A 286 F2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack on Cryptographic Processor

Matsuda, Kohei ; Fujii, Tatsuya ; Shoji, Natsu ; Sugawara, Takeshi ; Sakiyama, Kazuo ; Hayashi, Yu-ichi ; Nagata, Makoto ; Miura, Noriyuki

(Citation)
IEEE Journal of Solid-State Circuits,53(11):3174-3182

(Issue Date)
2018-11

(Resource Type)
journal article

(Version)
Accepted Manuscript

(URL)
https://hdl.handle.net/20.500.14094/90005512

A 286 F^2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser against Laser Fault Injection Attack on Cryptographic Processor

Kohei Matsuda, *Student Member*, *IEEE*, Tatsuya Fujii, Natsu Shoji,
Takeshi Sugawara, Kazuo Sakiyama, *Senior Member*, *IEEE*, Yu-ichi Hayashi, *Member*, *IEEE*,
Makoto Nagata, *Senior Member*, *IEEE*, and Noriyuki Miura, *Member*, *IEEE*

***Abstract*— Laser Fault Injection (LFI) attack on cryptographic processors is a serious threat to information security. This paper proposes a sense-and-react countermeasure against LFI. A distributed bulk-current sensor monitors the abnormal current conduction caused by laser irradiation to a silicon substrate. The single sensor occupies only 286 F^2/Cell and it is distributed across the entire cryptographic core for 100% attack detection coverage. Upon detection of LFI attack, a flush code eraser prevents a leakage of faulty ciphertext by immediately shunting the core supply path within nano-second order. In addition, the core supply during the shunting is electrically isolated from the global supply line to prevent side-channel information leakage of intermediate faulty codes. A test chip was designed and fabricated in 0.18μm standard CMOS, integrating a 128-bit Advanced Encryption Standard (AES) cryptographic processor with the proposed countermeasures. A protected AES processor can disable LFI attack with only +28% layout area penalty compared to an unprotected core.**

***Index Terms*—Fault Attack, Hardware Security, Laser Fault Injection Attack (LFI), Advanced Encryption Standard (AES), Bulk Built-In Current Sensor (BBICS)**

I. Introduction

CRYPTOGRAPHIC devices are widely used for protecting security and privacy of important and critical data especially in the current advanced information society. However, it is a well-known threat that such secret information protected by the cryptography can be easily disclosed by malicious physical attacks on the devices. One of the typical physical attacks is side-channel attack [1, 2] which reveals the secret information (e.g. secret key) by probing and collecting power consumption or electromagnetic radiation which are leaked from the cryptographic devices. Another serious threat is Fault Attack (FA) where an intentional fault is induced during a cryptographic operation, and a secret key is revealed by analyzing erroneous output and correct output. Both attacks have been intensively studied for more than two decades as realistic threats to real-world cryptographic devices [3].

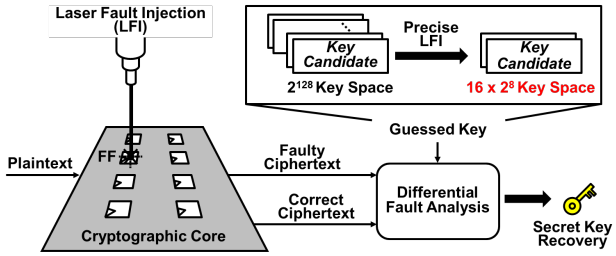


Fig. 1 Concept of differential fault analysis with laser injection.

Faulty operation of very large-scale integration (VLSI) has been studied so far in relation with soft error [4, 5]. This is an incidental memory (and also logic) error that occurs when electromagnetic waves such as cosmic rays are irradiated on the VLSI. Various safety techniques based on soft error detection and correction have been developed to prevent malfunction of the circuit by soft error [6, 7]. On the other hand, in FAs, secret information in cryptographic processors can be exposed by intentional fault injection. Against such attack, the conventional safety techniques are not sufficient and hence an active countermeasure to prevent information leakage is needed.

FA on public-key cryptography was first proposed by Boneh, DeMillio, and Lipton in 1997 [8]. Also, in 1997, Biham and

This work was supported by JSPS Grants-in-Aid for Scientific Research under Grant 15H01688 and 18H05289. The authors are grateful to Information-technology Promotion Agency (IPA) for the laser test setup and technical assistance. (*Corresponding author: Kohei Matsuda*)

K. Matsuda and N. Miura are with the Graduate School of System Informatics, Kobe University, Kobe 6578501, Japan (e-mail: k_matsuda@cs26.scitec.kobe-u.ac.jp; miura@cs.kobe-u.ac.jp).

T. Fujii was with The University of Electro-Communications, Tokyo 1828585, Japan. He is now with Anritsu Corp., Atsugi 2438555, Japan (e-mail: Tatsuya.Fujii@anritsu.com).

N. Shoji, T. Sugawara, and K. Sakiyama are with The University of Electro-Communications, Tokyo 1828585, Japan (e-mail: n.shoji@uec.ac.jp; sugawara@uec.ac.jp; sakiyama@uec.ac.jp).

Y. Hayashi is with the Graduate School of Information Science, Nara Institute of Science and Technology, Nara 6300192, Japan (e-mail: yu-ichi@is.naist.jp).

M. Nagata is with the Graduate School of Science, Technology, and Innovation, Kobe University, Kobe 6578501, Japan (e-mail: nagata@cs.kobe-u.ac.jp).

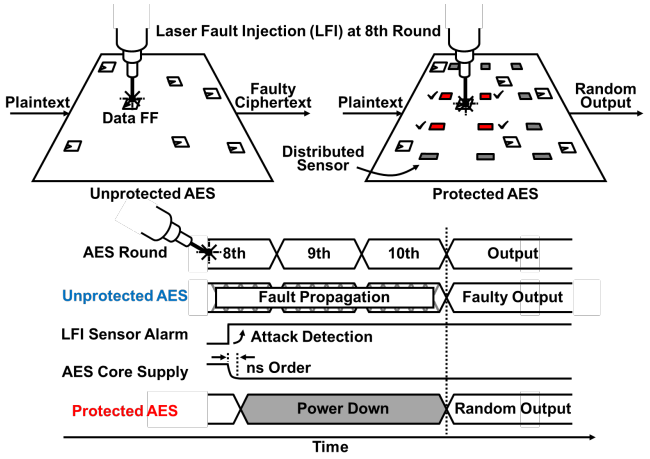


Fig. 2 Conceptual sketch of proposed sense-and-react countermeasure against laser fault injection attack.

Shamir proposed a Differential Fault Analysis (DFA) attack which is applicable to symmetric-key cipher [9]. In DFA, pairs of correct and faulty ciphertexts are collected and analyzed in order to reduce the key space based on a fault model. Since the first FA proposal in 1997 [8, 9], FA has been sophisticated for two different directions. One is its practical application such as to Advanced Encryption Standard (AES) by Piret and Quisquater in 2003 [10]. In this attack, only two pairs of correct and faulty ciphertexts are needed to totally break AES with 116-bit out of 128-bit secret key disclosure [11]. Another direction is Fault Sensitivity Analysis (FSA) proposed by Li *et al*. in 2010 [12] and then improved by Moradi *et al*. [13, 14]. The attack extends potential targets of FA by relaxing a requirement for the attacker: a pair of correct and faulty ciphertexts is no longer needed. It only requires the sensitivity threshold of fault occurrence. The effectiveness of the attack is proved with various processors implementing AES. As described above, the FA methodology is rapidly advancing, and the effective countermeasure is needed.

Among various fault injection techniques, it is considered that Laser Fault Injection (LFI) [15] is one of the most powerful physical attacks because LFI has high timing and positional resolution. For example, a single flip-flop used in a specific clock cycle for AES round operation can be targeted. High controllability of fault injection timing and position increases the efficiency of DFA/FSA (Fig. 1). By using a laser, temporary fault injection can be induced with arbitrary data registers and operational timing [15]. With such high spatial and positional resolution of LFI, it is possible to build an accurate fault model for the more efficient attack scheme.

Popular countermeasures against FAs involve doubling and verification [16, 17]. In doubling, encryption is performed redundantly with multiple encryption cores. The outputs from two cores are compared to detect a fault. In verification, on the other hand, an output of an encryption is immediately decrypted. Then, the decrypted message is compared with an original message to detect a fault. Although they need more than 200% penalty in power consumption and area, these countermeasures can be defeated by multiple laser injections with accurate timing and position control [18]. These countermeasures deal with only a secondary information caused as a result of fault injection (e.g. faulty ciphertext) and therefore its security level is limited even with the huge penalty in power and area resources. More fundamental approach would be directly dealing with the physical phenomenon primarily accompanying the fault injection.

There are such physical-level countermeasures integrated into IC chip. The one is a laser injection shield by utilizing metal interconnections of IC chip. However, this metal shield can be bypassed by Near Infra-Red (NIR) LFI from IC chip backside since the NIR laser can penetrate through silicon substrate and hit the cryptographic circuit layer [19]. Another countermeasure is integrating physical sensor into the IC chip for detecting laser irradiation [20]. In order to monitor abnormal temperature or light change due to laser irradiation, photodetector or temperature sensor are mounted with a cryptographic core. The challenge of this methodology is how hardware overhead can be suppressed. Although both of these countermeasures directly observe the physical phenomenon accompanying LFI, the output signal is a pure analog voltage or current, an Analog-to-Digital Converter (ADC) is required to finally detect the abnormal events and cooperate with a digital cryptographic core. Furthermore, in order to detect the local temperature and light amount change caused by the focused LFI, high-density sensor arrangement is required for the 100% detection coverage of the entire cryptographic core.

In this work, a compact sense-and-react countermeasure against LFI is proposed. This countermeasure consists of a distributed bulk-current sensor for LFI detection and secure flush code eraser for erasing internal data as shown in Fig. 2. Bulk-current sensor is monitoring abnormal transient current in the silicon substrate due to laser irradiation. Since this transient current spreads all over the shared silicon substrate, a sparse sensor array arrangement is possible for layout area penalty saving. Secure flush code eraser is essentially a power supply switch circuit of a cryptographic core. The power supply path is immediately switched and cut off in reaction to LFI detection alarm signal from the sensor module. By doing this, a cryptographic core is quickly discharged and faulty intermediate value can be quickly erased.

The rest of the paper is organized as follows. Next, Section II will review LFI mechanism and describe LFI sensor circuit and its operation. Section III will describe the secure flush code eraser circuit. Section IV and V will present the test chip, experimental setup, and the measurement results. With an actual laser injection test against AES core, the effectiveness of LFI sensor and flush code eraser is evaluated. Finally, concluding remarks will be drawn in Section VI.

II. LFI Detection Mechanism

A. *Physical Mechanism of LFI*

It is known that the physical mechanism of LFI is essentially the same as soft error that has been a critical issue in IC memory module since the 60's [4]. A soft error occurs mainly due to accidental cosmic rays and environmental electromagnetic

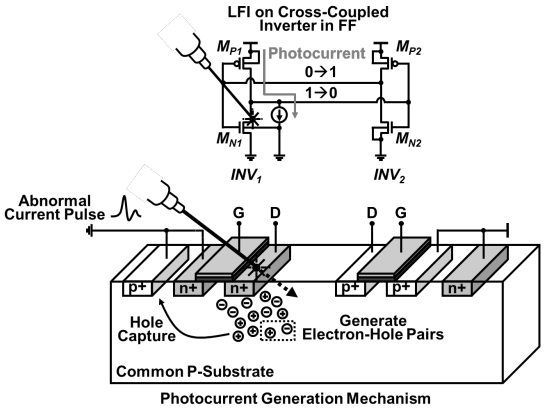


Fig. 3 Physical mechanism of laser fault injection.

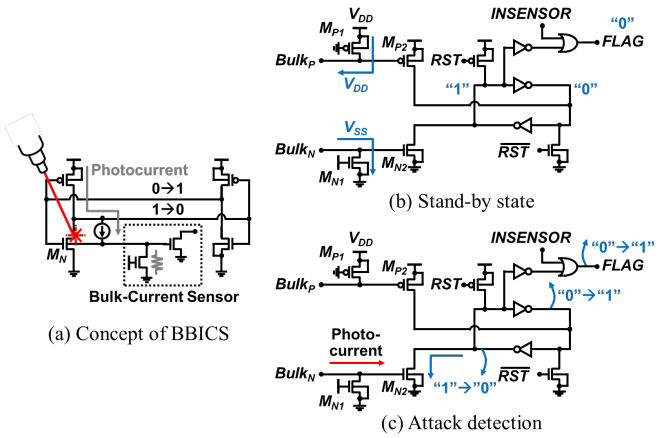


Fig. 4 Mechanism of bulk built-in current sensor (BBICS).

waves hit to a memory module. A laser has been used to produce soft errors since early times [5], and now, unfortunately, they are used for physical attacks on cryptographic cores [18, 19, 22].

Figure 3 explains the physical phenomena which is occurred by laser injection to a silicon substrate. When a laser is irradiated to the PN junction inside the silicon substrate, electron-hole pairs are generated. In the absence of a potential slope, these electron-hole pairs quickly disappear through a thermal relaxation process. However, if there are potential slopes around them, they do not disappear, and electrons and holes flow into positively and negatively biased regions, respectively. As a result, an abnormal transient current is generated inside the silicon substrate. This abnormal current charges or discharges an internal memory node voltage and causes data flip. Cross-coupled inverters are core circuits of the Static Random Access Memory (SRAM) and the D Flip-Flop used as the data register of cryptographic cores. In the case of LFI to drain terminal of turned-off transistor M_{N1}, as shown in Fig. 3, a photocurrent is generated between M_{N2} bulk-contact and drain terminal. Due to this generated transient current, the M_{P2} transistor of *INV2* is turned-on and the output value of *INV2* is changed. Finally, an error of the data held in the cross-coupled inverter occurs. This is the background physical mechanism of LFI so-called Single Event Upset (SEU). In scaled CMOS, a device becomes more vulnerable against LFI, same as the modern trend in soft error [23]. However, since the

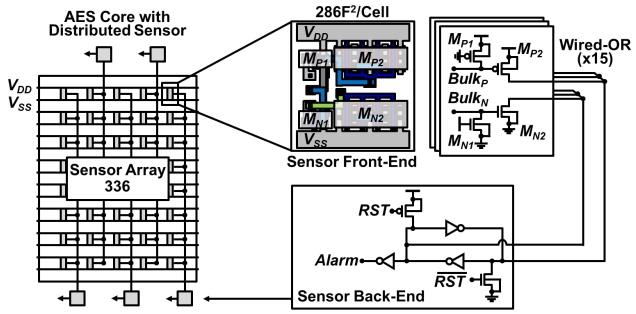


Fig. 5 Circuit detail of distributed bulk-current sensor for LFI detection.

device size shrinks, the position and focus control of the laser spot would be more difficult. The LFI attack is still possible by employing a shorter-wavelength laser source with more precise mechanical alignment.

B. Bulk Built-In Current Sensor (BBICS)

In 2006, Bulk Built-In Current Sensor (BBICS) was proposed by Neto *et al.* for soft-error detection [6]. Figure 4 (a) depicts a concept of BBICS. In order to detect the transient current due to LFI described in the previous section, a bulk-current sensor is inserted into the bulk contact of each transistor (Fig. 4). During normal operation, the current conduction at the bulk contact is very small. The mA order photocurrent generated by laser irradiation can be easily detected with a small resistor and a voltage amplifier as shown in Fig. 4 (a).

Figures 4 (b) and 4 (c) are circuit schematics of the enhanced BBICS proposed by Champeix *et al.* in 2015 [24]. $Bulk_P$ and $Bulk_N$ terminals are connected to bulk contacts of PMOS and NMOS, respectively. When LFI attack is detected, *FLAG* becomes "High" and an alarm is generated. Figure 4 (b) shows the stand-by operation of BBICS. In the standby state, bulk contacts are biased to V_{DD} and GND respectively through M_{P1} and M_{N1} which are always turned-on. In this stand-by state, no active power is consumed in the circuit including the additional BBICS. Figure 4 (c) depicts the BBICS operation at the LFI detection. When NMOS is the target of LFI, photocurrent generated in the bulk flows into M_{N1}. The $Bulk_N$ voltage is increased and M_{N2} is turned-on. The data held by the cross-coupled inverter at the subsequent stage is then inverted, and the alarm signal *FLAG* becomes "High". The cryptographic core can react upon this alarm signal for protecting internal data from malicious attack (e.g. system reset, stop operation).

C. BBICS Integration Methodology

Although BBICS can detect LFI on registers with low power consumption, there is no discussion about actual implementation methodology for cryptographic processors [6, 24, 25]. This paper proposes design methodology to integrate BBICS into cryptographic cores with low layout area penalty. Figure 5 shows a detailed composition of the protected AES core including BBICS circuits. In this design method, BBICS is divided into a front-end module for sensing abnormal bulk-current and a back-end module for generating an alarm signal. The front-end module consists of only four transistors, operating as a pair of small register and voltage amplifier

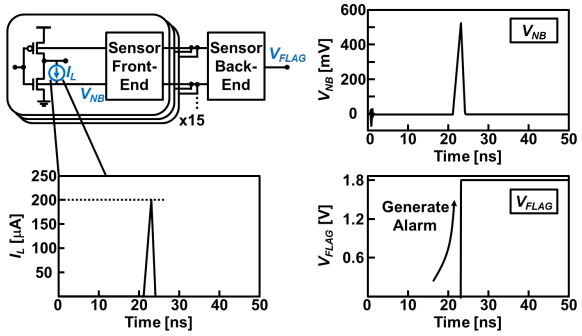


Fig. 6 Simulated LFI sensor sensitivity (1 back-end module for 15 front-end modules).

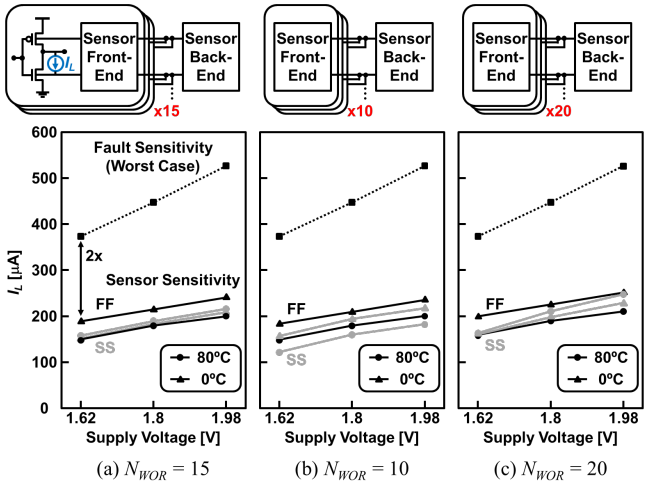


Fig. 7 Simulated LFI sensor sensitivity and fault sensitivity dependence on PVT variations and number of wired-OR outputs.

inserting to photocurrent path. The single sensor size is only 286 F^2/Cell (~2.6 gate equivalent of 2-input NAND), and it is distributed to across the entire cryptographic core for 100% detection coverage. In order to maximize the sensor sensitivity, all tap cells including body contacts are removed in the AES core. The body connections are provided through the sensor front-ends.

Sensor sensitivity and placement interval were determined based on a characterization of preliminary analysis result reported in [26]. A photocurrent generated by laser injection at PN junction was characterized based on measurement of substrate voltage bounce by using an on-chip monitor [26]. Without any confidential process parameters, the photocurrent power causing fault was finally derived by fitting a simple equivalent circuit response to the captured substrate voltage bounce waveform. The sensor sensitivity was designed to detect this photocurrent with large enough margin. The photocurrent propagation characteristics was also measured by multiple monitoring of the substrate voltages [26]. The sensor pitch in X-axis was set to 60 μm based on these analysis and measurement results. The sensor pitch in Y-axis was set to 5 μm for 100% detection coverage for all isolated n-wells. If a deep n-well option and also confidential process parameters are available, the sensor overhead especially for the Y-axis direction could be significantly reduced.

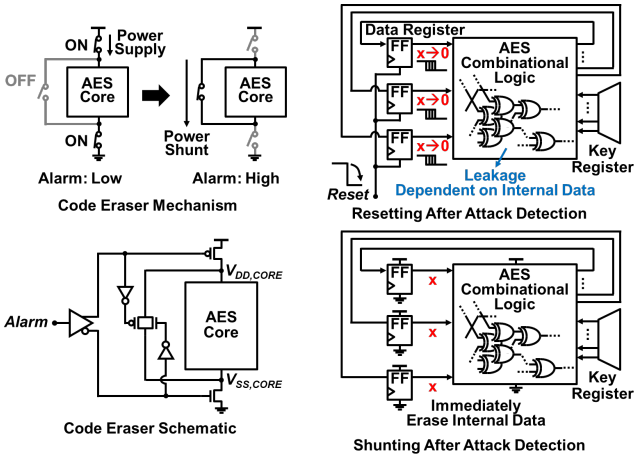
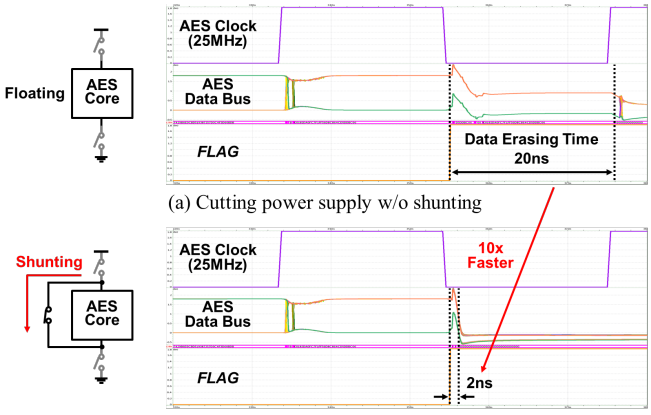


Fig. 8 Circuit detail of flush code eraser.

Since the output of front-end module is current, the output wires can be wired-OR into back-end module. The layout area penalty can be saved by reducing the number of required back-end modules. The output configuration of the distributed sensor front-ends is basically designed based on consideration of a trade-off among sensor sensitivity, layout area overhead, and detection range redundancy. In this design, 15 front-end outputs are wired-OR into one back-end module. With this configuration, 3 wired-OR outputs per column can be obtained also for the detection range redundancy. Figure 6 shows the simulated waveforms for verification of sensor sensitivity in the case of wired-OR design in 0.18 μm standard CMOS. The PVT conditions of the simulation are TT, 1.8 V, and 27 ºC. The photocurrent causing SEU of the FF in this process was measured to be around 500μA-peak pulse current based on the preliminary measurement with simulated analysis in [26]. LFI sensor sensitivity was secured against 200μA-peak current pulse which is 2.5x smaller than current pulse required for fault injection. Figure 7 presents simulated sensor sensitivity considering PVT variations and number of wired-OR outputs N_{WOR}. The fault sensitivity represents required current power I_L for temporary bit error, and the worst-case minimum I_L is plotted in the graph. The sensor sensitivity represents the minimum photocurrent power for the LFI sensor reaction. As shown in Fig. 7, the sensor sensitivity is degraded by increasing the number of wired-OR outputs N_{WOR} while the layout area overhead for the sensor back-ends can be reduced. With the temperature increase, both the fault and sensor sensitivity increase because the latch, the common core circuit of both the register and the sensor back-end, becomes weak in its data retention force. This matched circuit structure between the register and sensor back-end increases the design margin against temperature variation. In this design, N_{WOR} = 15 was chosen to finally guarantee >2x sensitivity margin even in the worst case.

III. Secure Flush Code Eraser

In order to prevent leakage of confidential information from the cryptographic core, it is necessary not only to detect LFI but also to integrate a post-detection countermeasure with small layout area penalty. Figure 8 shows details of proposed reactive



(a) Cutting power supply w/o shunting

(b) Cutting power supply w/ shunting (Proposed)

Fig. 9 Simulated results of required time for erasing intermediate value of AES operation.

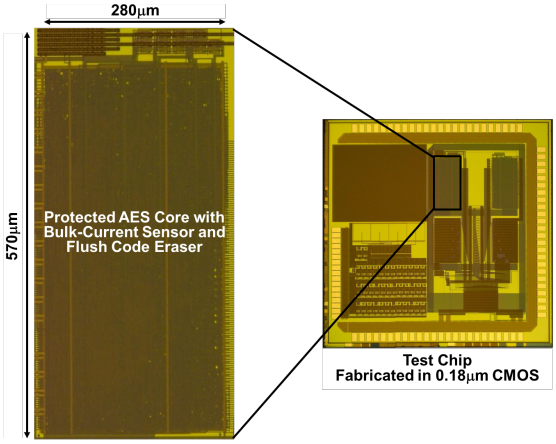


Fig. 10 Die micrograph of the test chip.

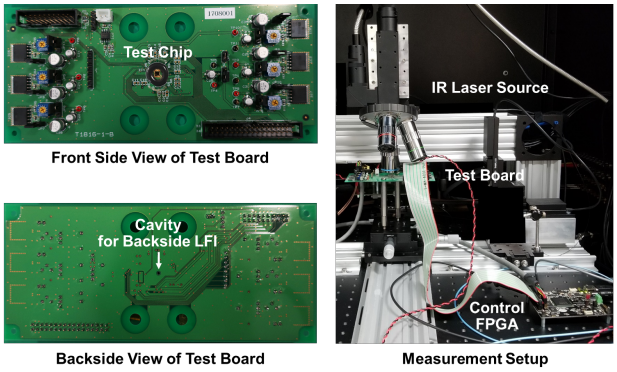


Fig. 11 Test board and measurement system setup.

countermeasure circuit, namely a flush code eraser. When the LFI sensor detects an attack against a cryptographic core, power switches inserted into the supply and the ground path (V_{DD} and GND) are instantaneously cut off. The additional shunt switch is then turned on and the floating supply charge for the AES core is immediately discharged. By doing this, the internal sensitive faulty data in the AES core is quickly erased. Figure 9 (a) shows a simulated result of required time for erasing AES data bus in the case without the shunt switch (the power supply is floating), and Figure 9 (b) shows the case with shunt switch. In either simulation, the power supply path is switched in accordance with the rise of the alarm signal. With the aid of the shunt switch, the intermediate faulty cipher code can be erased 10x faster than that without the shunt switch. The effect of the shunt transistor becomes significant in very low temperature. If there are only power cut switches, the data erase time would be significantly increased, which can be utilized as a cold boot attack [27]. The shunt transistor guarantees the instantaneous data erase even in the very low temperature where the connectivity of the shunt transistor would become even stronger for instantaneous shunt down. The code erase time with this shunt scheme is also shorter than that with a DFF reset scheme by the delay time of internal combination logic. Moreover, the proposed code eraser is securer than reset scheme because the core supply line is electrically separated from global power supply line. In reset scheme, the side-channel power noise which depends on holding data in FF is leaked through a global supply line. The register data inside the cryptographic core can be revealed by collecting and analyzing power supply noise waveforms.

IV. Experimental Setup

A. Test Chip Design

A test chip was designed and fabricated in 0.18 μm standard CMOS process (Fig. 10). A 128-bit AES cryptographic processor was chosen as a target design. The AES core was implemented in a round-based sequential logic with 128-bit round key and intermediate data registers. The data in the registers are updated at every round operation. Two AES cores are integrated in the test chip. One is a protected AES with the distributed bulk-current sensor and the flush code eraser and the other is an unprotected AES for comparison. The both AES cores were designed by a standard digital circuit design flow with commercial Electronic Design Automation (EDA) toolchain. In order to detect LFI throughout the AES core, the arrangement interval of the sensor front-end modules was set to 60 μm in the X-direction and 6 μm in the Y-direction based on the preliminary characterization. Since photocurrent propagates widely in a common silicon substrate, it is possible to realize a sparse sensor arrangement interval and therefore save layout area penalty. There are 336 front-end modules and 23 back-end modules integrated into the protected AES core. Total layout area overhead including code eraser was only +28% compared with the unprotected AES core which was designed in the same process.

B. Evaluation System

Figure 11 depicts photographs of test board and measurement system. The test chip was mounted on the test board and the IO pads were wire-bonded. The test chip surface is exposed for laser irradiation to AES core. In addition, on the backside of the test board, a small cavity is created under the test chip in order to perform LFI from the chip backside substrate. An invisible NIR laser is used as a laser source for capable of the backside LFI that bypasses the metal shielding at the top of the cryptographic core. The test chip was fixed under the laser module, and the laser irradiation spot was focused down to 2

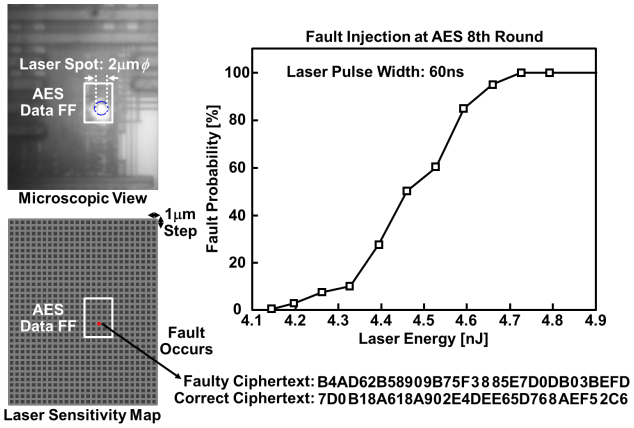


Fig. 12 Measured laser sensitivity map and fault probability dependence on laser energy.

μm in a diameter through an optical microscope with a 50x magnification lens. The laser irradiation position can be controlled with 1 μm step in every XYZ directions. This 1 μm step is the minimum step available in the measurement setup where the laser irradiating scope is mechanically position-controlled by DC servo actuators. This setup is fine enough for attacking 0.18 μm CMOS AES. A finer control would be needed for attacking scaled devices. Since the sensor detects abnormal photocurrent due to the irradiation and the current spreads in the shared substrate, the dense sensor arrangement is not needed against such advanced laser irradiation system with the fine control. The state and setting of the test chip and measurement system were controlled by FPGA (Fig. 11). The laser pulse width was set to 60 ns based on multiple-samples measurement trials. If it is too short, the light energy is not high enough to induce fault. Too long on the other hand, the device could be permanently destroyed. The laser injection timing setting is also important. In this setup, it is possible to perform LFI to an arbitrary AES operation round synchronously with the laser trigger signal from the FPGA. However, even if AES operation timing cannot be fine-grained control, an attacker can externally identify it by observing the power line spike and inject fault at the appropriate timing [28]. The attacker can also verify the successful fault from the core output.

V. Measurement Result

A. Fault Sensitivity

Firstly, the fault sensitivity of DFF which is one of the AES data registers was measured (Fig. 12). The laser irradiation position was swept with 1 μm step in the area containing DFF and a fault injection point was scanned. In this experiment, 8th round laser fault injection is used as this is one of the most efficient DFAs [10]. The secret key could be actually disclosed from faulty ciphertext obtained by LFI on the 8th round of AES operation. A measurement result of the fault probability for that point is also shown in Fig. 12. The X-axis represents the minimum laser energy required to induce a fault and the Y-axis represents the fault probability. It was confirmed that the fault

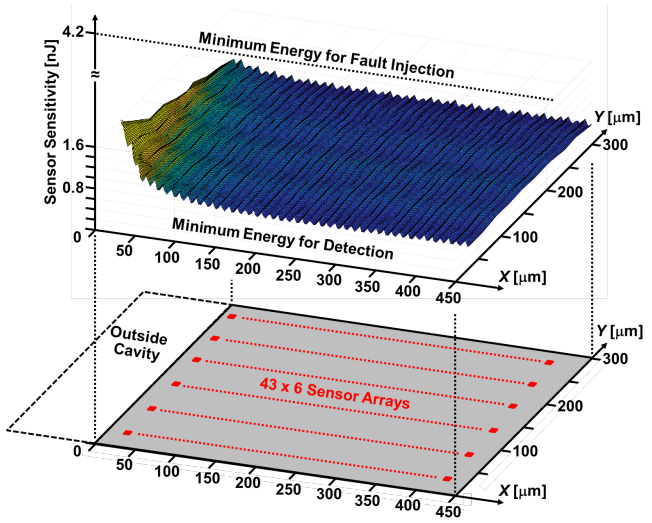


Fig. 13 Measured sensor sensitivity map of protected AES core.

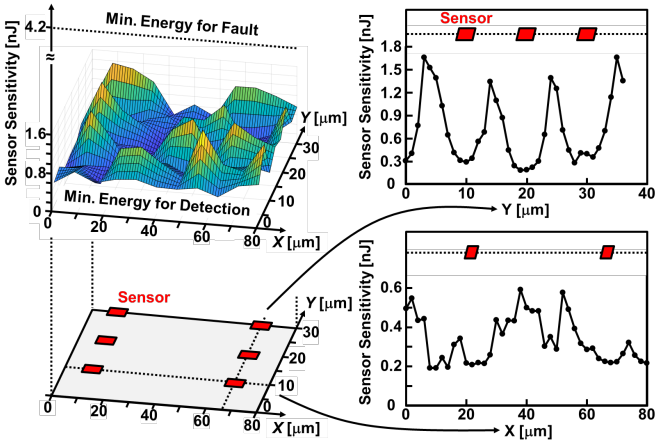


Fig. 14 Measured minimum laser energy detected by distributed sensor.

probability increases from 0% to 100% as the laser energy increases. Moreover, in this experiment, if a laser energy is larger than 4.2 nJ, data register outputs start to flip. In order to react the LFI attack, the LFI sensor needs to detect laser irradiation of 4.2 nJ energy with enough detection margin.

B. Sensor Sensitivity

Next, LFI sensor sensitivity of the distributed bulk-current sensor integrated into the protected AES core was measured. Backside laser injection was performed from the cavity on the backside of the test board shown in Fig. 11. Sensor sensitivity represents a minimum laser energy required for the sensor to raise the alarm signal. Figure 13 shows a sensor sensitivity map and corresponding sensor location of protected AES core. In this experimental setup, only 258(43x6) out of 336(56x6) sensor modules were exposed from the backside cavity. The LFI sensitivity was evaluated only at these exposed sensors. Except at the cavity edge, the sensor sensitivity was very flat and stably high to safely detect LFI. The measured sensor sensitivity was slightly degraded due to run-over glue at the cavity edge. However, without this, the continuous and flat sensitivity would be obtained for the entire core area. Figure 14 depicts more detailed sensor sensitivity map and the sensor

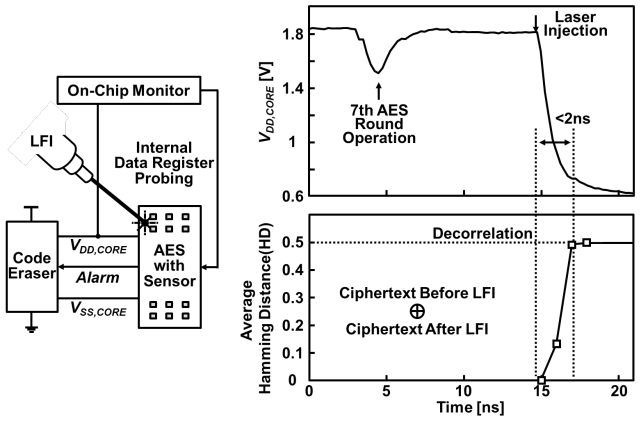


Fig. 15 Measured core supply waveform and average HD between ciphertext before and after LFI.

TABLE I
PERFORMANCE COMPARISON TABLE

Parameter	This Work (0.18μm CMOS)		[17] (0.13μm CMOS)
	Unprotected	Protected	
Area [mm²]			
AES Core	0.138	0.165 (+19.6%) (w/ Sensor Front-End)	-
Sensor Back-End	-	0.005	-
Code Eraser	-	0.006	-
Total	0.138	0.176 (+28%)	(+104%)
Power Consumption [mW]	14.96	15.01 (+0.3%)	-
Operating Range [V]	1.25 - 1.8	1.25 - 1.8	-
Maximum Frequency [MHz]	160.5	149.5 (-6.8%)	50
Side-Channel Attack Resistance	No	No	Yes

sensitivity along with X-axis and Y-axis. The sensor sensitivity is far smaller than the laser energy required for fault injection described previously. Moreover, as shown in Fig. 14, even in LFI of the intermediate position of each sensor, this LFI sensor can be detected laser irradiation with enough margin. Based on the results, the well-designed sensor by preliminary characterization has sufficient LFI detection sensitivity even when integrated into the actual cryptographic core.

C. Evaluation of Code Eraser

Finally, a code eraser function which is reacting countermeasure against LFI was evaluated. On the test chip, an On-Chip Monitor (OCM) circuit [29] was integrated to monitor the V_{DD} of the cryptographic core. A digital bus monitor was also integrated to see internal data registers value. In this experiment, a fixed plaintext was used for evaluation. Figure 15 shows a behavior of power supply voltage and the internal data register value of the protected AES core, respectively. In both results, LFI was performed in the 8th round of AES operation. It was confirmed that the power supply voltage rapidly dropped to around 0.6 V in 2 ns with LFI. The code eraser functionality was evaluated by calculating the average Hamming Distance (HD) between 128-bit correct ciphertext and the erased text upon LFI detection by taking XOR and comparing their bit code. As shown in Fig. 15, with the 2 ns rapid power shut down, the average HD quickly reaches 0.5 which denotes the erased data to be completely uncorrelated with the ciphertext. The average HD of 0.1 was instantaneously measured at 16 ns. This is because a short skew before completely erasing the data in the 128-bit data registers globally distributed over the entire AES core. It was also confirmed that the output code was significantly fluctuated at each operation. Further measurement would be needed to conclude whether this is truly random or not.

D. Performance Comparison

Table I compares the performances of the protected, unprotected AES cores and prior art [17]. The layout area overhead of protected AES core which is integrated with 336 distributed bulk-current sensor arrays is +19.6% compared with an unprotected core. And, the total overhead including sensor back-end modules and flush code eraser block is only +28%. The power consumption of the protected AES core was 15.0 mW at 24 MHz 1.8 V operation (calculated by post-layout analog circuit simulation). The power increase due to all the additional protection circuit was measured to be 0.05 mW. The power overhead is calculated to be only 0.3%. The operating voltage range was the same for both cores from 1.25 V to 1.8 V. Also, the overhead of maximum operating frequency is only 6.8% compared to the unprotected core. This maximum frequency reduction is caused by the supply voltage drop due to the power and ground switches series-inserted in the power rail. Although the proposed countermeasure has no side-channel attack resiliency, a combinational integration with small-overhead side-channel countermeasures [30-31] is possible to enhance the security level.

VI. CONCLUSION

This paper presents a compact sense-and-react countermeasure against laser fault injection attack. This countermeasure consists of distributed bulk-current sensor and secure flush code eraser. With LFI, abnormal transient current occurs in the substrate as an inevitable physical phenomenon. Since this transient current propagates widely on the common substrate of the cryptographic core, it can be easily detected with sparse sensor arrays. The layout area of the bulk-current sensor is only 286 F^2/Cell, and it is distributed to the entire cryptographic core for 100% detection coverage. In addition, as a reactive countermeasure against LFI, a flush code eraser that instantly erases the internal data was integrated. In accordance with attack detection alarm, the power supply path of the core is cut off and rapidly discharged. A test chip was designed and fabricated in 0.18 μm standard CMOS process for evaluating proposed countermeasure. A protected AES core which is integrated with distributed bulk-current sensor and flush code eraser was mounted on the test chip. The hardware overhead was only +28% compared with unprotected 128-bit AES processor.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *CRYPTO, Lecture Notes in Computer Science*, vol. 1666, pp. 388-397, Aug. 1999.

[2] E. Brier, C. Clavier, and F. Oliver, "Correlation Power Analysis with a Leakage Model," *Conference on Cryptographic Hardware and Embedded Systems (CHES), Lecture Notes in Computer Science*, vol. 3156, pp. 16-29, Aug. 2004.

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

[4] J. L. Wirth, and S. C. Rogers, "The Transient Response of Transistors and Diodes to Ionizing Radiation," *IEEE Transactions on Nuclear Science*, vol. 11, pp. 24-38, Nov. 1964.

[5] D. H. Habing, "The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits," *IEEE Transactions on Nuclear Science*, vol. 12, pp. 91-100, Dec. 1965.

[6] 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.

[7] S. Das, C. Tokunaga, S. Pant, W.-H. Ma, S. Kalaiselvan, K. Lai, D. M. Bull, and D. T. Blaauw, "Razor II: In Situ Error Detection and Correction for PVT and SER Tolerance", *IEEE Journal of Solid-State Circuits*, vol. 44, No. 1, pp. 32-48, Dec. 2008.

[8] 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.

[9] 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.

[10] G. Piret and J. J. Quisquater, "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD," *Conference on Cryptographic Hardware and Embedded Systems (CHES), Lecture Notes in Computer Science*, vol. 2779, pp. 77-88, Aug. 2003.

[11] K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, "Information-Theoretic Approach to Optimal Differential Fault Analysis," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 1, pp. 109-120, Feb. 2012.

[12] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault Sensitivity Analysis," *Conference on Cryptographic Hardware and Embedded Systems (CHES), Lecture Notes in Computer Science*, vol. 6225, pp. 320-334, Aug. 2010.

[13] 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," *Conference on Cryptographic Hardware and Embedded Systems (CHES), Lecture Notes in Computer Science*, vol. 6917, pp. 292-311, Sep. 2011.

[14] A. Moradi, O. Mischke and C. Paar, "One Attack to Rule Them All: Collision Timing Attack versus 42 AES ASIC Cores," *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1786-1798, Sep. 2013.

[15] S. P. Skorobogatov and R. J. Anderson, "Optical Fault Induction Attacks," *Conference on Cryptographic Hardware and Embedded Systems (CHES), Lecture Notes in Computer Science*, vol. 2523, pp. 2-12, Aug. 2002.

[16] T. G. Malkin, F. X. Standaert, and M. Yung, "A Comparative Cost/Security Analysis of Fault Attack Countermeasure," *Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 109-123, Sep. 2005.

[17] M. Doulcier-Verdier, J. Dutertre, J. Fournier, J. Rigaud, B. Robisson, and A. Tria, "A Side-Channel and Fault-Attack Resistant AES Circuit Working on Duplicated Complemented Values," *ISSCC Dig. Tech. Papers*, pp. 274-275, Feb. 2011.

[18] E. Trichina and R. Korkikyan, "Multi Fault Laser Attacks on Protected CRT-RSA," *Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 75-86, Aug. 2010.

[19] J. Woudenberg, M. F. Witteman, and F. Menarini, "Practical Optical Fault Injection on Secure Microcontrollers," *Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 91-99, Sep. 2011.

[20] Renesas Technology Corporation, "IC Card System using Photo-Detectors for Protection," US Patent US7042752 B2.

[21] K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y. Hayashi, M. Nagata, and N. Miura, "A 286F²/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack," *ISSCC Dig. Tech. Papers*, pp. 352-353, Feb. 2018.

[22] C. Roscian, J.M. Dutertre, and A. Tria, "Frontside Laser Fault Injection on Cryptosystems –Application to the AES Last Round–," *IEEE Hardware-Oriented Security and Trust (HOST)*, pp. 119-124, June 2013.

[23] R. Baumann, "The Impact of Technology Scaling on Soft Error Rate Performance and Limits to the Efficacy of Error Correction," *Dig. International Electron Devices Meeting*, pp. 329-332, Dec. 2002.

[24] C. Champeix, N. Borrel, J.-M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, "Experimental validation of a Bulk Built-In Current Sensor for detecting laser-induces currents," *IEEE International On-Line Testing Symposium (IOLTS)*, pp. 150-155, July 2015.

[25] J.-M. Dutertre, R. P. Bastos, O. Potin, M. L. Flottes, B. Rouzeyre, G. D. Natale, "Sensitivity tuning of a bulk built-in current sensor for optimaltransient-fault detection," *Microelectronics Reliability*, vol. 53, pp. 1320-1324, Sep. 2013.

[26] 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.

[27] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest We Remember: Cold Boot Attacks on Encryption Keys," *Proc. of the 17th USENIX Security Symposium*, pp. 45-60, July 2008.

[28] M. Joye, and M. Tunstall, "Fault Analysis in Cryptography," *Springer*, June. 2012.

[29] 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.

[30] 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.

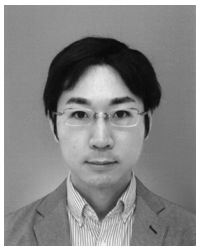
[31] N. Miura, D. Fujimoto, D. Tanaka, Y. Hayashi, N. Homma, T. Aoki, and M. Nagata, "A Local EM-Analysis Attack Resistant Cryptographic Engine with Fully-Digital Oscillator-Based Tamper-Access Sensor," *Symposium on VLSI Circuits Dig. Tech. Papers*, pp. 172-173, June 2014.

Kohei Matsuda (S'17) received the B.S. and M.S. degrees in computer science from Kobe University, Kobe, Japan, in 2015 and 2017, respectively. He is currently working toward the Ph.D. degree.

His research interests include circuit-level countermeasure against physical attacks and design methodology for cryptographic processors.

Tatsuya Fujii received the B.S. and M.S. degrees from The University of Electro-Communications (UEC), Tokyo, Japan in 2016 and 2018, respectively. During his degrees, he was involved in a research project, and in charge of security analysis of fault-injection attacks against cryptographic processors. He is currently with Anritsu Corp., Atsugi, Japan.

Natsu Shoji received the B.E. degree in Informatics from The University of Electro-Communications (UEC), Tokyo, Japan, in 2018. She is currently a graduate student pursuing a Master's degree at the department of Informatics, UEC, and working on hardware security, especially focusing on security evaluation for physical attacks.



Takeshi Sugawara received B.E., M.Is., and Ph.D. degrees from Tohoku University, Japan, in 2006, 2008, and 2011, respectively. In 2011, he joined Mitsubishi Electric Corporation. He is currently an Associate Professor at The University of Electro-Communications, Tokyo since 2017. His research interests include cryptography, side-channel analysis, and analog cybersecurity.

Kazuo Sakiyama (S'06–M'07–SM'16) is a professor at The University of Electro-Communications (UEC), Tokyo, Japan. At UEC, he leads the hardware security research for embedded cryptosystem, cyber-physical system, and physical authentication. Before joining UEC in 2008, he worked for Hitachi, Ltd., Japan (now Renesas Electronics) as a digital hardware designer, and later at Katholieke Universiteit Leuven (KU Leuven), Belgium as a Ph.D. research assistant. He received the B.E. and M.E. degrees from Osaka University, Japan in 1994 and 1996, respectively, the M.S. degree from The University of California, Los Angeles (UCLA) in 2003, and the Ph.D. degree in electrical engineering from KU Leuven, Belgium in 2007. He is a member of IACR, IEICE and IEEE.

Yu-ichi Hayashi (M'12) received the M.S. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2005 and 2009, respectively. He is currently a Professor in the Graduate School of Information Science, Nara Institute of Science and Technology, Nara, Japan. His research interests include electromagnetic compatibility and information security. Dr. Hayashi is the Chair of EM Information Leakage Subcommittee in IEEE EMC Technical Committee 5.

Makoto Nagata (S'95–M'02–SM'07) received the B.S. and M.S. degrees in physics from Gakushuin University, Tokyo, Japan, in 1991 and 1993, respectively, and the Ph.D. degree in electronics engineering from Hiroshima University, Hiroshima, Japan, in 2001.

From 1994 to 2002, he was a Research Associate with Hiroshima University. He was an Associate Professor with Kobe University, Kobe, Japan, from 2002 to 2009, where he promoted to a Full Professor in 2009, and currently a Professor with the Graduate School of Science, Technology and Innovation. His current research interests include design techniques toward high performance mixed analog, RF, and digital VLSI systems with particular emphasis on power/signal/substrate integrity and electromagnetic compatibility, testing and diagnosis, 3-D system integration, as well as their applications for hardware security and safety.

Dr. Nagata has been a member of a variety of Technical Program Committees of international conferences such as the Symposium on VLSI Circuits from 2002 to 2009, Custom Integrated Circuits Conference from 2007 to 2009, Asian Solid-State Circuits Conference from 2005 to 2009, and International Solid-State Circuits Conference from 2014 to 2017. He is a Senior Member of IEICE. He was a co-recipient of the Best Paper Awards from the IEEE 3D-Test 2013, IACR CHES 2014, and IEEE APEMC 2015. He is the Chair of Technology Directions Subcommittee for International Solid-State Circuits Conference. He was a Technical Program Chair from 2010 to 2011 and a Symposium Chair from 2012 to 2013 for Symposium on VLSI circuits. He has been an Associate Editor of the IEEE TRANSACTIONSON VLSI SYSTEMS since 2015, and also a Chair for the IEEE SSCS Kansai Chapter since 2017. He also served as an Associate Editor for the IEICE TRANSACTIONS ON ELECTRONICS from 2002 to 2005.

Noriyuki Miura (S'06–M'08) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Keio University, Yokohama, Japan, in 2003, 2005, and 2007, respectively. From 2005 to 2008, he was a Research Fellow with the Japan Society for the Promotion of Science and since 2007 an Assistant Professor with Keio University, Yokohama, Japan, where he was involved in short-range wireless transceiver circuit design and wireless interconnect technology for 3-D system integration. He is currently an Associate Professor with Kobe University, Kobe, Japan, working on hardware security, smart sensor design, and heterogeneous integration. He has authored over 100 technical publications, including four invited papers and three book chapters. Dr. Miura was a recipient of the Top ISSCC Paper Contributors from 2004 to 2013, the IACR CHES Best Paper Award in 2014, and IEICE Suematsu Yasuharu Award in 2017. He is a member of IEICE and a Secretary of the IEEE SSCS Kansai Chapter. He is currently serving as a Technical Program Committee (TPC) Member for A-SSCC and Symposium on VLSI Circuits. He served as the TPC Vice Chair of 2015 A-SSCC.