measure, since the voltage variation by the laser irradiation is induced on Si substrate and spread concentrically from the point of laser irradiation. The area of spread is governed by the resistivity of a Si substrate, however, it is detectable by the OCM without difficulty even at 30 μm apart from the spot in the given technology, as was shown in Fig. 6. The voltage amplitude of 200 mV can be the threshold for the sensor to judge the occurrence of laser fault injection attack (LFIA).

The idea of distributed voltage sensors in the area of cryptographic processor is introduced in Fig. 10. The sensor is tiled and located at every 60 μm among the regularly placed and routed standard logic cells. When an attacker irradiates laser anywhere in the sea of logic cells, the sensor detects it and forces the cryptographic functionality to be halted or transitioned into a dummy state, once the voltage variation reaches the threshold.

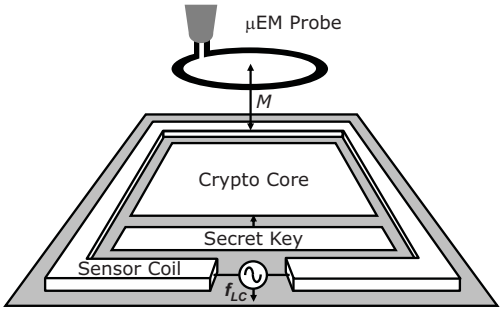


Figure 7: Local EM attack (LEMA) sensing principle.

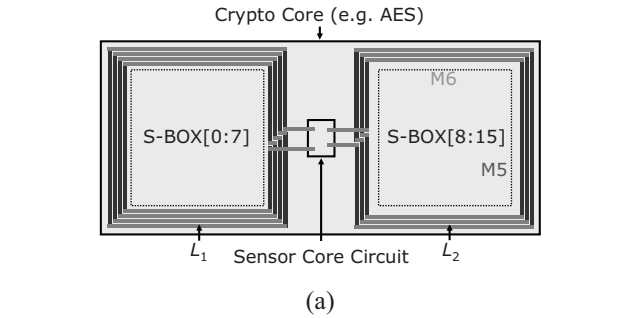


Figure 8: (a) Dual coil architecture of LEMA sensor and (b) detailed circuits.

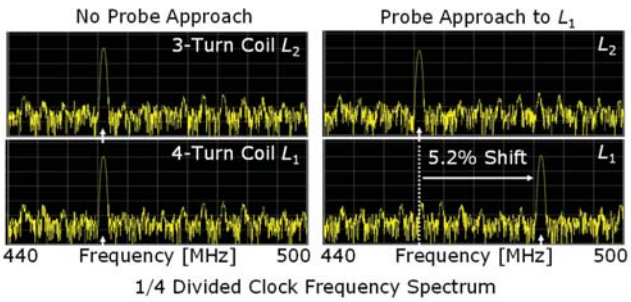


Figure 9: Measured results of sensing LEMA.

This sensory operation is valid also for laser irradiation from the backside of Si.

The miniature design of sensor circuits is achieved as in Fig. 11 [32]. The current I is induced by the laser irradiation when it hits the biased drain junctions of logic cells, and flows into the local resistor R of the sensor circuit. The R is formed by either M_{N1} or M_{P1} transistor kept in its on state, for the branch of core V_{DD} or core V_{SS}, respectively. The local voltage of IR is then amplified by a common-source (CS) amplifier transistor, by either M_{N2} or M_{P2} transistor biased in saturation. The fundamental mechanism of sensing is referred to the soft error sensing scheme [33]. The output of CS transistor is in a current mode and thus connected to a common wire shared by some sensors (wired OR.) Once some sensor circuits detect the laser induced current, the latch in the sensor backend flips in its logical state and digitally informs the cryptographic processor.

The size of sensing frontend is only 286F^2 /cell (almost same as 2.6 equivalent gates of 2-input NAND) after physical layout. A 128-bit AES core with 336 distributed sensing frontends, followed by 15 backend latch circuits, has been designed and fabricated in a 0.18 μm standard CMOS technology. The AES core also includes the post-detection function of secure flush code eraser [32] to prevent from information leakage due to LFIA. The intermediate data during AES processing are promptly erased with power gates and shunt switches. The cost of LFIA sensor and post-detection code eraser circuits was 28% increase in Si area.

The measurement results of the test chip are summarized in Fig. 12. The vertical axis is calibrated with the energy at the source of NIR laser module. The horizontal axis corresponds to the distance between the spot of laser irradiation and the nearest sensing frontend. The minimum energy for the faulty operation of SR was measured to be 4.2 nJ. With regard to this number, the LFIA sensor exhibits the minimum energy for detection from 0.3 nJ to 1.5 nJ, for the minimum to the maximum distance respectively, and therefore is proven to be sufficiently sensitive. It was also demonstrated that the time of post-detection code erase was as small as 2 ns.

V. Conclusions

On-chip protection circuits against physical attacks were introduced for cryptographic devices. The passive SCA according to electromagnetic coupling is sensed through the change in the respective frequencies among dual LC oscillators. The active FA using laser irradiation is detected by measuring voltage bounces due to induced currents spread over a Si substrate. The post-detection countermeasures are shut-down, halt, or even going to dummy operations. The details of sensing circuitry were discussed and demonstrated for sufficient sensitivity under realistic threats of attacks.

The advent of novel physical attacks is a continuous threat in modern hardware security. On-chip sensing and protection mechanisms are fundamentally effective, where further miniaturization and higher sensitivity need to be pursued, and their adaptation to advanced packaging technologies will become of importance.

Distance between sensors	60 [μm] (diagonal)
Sensor threshold voltage (V_{th})	200 [mV]

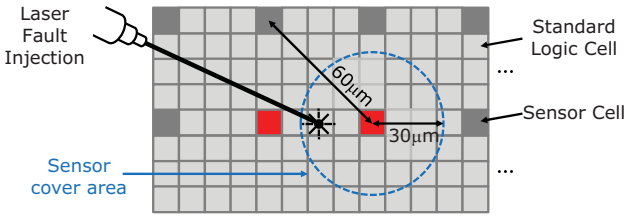


Figure 10: Placement of OCM sensors in standard logic cells for detecting laser irradiation.

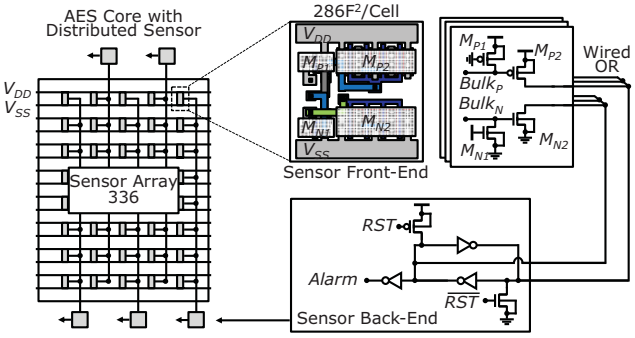


Figure 11: Sensor array architecture and detailed circuits for detecting laser fault injection attack (LFIA).

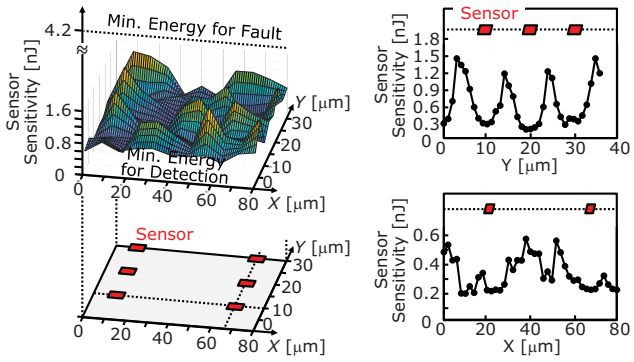


Figure 12: Measurement results of LFIA sensors.

ACKNOWLEDGMENT

The authors would like to deeply thank Mr. K. Matsuda and Mr. A. Tsukioka for their valuable help, and also Prof. K. Sakiyama, Prof. N. Homma, Prof. Y. Hayashi, and Dr. D. Fujimoto for scientific discussions.

This work was partly supported by JSPS KAKENHI Grant Numbers JP2624005, JP15H01688, and JP18H05289. This work was also partly supported by Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Cyber-Security for Critical Infrastructure"(funding agency: NEDO).

REFERENCES

[1] "Secure Integrated Circuits and Systems," I. Verbauwhede, Ed., Springer, 2010 (ISBN 978-0-387-71829-3).

[2] I. Verbauwhede, J. Balasch, S. S. Roy, and A. Van Herrewege, "Circuit Challenges from Cryptography," *ISSCC Dig. Tech. Papers*, pp. 428-429, Feb. 2015.

[3] S. K. Mathew,F. Sheikh, M. Kounavis, S. Gueron,A. Agarwal, S. K. Hsu, H. Kaul, M. A. Anders, and R. K. Krishnamurthy, "53 Gbps Native GF(2^4)^2 Composite-Field AES-Encrypt/Decrypt Accelerator for Content-Protection in 45 nm High-Performance Microprocessors," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 4, pp. 767-776, Apr. 2011.

[4] M. Tamura and M. Ikeda, "1.68μJ/signature-generation 256-bit ECDSA over GF(p) signature generator for IoT devices," *Proc. 2016 IEEE Asian Solid-State Circuits Conference*, pp. 341-344, Nov. 2016.

[5] P. Chodowiec and K. Gaj, "Very compact FPGA implementation of the AES algorithm," *CHES*, *Lecture Notes in Computer Science*, vol. 2779, pp.319-333, 2003.

[6] T. Good and M. Benaissa, "AES on FPGA from the Fastest to the Smallest," *CHES*, *Lecture Notes in Computer Science*, vol. 3659, pp. 427-440, 2005.

[7] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," *CRYPTO 1996, Lecture Notes in Computer Science,* vol. 1109, pp. 104–113, Aug. 1996.

[8] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *CRYPTO 1999, Lecture Notes in Computer Science*, vol. 1666, pp. 388–397, Aug. 1999.

[9] "Hardware Security and Trust, Design and Deployment of Integrated Circuits in a Threatened Environment," N. Sklavos, R. Chaves, G. D. Natale, and F. Regazzoni, Eds., Springer, 2017 (ISBN 978-3-319-44316-4).

[10] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Fault," *EUROCRYPTO*, *Lecture Notes in Computer Science*, vol. 1233, pp. 37-51, May 1997.

[11] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," *CRYPTO*, *Lecture Notes in Computer Science*, vol. 1294, pp. 513-525, Aug. 1997.

[12] D. Karaklajić, J-M. Schmidt, and I. Verbauwhede, "Hardware Designer's Guide to Fault Attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 12, pp. 2295-2306, Dec. 2013.

[13] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault Sensitivity Analysis," *CHES, Lecture Notes in Computer Science*, vol. 6225, pp. 320-334, Aug. 2010.

[14] A. Moradi, O. Mischke, C. Paar, Y. Li, K. Ohta, and K. Sakiyama, "On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attacks in a Combined Setting," *CHES*, *Lecture Notes in Computer Science*, vol. 6917, pp. 292-311, Sep. 2011.

[15] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-25, Feb. 2010.

[16] Y. Jin and Y. Makris, "Hardware Trojans in Wireless Cryptographic ICs," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 26-35, Feb. 2010.

[17] M. Nagata, J. Nagai, T. Morie, and A. Iwata, "Measurements and Analyses of Substrate Noise Waveform in Mixed Signal IC Environment," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 19, No. 6, pp. 671-678, 2000.

[18] T. Hashida, and M. Nagata, "An On-Chip Waveform Capture and Application to Diagnosis of Power Delivery in SoC Integration," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 4, pp. 789-796, Apr. 2011.

[19] A. Tsukioka, M. Nagata, K. Taniguchi, D. Fujimoto, R. Akimoto, T. Egami, K. Niinomi, T. Yuhara, S. Hayashi, R. Mathews, K. Srinivasan, Y-S. Li, and N. Chang, "Simulation Techniques for EMC Compliant Design of Automotive IC Chips and Modules," *Proc. International Symposium on Electromagnetic Compatibility (EMC Europe)*, pp. 1-5, Sep. 2017.

[20] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23-31, Dec. 2009.

[21] N. Miura, D Fujimoto, R. Korenaga, K. Matsuda, and Makoto Nagata, "An Intermittent-Driven Supply-Current Equalizer for 11x and 4x Power-Overhead Savings in CPA-Resistant 128bit AES Cryptographic Processor," *Proc. 2014 IEEE Asian Solid-State Circuits*, pp. 225-228, Nov. 2014.

[22] M. Kar, A. Singh, S. Mathe2, A. Raja, V. De, and S. Mukhopadhyay, "Improved Power-Side-Channel-Attack Resistance of an AES-128 Core via a Security-Aware Integrated Buck Voltage Regulator," *Dig. Tech. Papers, IEEE International Solid-State Circuits Conference*, pp. 142-143, Feb. 2017.

[23] W-H. Yang, L-C. Chu, S-H. Yang, Y-J. Lai, S-Q. Chen, K-H. Chen, Y-H. Lin, S-R. Lin, and T-Y. Tsai, "An Enhanced-Security Buck DC-DC Converter with True-Random-Number-Based Pseudo Hysteresis Controller for Internet-of-Everything (IoE) Devices," *Dig. Tech. Papers, IEEE International Solid-State Circuits Conference*, pp. 126-127, Feb. 2018.

[24] "Power Analysis Attacks – Revealing the Secrets of Smart Cards," S. Mangard, E. Oswald, and T. Popp, Springer, 2007 (ISBN 978-0-387-38162-6).

[25] "Introduction to Hardware Security and Trust," M. Tehranipoor and C. Wang, Eds., Springer, 2012 (ISBN 978-1-4419-8080-9).

[26] "Security of Block Ciphers: From Algorithm Design to Hardware Implementation," K. Sakiyama, Y. Sasaki, and Y. Li, Wiley, 2015 (ISBN: 978-1-118-66001-0).

[27] T. Sugawara, D. Suzuki, M. Saeki, M. Shiozaki, and T. Fujino, "On Measurable Side-Channel Leaks Inside ASIC Design Primitives," *CHES*, *Lecture Notes in Computer Science*, vol. 8086, pp.159-178, Aug. 2013.

[28] D. Fujimoto, D. Tanaka, N. Miura, and M. Nagata, "Side-Channel Leakage on Silicon Substrate of CMOS Cryptographic Chip," *Proc. IEEE International Symposium on Hardware- Oriented Security and Trust (HOST),* pp. 32-37, May 2014.

[29] K. Matsuda, N. Miura, M. Nagata, Y. Hayashi, T. Fujii, and K. Sakiyama, "On-Chip Substrate-Bounce Monitoring for Laser-Fault Countermeasure," *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, pp. 1-6, Dec. 2016.

[30] N. Miura, D. Fujimoto, D. Tanaka, Y. Hayashi, N. Homma, T. Aoki, and M. Nagata, "A Local EM-Analysis Attack Resistant Cryptographic Engine with Fully-Digital Oscillator-Based Tamper-Access Sensor," *Symposium on VLSI Circuits Dig. Tech. Papers*, pp. 172-173, June 2014.

[31] N. Homma, Y. Hayashi, T. Aoki, N. Miura, D. Fujimoto, and M. Nagata, "Design Methodology and Validity Verification for a Reactive Countermeasure Against EM Attacks," *IACR Journal of Cryptology*, pp. 1-19, Online, Dec. 2015.

[32] K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y. Hayashi, M. Nagata, and N. Miura, "A 286 F^2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack on Cryptographic Processor," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 11, pp. 3174-3182, Sep. 2018.

[33] E. H. Neto, I. Ribeiro, G. Wirth, F. Kastensmidt, and M. Vieira, "Using Bulk Built-in Current Sensors to Detect Soft Errors," *IEEE Micro*, vol. 26, no. 4, pp. 10-18, Sep. 2006.