Japanese Journal of Applied Physics

REGULAR PAPER • OPEN ACCESS

An IC-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density

OPEN ACCESS

Japanese Journal of Applied Physics **59**, SGGL02 (2020) **REGULAR PAPER**

https://doi.org/**10.7567/1347-4065/ab65d3**

An IC-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density

Kohei Matsuda[1*], Sho Tada[2], Makoto Nagata[2], Yuichi Komano[3], Yang Li[4], Takeshi Sugawara[4], Mitsugu Iwamoto[4], Kazuo Ohta[4], Kazuo Sakiyama[4], and Noriyuki Miura[1*]

[1]*Graduate School of System Informatics, Kobe University, Kobe, Hyogo 657-8501, Japan*
[2]*Graduate School of Science, Technology, and Innovation, Kobe University, Kobe, Hyogo 657-8501, Japan*
[3]*Corporate R&D Center, Toshiba Corporation, Kawasaki, Kanagawa, 212-8582, Japan*
[4]*Department of Informatics, The University of Electro-Communications, Chofu, Tokyo 182-8585, Japan*

[*]E-mail: k_matsuda@cs26.scitec.kobe-u.ac.jp; miura@cs.kobe-u.ac.jp

Received September 30, 2019; revised December 5, 2019; accepted December 27, 2019; published online February 28, 2020

Laser fault injection (LFI) attacks on cryptographic processor ICs are a critical threat to information systems. This paper proposes an IC-level integrated countermeasure employing an information leakage sensor against an LFI attack. Distributed bulk current sensors monitor abnormal bulk current density caused by laser irradiation for LFI. Time-interleaved sensor operation and sensitivity tuning can obtain partial secret key leakage bit information with small layout area penalty. Based on the leakage information, the secret key can be securely updated to realize high-availability resilient systems. The test chip was designed and fabricated in a 0.18 μm standard CMOS, integrating a 128-bit advanced encryption standard cryptographic processor with the proposed information leakage sensor. This evaluation successfully demonstrated bulk current density and leakage bit monitoring. © 2020 The Japan Society of Applied Physics

1. Introduction

In the era of the Internet-of-Things (IoT), information security is one of the most critical technical issues where a tremendous number of sensor devices pervade our daily life and autonomously collect and share sensitive information. Cryptographic processing is a critical component for preserving the confidentiality of such sensitive information (Fig. 1). The cryptographic algorithms widely used today are all developed to resist theoretical cryptanalysis. However, physical attacks on cryptographic processor ICs can break security holes and have recently become a serious security threat.[1)]

A side-channel attack is one of the most well-known physical attacks in which the secret key information embedded in cryptographic ICs is revealed by analyzing physical side-channel leakage (e.g. power consumption, electromagnetic radiation).[2,3)] Fault analysis (FA) is known as a more powerful physical attack scheme where intentional and temporary faults are injected during cryptographic operation (Fig. 1). The attacker utilizes the associated faulty ciphertext output to analyze and then reverse-calculate the secret key information. This attack becomes a serious threat, especially in the coming IoT era where the accessibility of pervasively distributed devices would be increased for the attackers.

The fundamental theory of FA was first proposed on a public-key cipher RSA in 1997 by Boneh, DeMillo, and Lipton,[4)] and on a symmetric-key cipher data encryption standard in the same year by Biham and Shamir.[5)] In both attacks, the pairs of correct and faulty ciphertext were collected and analyzed based on the fault model of the target cipher algorithm to disclose the secret key information, namely differential fault analysis (DFA). Later, in 2001, Piret and Quisquater applied DFA to a de facto standard cipher advanced encryption standard (AES).[6,7)] There have been various other active projects conducted on an AES, researching how to reduce the attacker's calculation cost.[8–11)] Li et al. in 2010 proposed fault sensitivity analysis (FSA) where the secret information can be revealed by only analyzing the threshold (sensitivity) of the fault occurrence.[12)] No pairs of faulty and correct ciphertext are needed in this attack, but detailed information of the circuit implementation is needed. Moradi et al. enhanced this FSA by combining it with side-channel analysis[13,14)] where even detailed circuit information is not needed. The above-mentioned theoretical research helps make FA of practical use.

In practice, there are many variations in physical fault injection approaches.[15)] Among these approaches, laser fault injection (LFI)[16)] is known as one of the most powerful physical attacks. The attacker injects a temporal fault during a cryptographic operation by using a laser module. The calculation cost of FA can be greatly reduced by the precise control of the fault injection timing and position of the laser. Compared to other injection approaches such as over-clocking, supply voltage perturbation, and electro magnetic (EM) injection, LFI has the highest time and space resolution for the most efficient attack capability.

As a countermeasure against FAs, doubling and verification[17,18)] can be considered to be a simple solution. In a spatial doubling scheme, redundant cryptographic processors are integrated and each of the outputs are verified to detect single fault injection. Or, in the temporal doubling approach, both encryption and decryption are performed sequentially to check the consistency of the operation. However, in either countermeasure, more than doubling the hardware overhead in power or area would inevitably be a burden. In addition, these countermeasures can be easily bypassed by multiple laser injection.[19)] There are clear limitations in cost and security level for these logic-level countermeasures.

Another approach would be a physical-level countermeasure. Top-layer metal shielding is one approach to physically protect

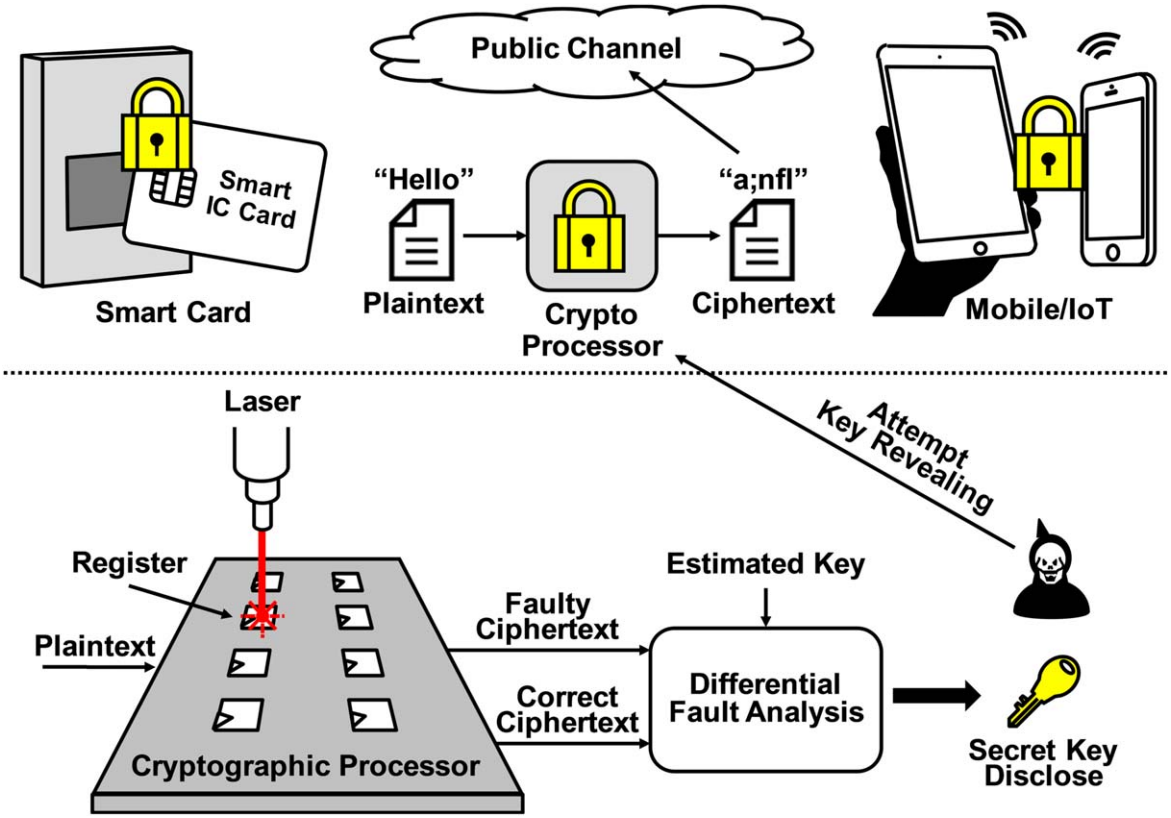

Fig. 1. (Color online) Smart devices using cryptographic processors, and a laser fault injection attack against these devices.

the cryptographic core from laser irradiation.[20] The hardware overhead is only one single metal layer with effectively no area penalty. However, it is only effective against front-side LFI. Back-side LFI utilizing an NIR laser can bypass this metal shield because an NIR laser can penetrate the Si IC substrate.[21] A physical sensor-based approach is one powerful countermeasure against LFI. It detects physical disturbance due to LFI, typically in either temperature or light illuminance[22] and has the capability to disable both back-side and multiple LFI. The technical challenge is in how to implement the sensor with a small area and how to react upon detection of an attack. Conventional temperature or photo-sensor implementations[22] result in huge area penalties because a dense sensor array arrangement is needed to protect the entire cryptographic core from focused laser irradiation spots. In addition, not much discussion has taken place of the response after attack detection. Recently, a compact sense-and-react IC-level countermeasure has been proposed.[23] Unlike in the photo-sensor, abnormal opto-electric bulk current is detected. Since this current spreads over the Si bulk substrate, a sparse sensor array arrangement is possible for 100% detection coverage of the entire cryptographic core with a small area overhead. However, this sensor only detects whether the cryptographic core is under attack or not. The only possible reaction is to disable (halt) the cryptographic operation to protect the key, which significantly degrades its availability.

This paper extends the conventional sense-and-react countermeasure[23] by introducing the capability to detect a partial secret key bit at risk of leakage. This so-called information leakage sensor[24] enables a secure key update (or key distillation) to continue even after the LFI attack for highly available resilient cryptographic systems (Fig. 2). The rest of this paper is arranged as follows. In Sect. 2, the LFI mechanism and the operation principle of the bulk current sensor will be briefly reviewed. In Sect. 3, details of the proposed information leakage sensor will be described. In Sects. 4 and 5, the experimental setup and results will be presented for the proof-of-concept of the proposed sensor. In Sect. 6, resilient cryptographic systems based on the information leakage sensing will be discussed. Finally, in Sect. 7, concluding remarks will be made.

2. Bulk current sensor

2.1. The LFI mechanism

LFI is based on the same mechanism as that of soft errors in ICs, a classic well-known problem since the early 1960s.[25] A temporal bit flip occurs accidentally in an IC memory due to an incident cosmic ray. In 1965, Habing actually employed a laser to emulate the soft error phenomenon in ICs.[26] In LFI, the attacker exploits a strong laser to inject an intentional fault with time- and space-controlled bit flip.[16,19,21,27] In addition, it is known that a recently scaled CMOS device becomes more vulnerable to soft error.[28] LFI would also become a more critical threat in a scaled CMOS.

Figure 3 depicts the detailed mechanism of LFI for a register with "Low" data stored. The bit flip occurs when the laser irradiates a drain of an off-state transistor, in the case of Fig. 3, the N-channel metal oxide semiconductor (NMOS) M_{NT} in INV_T. Due to the laser injection, electron–hole pairs are generated at the PN junction of the drain. Since this drain is biased at a "High" supply voltage V_{DD}, there exists a potential slope between the drain and the substrate biased at a "Low" ground voltage V_{SS}. The generated electrons (holes) flow due to this potential slope and this generates transient

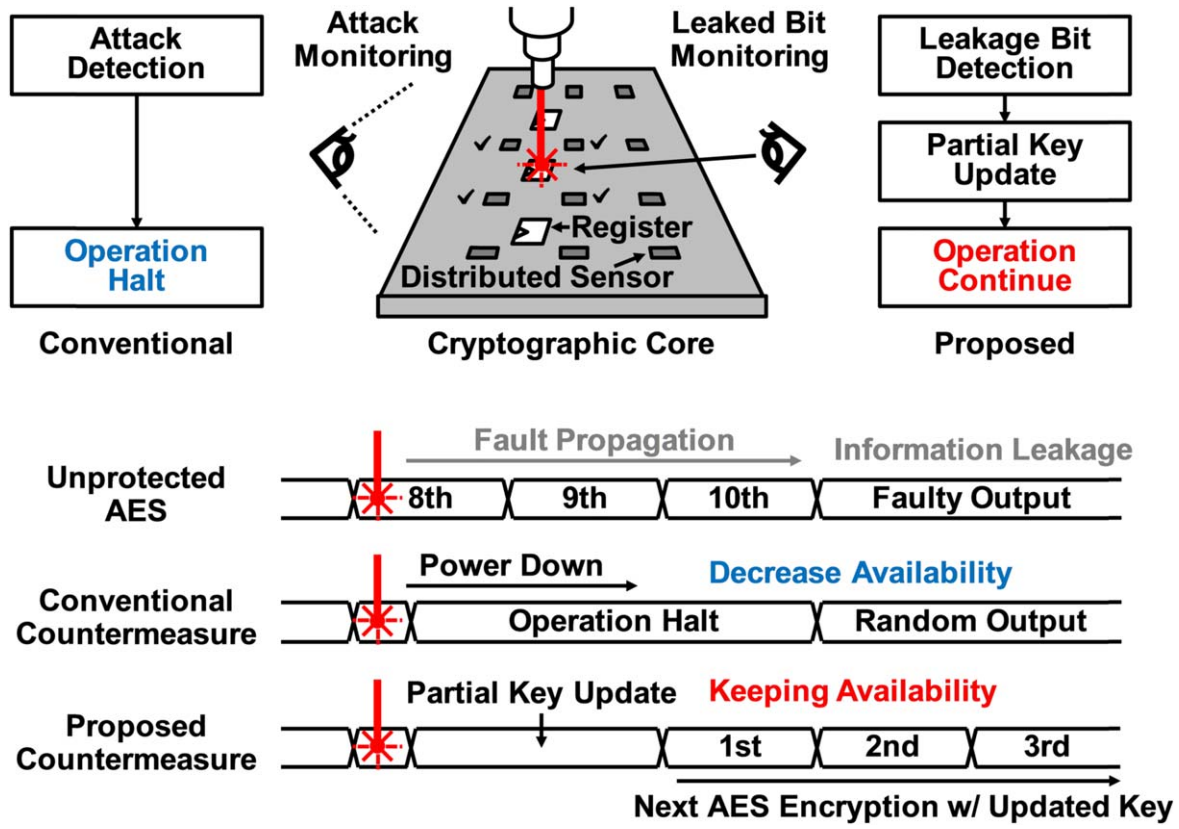

Fig. 2. (Color online) Conceptual sketch of the proposed information leakage sensor against an LFI attack.

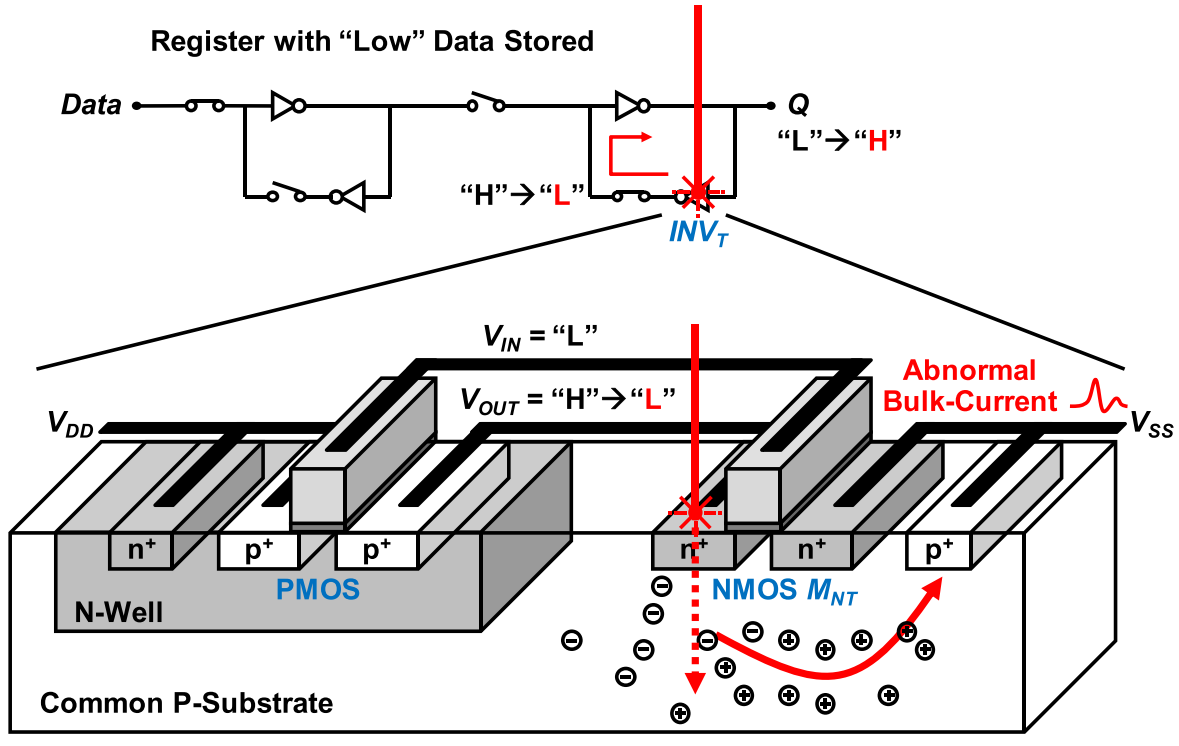

Fig. 3. (Color online) Mechanism of a temporary bit error caused by laser irradiation.

bulk current. (In the on-state case, there is no potential slope and hence no bulk current is generated even with the laser injection). This bulk current discharges the drain node voltage and causes temporal bit flip. This is a so-called single event upset in the soft error research field.

2.2. Sensor operation principle

The bulk current sensor was first developed by Neto et al. in 2006 for soft error detection.[29] Later, in 2015, Champeix et al. modified the sensor for the detection of laser injection.[30] Figure 4 shows the circuit schematic and its

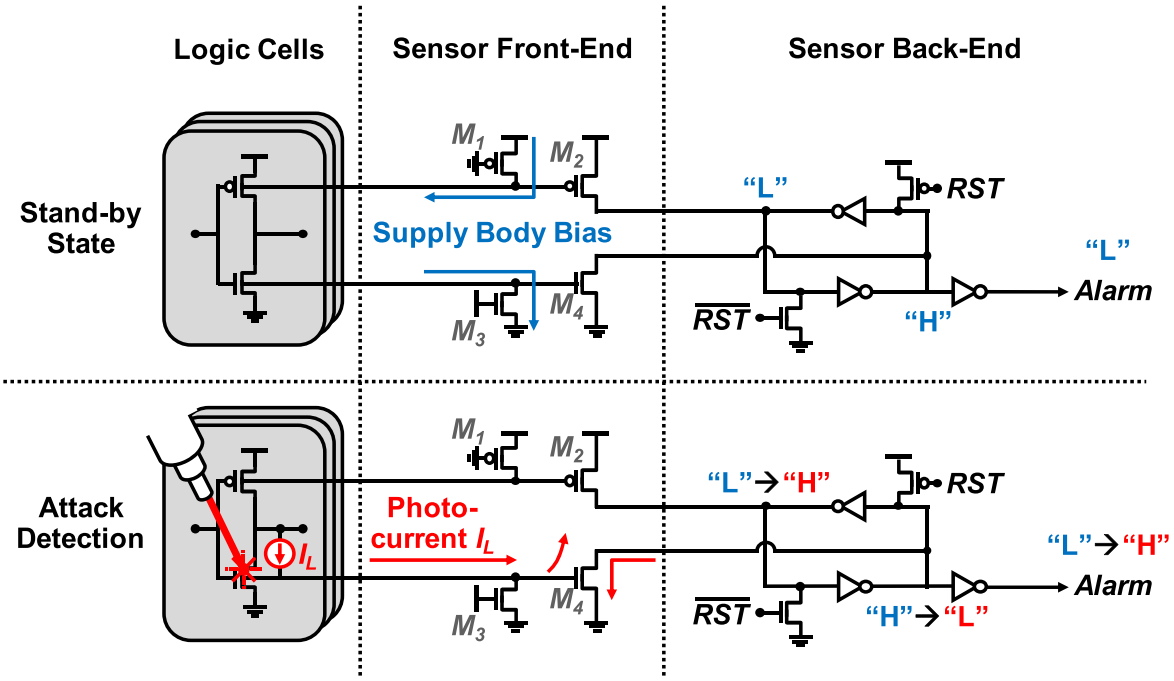

Fig. 4. (Color online) Soft error detection mechanism of the bulk built-in current sensor.

operation principles. As mentioned in the previous section, the laser-induced bulk current can be seen as an abnormal current flow from the drain to the bulk. The bulk current sensor converts this current into voltage and then raises an alarm on LFI detection. The sensor therefore consists of two blocks: the sensor front-end for the current to voltage conversion, and the back-end for the digital *Alarm* signal generation. The front-end is a simple resistor-based converter with an always-on transistor. The drain as the input of the front-end is connected to the bulk of the logic-cell transistors. The always-on transistor gives the bulk bias for the logic in a normal operation state. When the laser is induced and the bulk current is generated, the always-on transistor acts as a resistor to convert the current into voltage. The succeeding common-source stage amplifies this voltage and drives the back-end. The back-end consists of a simple pre-charged cross-coupled inverter latch which generates the digital *Alarm* signal upon the front-end activation. The sensor circuit is composed of only 12 transistors and no active stand-by current consumption, resulting in a small area and almost no power overhead penalty.

3. Information leakage sensor

In the recently published sense-and-react countermeasure,[23] the legacy bulk current sensors are simply arranged in a 2D array. The distributed sensors can obtain information only of the attack event occurring, but no detailed information on where and how strong the attack is. In this work, the sensor circuit and architecture are modified to detect the position and strength of the LFI attack. Namely, this information leakage sensor can obtain information on the partial bit at risk of leakage. The key circuit techniques are (1) time-interleaving operation of the arrayed sensor front-ends, and (2) sensitivity tuning in the sensor back-end. Figure 5 shows a schematic of

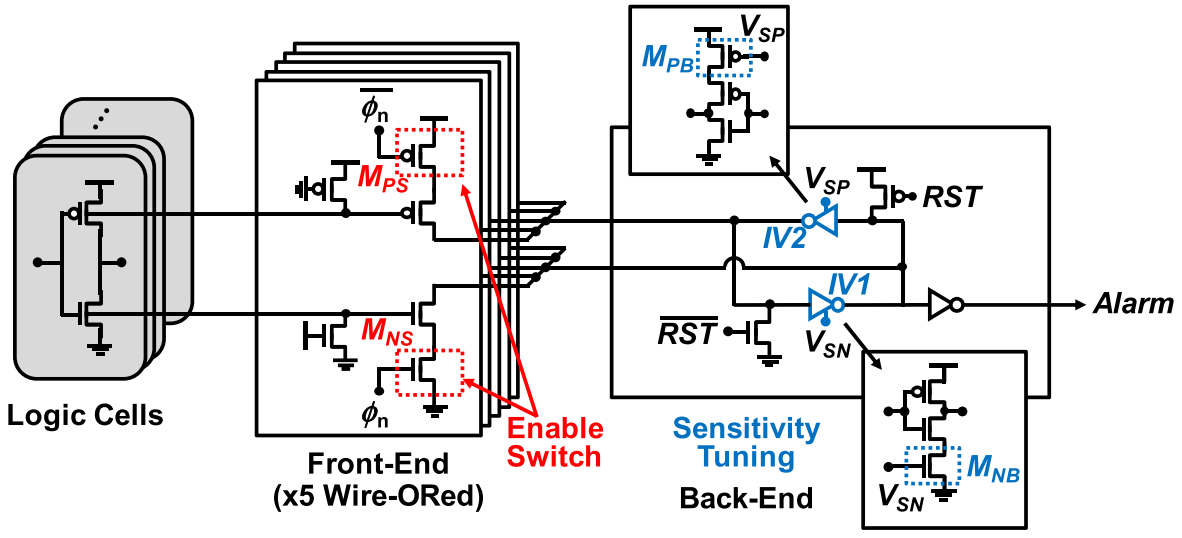

Fig. 5. (Color online) Schematic of proposed information leakage sensor.

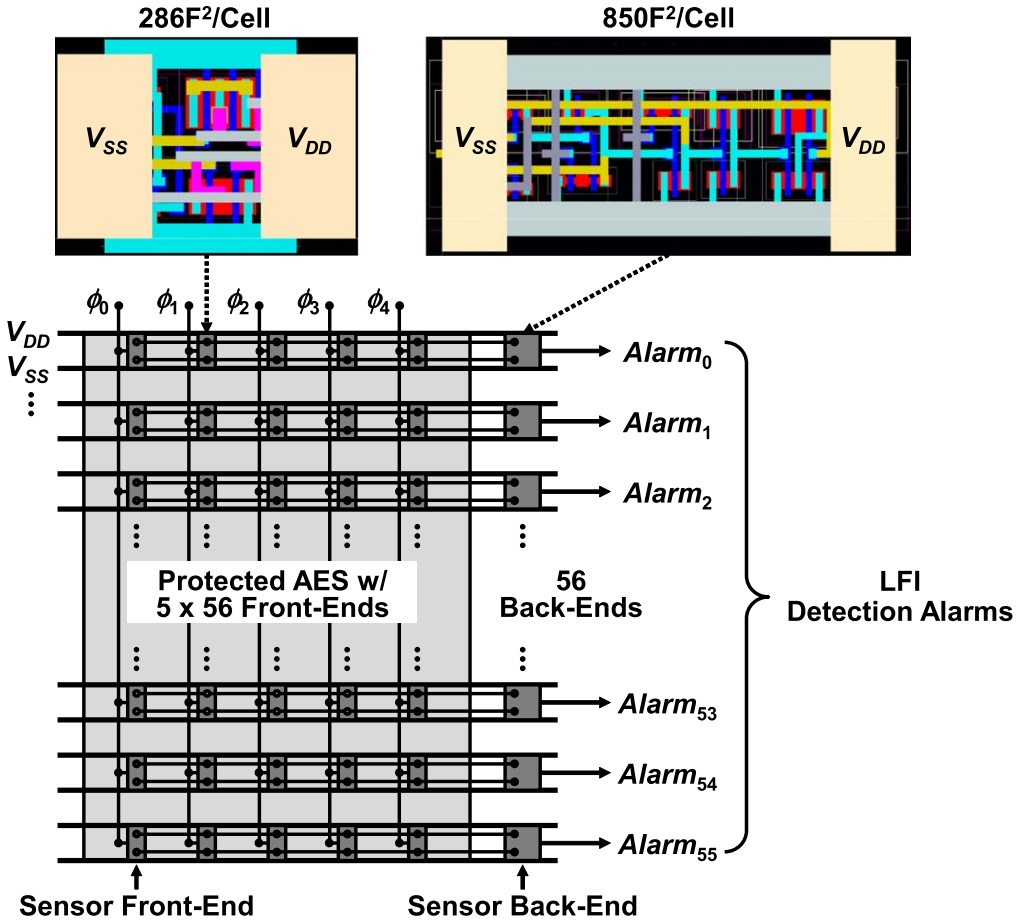

Fig. 6. (Color online) Implementation of a protected AES processor integrated with the proposed information leakage sensors.

the proposed sensor. The core circuit is based on the legacy sensor.[30] Outputs of n arrayed sensor front-ends are wire-ORed together and connected to the input of one sensor back-end to build one sensor block. The sensor blocks are again arranged to cover the entire cryptographic core for protection. In the sensor front-end, two enable switches M_{PS} and M_{NS} are newly added for the time-interleaving operation. By multi-phase clocks ϕ_n, an active front-end can be selected among the wire-ORed sensors to detect the LFI spot and hence partial leakage bit information. Compared to a fully parallel access scheme, the number of required sensor back-ends and interconnection resources for the front-end outputs can be significantly reduced for area saving. Since the circuit designer has knowledge of both the registers' and sensor front-ends' positions, the sensor can estimate the bit error positions based on this geometric information. The partial secret key bit position at risk of leakage can then be calculated for the proper key update process. In the sensor back-end, tail-bias transistors M_{PB} and M_{NB} are newly added for sensitivity tuning. The threshold voltage to raise the *Alarm* can be controlled by the bias voltage of these transistors: V_{SP} for tuning the *Alarm* threshold when the NMOS is under LFI and V_{SN} for P-channel metal oxide semiconductor (PMOS). The sensitivity tuning realizes precise LFI spot detection. In the case of strong laser irradiation, it is difficult to specify the actual laser spot precisely without sensitivity tuning because many neighboring sensors raise the *Alarm*. By sweeping V_{SN} and V_{SP}, the actual laser spot can be narrowed down and the targeted registers can be distinguished precisely.

In order to design the sensor sensitivity tuning range properly at the design stage, estimation of the laser-induced photocurrent is important. Si photo-electric reactions of an NIR laser beam have been modeled in Refs. 25 and 31–33. The peak amplitude of laser-induced photocurrent I_{Ph_peak} can be modeled as

$$I_{Ph\_peak} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_{\omega} \times S, \quad (1)$$

where V is the reverse-biased voltage of the exposed PN junction, a and b are process-dependent photo-electric conversion factors, $\alpha_{gauss(x,y)}$ is a term related to the bivariate normal distribution of the laser beam amplitude in space, $Pulse_{\omega}$ is a laser pulse duration and S is the area footprint of the PN junction. The minimum I_{Ph_peak} required to induce the temporary bit flip (i.e. fault) can be estimated by circuit simulation of the register with the equivalent laser current model I_L, such as in Fig. 4 (~0.5 mA in a 0.18 μm CMOS register[34]). For a chip designer who can access the process parameters a and b, the relationship between fault and minimum laser energy can be theoretically calculated using Eq. (1). However, generally a fabless chip designer cannot obtain the process-dependent a and b values because confidential device parameters (e.g. depletion area width, carrier density, etc) are needed to calculate these parameters. To solve this problem, circuit simulation with an equivalent laser current model and preliminary direct register device measurement of photo-electric characterization with a simple test element group should be employed to directly measure the minimum laser energy for the bit flip.[34]

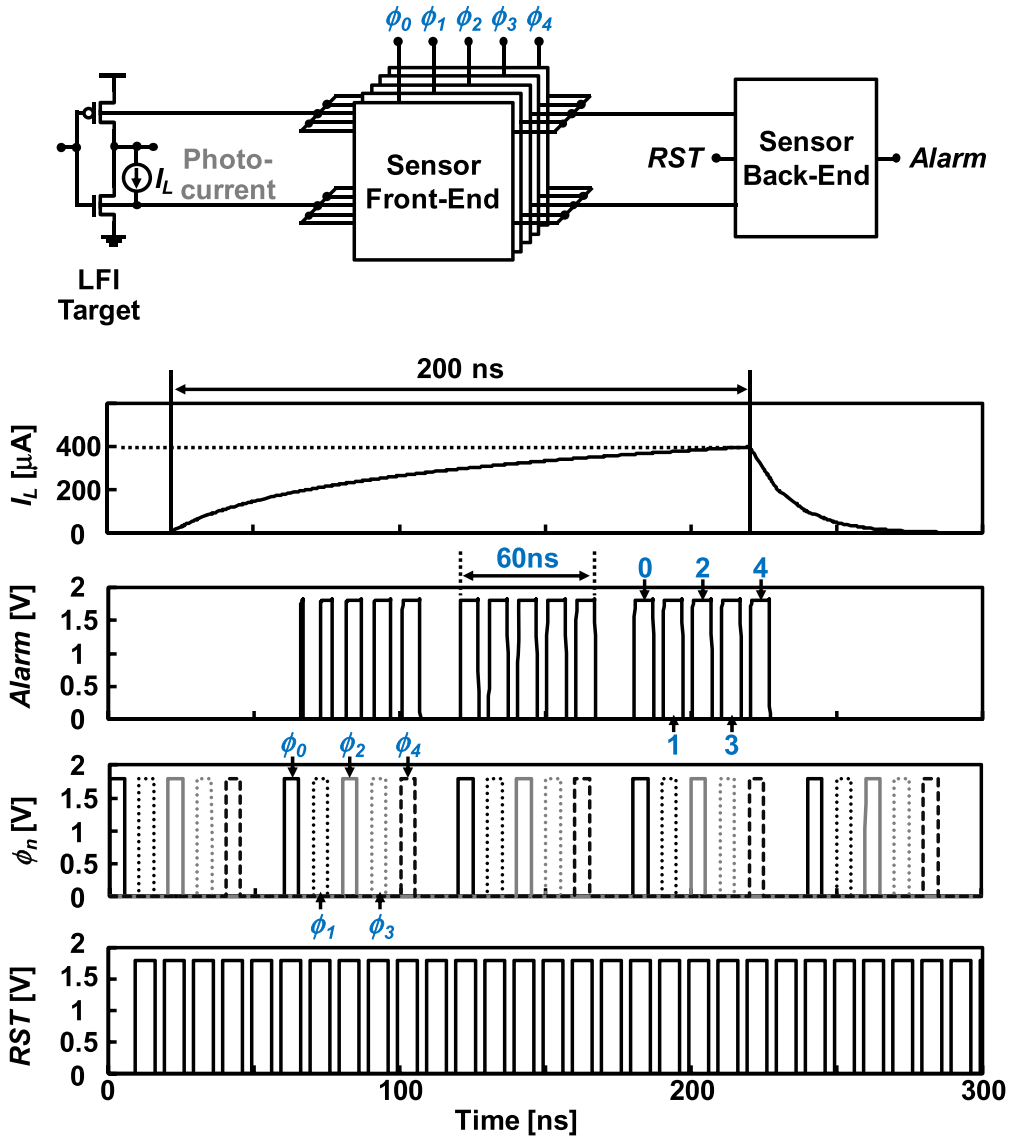

Fig. 7. (Color online) Simulated results of time-interleaving sensor operation.

For the prototype demonstration, a 128-bit AES cryptographic processor was designed together with the proposed information leakage sensor in a 0.18 μm standard CMOS (Fig. 6). A commercial electronic design automation (EDA) toolchain was used and no analog process options were needed for the design. In the protected processor, 5×56 sensor front-ends and 56 back-ends are integrated. The example layout of the proposed sensor front-end and back-end are also presented in Fig. 6. The layout area of the front-end is only 286 F^2/cell (~2.6 gate equivalent of two-input NAND) and that of the back-end 850 F^2/cell (~7.7 gate equivalent). The total layout area penalty can therefore be suppressed significantly. Thanks to these tiny sensor circuits and sparse sensor arrangement, the total area overhead is only +23% compared with the unprotected AES processor. The horizontal placement interval between sensor front-ends was set to 60 μm based on preliminary characterization.[34] Since the bulk current is spread over the Si substrate, 100% detection coverage can be realized even with such a sparse sensor arrangement. Five front-ends were placed in the same row and connected to one back-end. All sensor outputs are scanned within five steps by triggering ϕ_0 to ϕ_4 signals sequentially. Figure 7 presents the simulated waveforms of this sensor output scanning process. I_L represents the emulated photocurrent caused by LFI with 200 ns duration. ϕ_0 to ϕ_4 signals are triggered sequentially together with the reset signal *RST*. It was confirmed that a corresponding sensor is activated and the *Alarm* is successfully raised. Moreover, it was also confirmed that five sensor outputs can be scanned within only 60 ns. Figure 8 shows simulated results of sensor sensitivity tuning. I_{LN} and I_{LP} represent the photocurrent caused by LFI on the NMOS and PMOS, respectively. These simulations evaluate the minimum photocurrent with *Alarm* raising as the sensor sensitivity. By sweeping the V_{SP}, sensor sensitivities can be controlled within 20 μA, and V_{SN} within 60 μA.

This proposed information leakage sensor is fully compatible with standard CMOS technology. No additional process options such as a triple well are needed for sensor implementation. Since the sensor detects laser-induced bulk current, the proposed technique can be easily applied to any kind of bulk-based CMOS process. In in field-effect transistor technologies, since the charge-collection efficiencies decrease with decreasing transistor size and increasing doping densities,[35] the

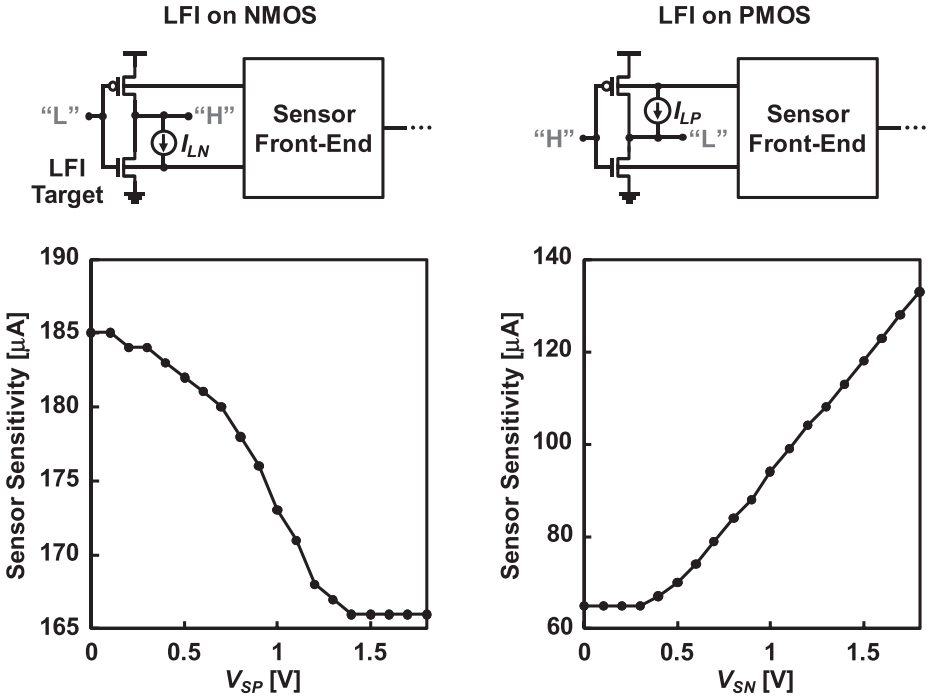

Fig. 8. Simulated results of sensor sensitivity tuning.

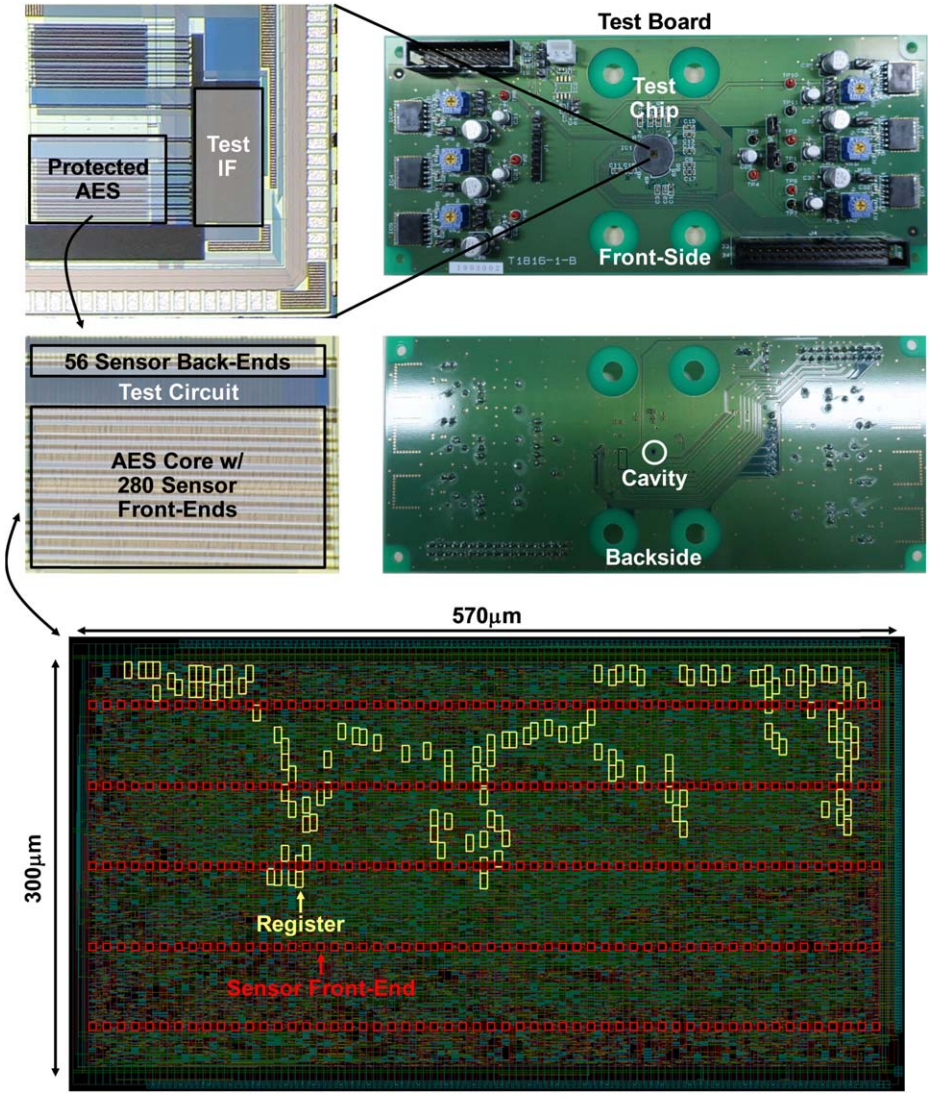

Fig. 9. (Color online) Photograph of the test chip and evaluation board.

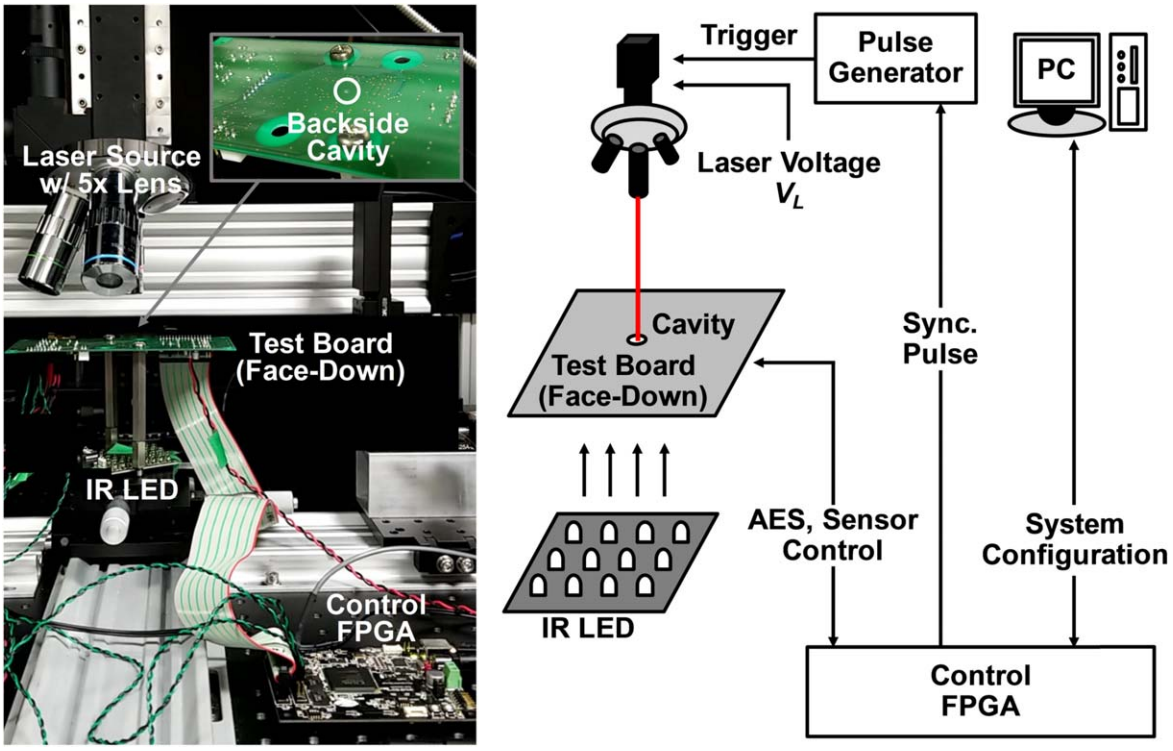

Fig. 10. (Color online) Measurement system setup.

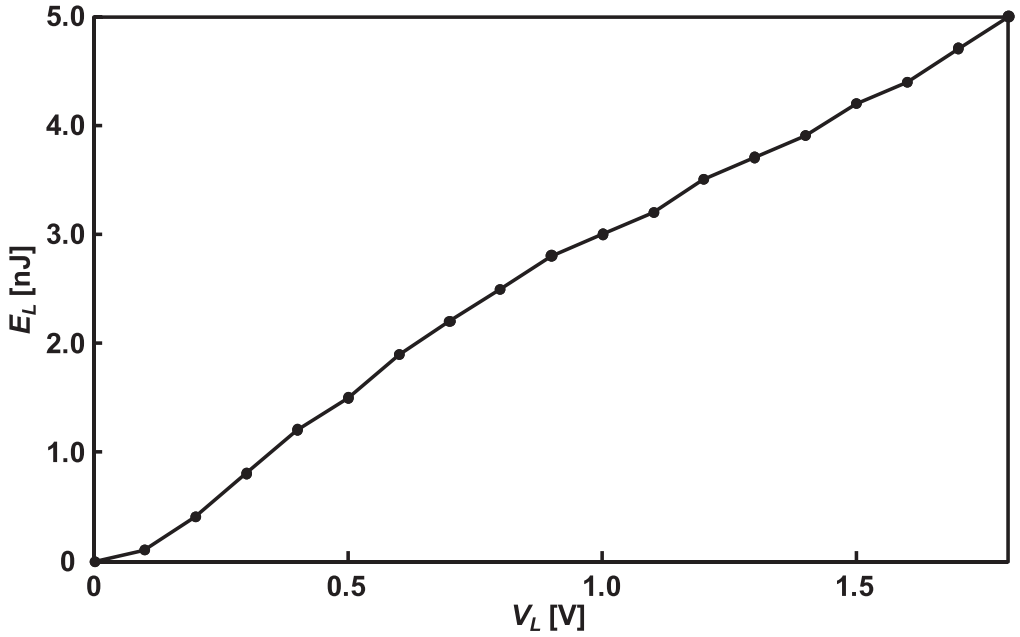

Fig. 11. Measured relationship between laser control voltage V_L and laser energy E_L.

device becomes more robust against both soft error and fault injection. The associated bulk photocurrent and its spread range might be reduced accordingly. The sensor array density and sensitivity should be tuned based on the preliminary testing of photo-electric characteristics of each process.

4. Experimental setup

For the proof-of-concept, the test chip was fabricated in a 0.18 μm standard CMOS. Figure 9 shows photographs of the test chip and test board for evaluation. The protected 128-bit AES processor and test interface circuits are mounted on the test chip. Test chip input/output pads are connected to the test board with wire-bonding. For stable measurement, the test chip is molded by resin except for the chip surface. Additionally, the test board has a small back-side cavity for back-side LFI evaluation.

Figure 10 shows the measurement system setup. The test board is fixed face-down under an NIR laser source of 970 nm wavelength. In this evaluation, the laser spot was focused down to 20 μm through a 5$\times$ magnification lens for precise measurement of fault injection. Also, precise laser position control with 1 μm steps in the *X*-, *Y*-, and *Z*-directions contributed to accurate position setting and to securing the repeatability of measurements. In this

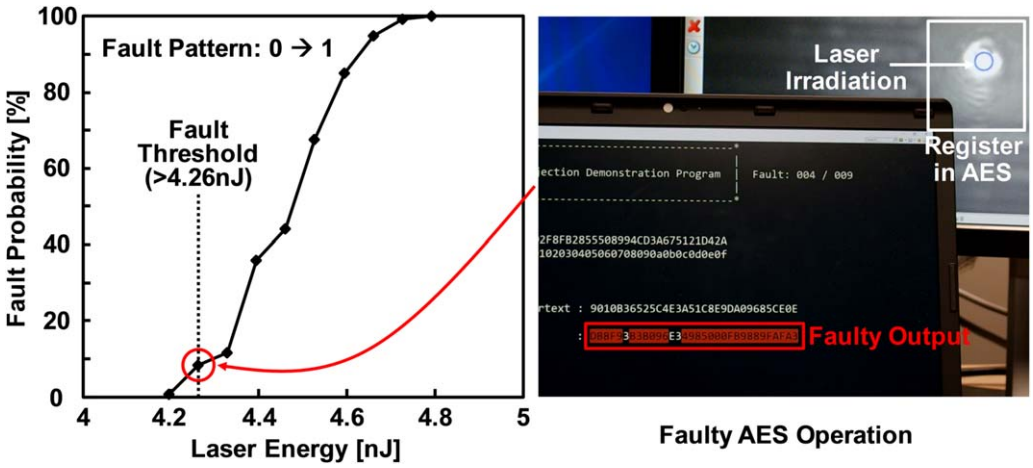

Fig. 12. (Color online) Measured fault probability and LFI demonstration.

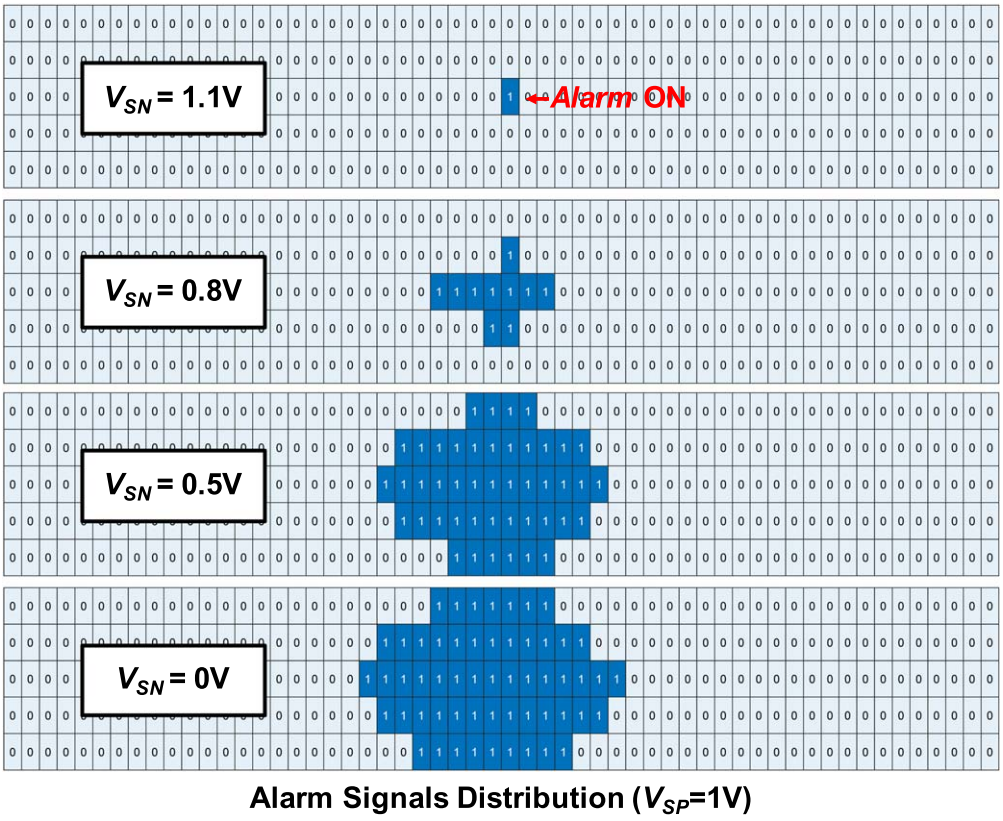

Fig. 13. (Color online) Measured sensor output distribution depending on sensitivity tuning voltage V_{SN}.

evaluation, the laser pulse width was set to 200 ns. To capture chip back-side images through the microscope, an IR LED board was utilized. Control signals for the test chip and the laser trigger were generated in the control field-programmable gate array for precise and arbitrary fault injection on AES operation. The laser energy E_L could be linearly controlled by the laser diode bias voltage V_L as shown in Fig. 11.

5. Measurement results

For a preliminary characterization, a fault probability was evaluated by LFI on the 0.18 μm CMOS AES processor (Fig. 12). In this evaluation, "fault" means incorrect cryptographic operation due to temporal data bit flip by the laser irradiation, and "fault probability" means the probability of this temporary bit flip occurring. The *X*-axis and *Y*-axis represent laser energy and fault probability, respectively. In this evaluation, the register with "Low" data stored was targeted by the laser. The fault probability increased gradually with increasing laser energy. When the laser energy exceeded 4.26 nJ, the temporal fault started to occur and the faulty ciphertext could be successfully obtained, as shown in Fig. 12. The sensitivity of the information leakage sensor should be designed to be high enough to detect this 4.26 nJ laser energy injection with a safe margin. Based on this preliminary characterization and the circuit simulation, the sensor sensitivity range can be properly adjusted, and robust sensor design and configuration can be realized without confidential device parameters.

The effectiveness of the time-interleaved sensor operation and the sensitivity tuning were evaluated. Figure 13 presents

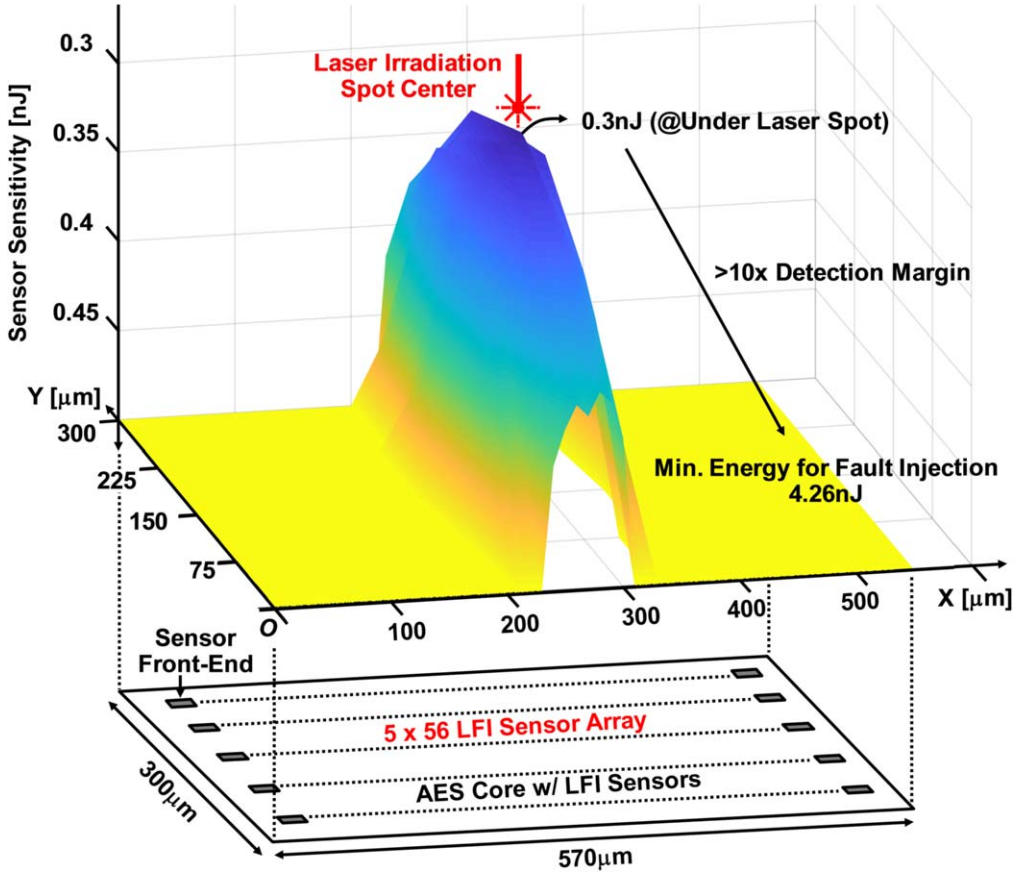

Fig. 14. (Color online) Measured sensor sensitivity distribution.

Table I. Comparison table of area overhead.

Component	This work (0.18 μm CMOS)		[18] (0.13 μm CMOS)
	Unprotected	Protected	
AES Core	0.140 mm^2	0.168 mm^2(+20%) (w/Sensor Front-End)	—
Sensor Back-End	—	0.0045 mm^2	—
Total	0.140 mm^2	0.1725 mm^2 (+23%)	(+104%)

the *Alarm* signal distribution in the 2D sensor array. In this measurement, the laser spot is fixed to the center of the protected AES core, and the register values were set to "Low". To evaluate "Low" to "High" fault injection, V_{SP} was fixed at 1 V and V_{SN} was swept from 0 V to 1.1 V. The laser control voltage was also fixed at 0.188 V. A dark blue box represents the sensor position with the *Alarm* signal raised, and light blue not raised. When V_{SN} is set to 0 V, the sensor sensitivity becomes highest and a lot of sensors raised the *Alarm*. By contrast, when V_{SN} is 1.1 V, only the sensor placed near the laser spot raised the *Alarm*. With appropriate control of sensor sensitivity, the laser irradiation spot can be detected. By sweeping the sensor sensitivity, a 3D heat map of the bulk current spread could be visualized, as shown in Fig. 14. In this evaluation, the minimum laser energy at which the sensor raises the *Alarm* signal in each sensor was measured. This minimum laser energy is denoted the sensor sensitivity. The sensor sensitivity was measured by sweeping the laser energy with a fixed laser irradiation spot at the center of the protected AES processor. In this measurement, V_{SN} and V_{SP} were set to 0 V and 1.0 V, respectively. The vertical scale represents sensor sensitivity, and the *X*- and *Y*-axes represent the region of the protected AES processor including the 5 × 56 sensor front-end arrays (the gray boxes illustrate the front-ends' positions). As shown in Fig. 13, the minimum laser energy for fault injection was 4.26 nJ. Based on the 3D heat map results, the proposed information leakage sensor at the laser irradiation spot can raise the *Alarm* by detecting >0.3 nJ laser energy injection. This guarantees a >14 × safety detection margin against the minimum 4.26 nJ laser irradiation for the fault injection. Other multiple sensors located near the spot could also raise the *Alarm* with a >10 × margin for secure protected operation against LFI attack.

Table I compares the area overhead of the protected and unprotected AES cores and the prior art.[18] The layout area overhead of the protected AES core integrated with the 280 information leakage sensor front-ends is +20% that of the unprotected core. The total area overhead including sensor back-ends is only +23%. This is much smaller than that of the prior art (+104%) where two AES cores are needed for doubling and verification. In addition, the proposed leakage sensor does not consume any active standby power during normal cryptographic operation. There is almost no power overhead burden with the proposed technique, while the prior art power overhead was double.[18]

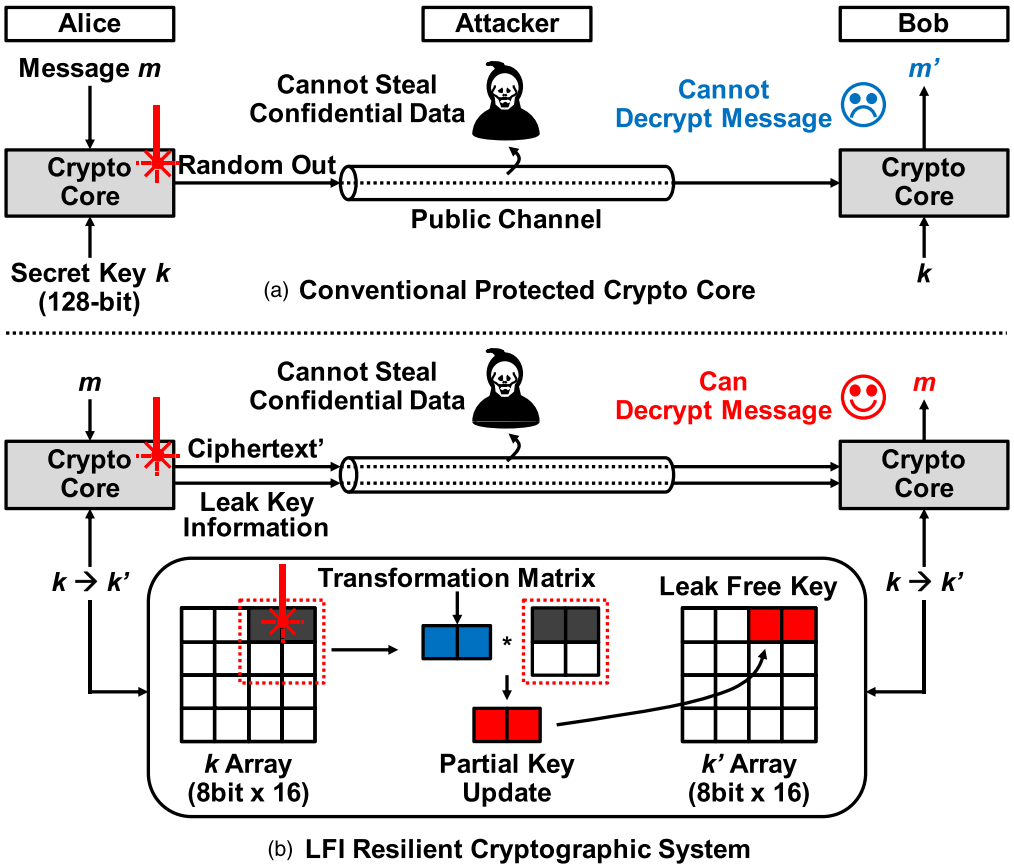

Fig. 15. (Color online) Concept of a resilient cryptographic system using partial key update.

6. Discussion on a resilient cryptographic system

With the obtained knowledge of the partial leakage bit information, an LFI-resilient cryptographic system with secure key update after the attack can be realized. Compared to the conventional countermeasure with immediate system halt after the attack[23] [Fig. 15(a)], a secure continuous operation becomes possible, enhancing availability. A similar concept can be seen in a re-keying scheme as a side-channel attack countermeasure.[36] Medwed et al. introduced a "separation of duties" approach.[37] This generates a session key from a master secret key in a secure way without any side-channel leakage, and this session key is then used for encryption. Since the session key is frequently updated, the encryption can be performed with a cryptographic processor unprotected against side-channel attack. There are several other improved schemes proposed in this re-keying scheme.[38,39]

In this paper, the key update scheme can be drastically simplified based on the detailed leakage bit information obtained by the sensor. The core idea is based on a theoretical study.[40] Figure 15(b) presents the concept of our proposed LFI-resilient cryptographic system with the information leakage sensor. After LFI attack detection, the secret key k is immediately updated to k' by only one-step matrix multiplication between the partial leakage bits and the rest of the secret key bits. The secure key update is possible even if the attacker has knowledge of the leakage bit positions and the update rule (i.e. transformation matrix) because the secret key is unknown to the attacker. The key update between Alice and Bob can be synchronized by sharing the matrix and the positions of the leakage bits even with the public communication channel. Compared to the re-keying system, the matrix size and hence the calculation overhead can be significantly reduced with the aid of the information leakage sensor.

7. Conclusion

With the recent increase in smart IoT devices available, the physical security of a cryptographic processor has become a more critical issue. In this paper, an information leakage sensor against LFI was proposed. This sensor not only detects LFI but also provides leakage bit information by sensing laser irradiation spots and strengths. The distributed sensor with time-interleaved operation can scan all sensor outputs for laser spot positioning with a small layout area penalty. Sensor sensitivity tuning detects LFI energy and hence obtains partial leakage bit information. A test-chip measurement in a 0.18 μm CMOS successfully demonstrated the sensor operation with only +23% layout area penalty. The concept of an LFI-resilient cryptographic system with partial key update is also proposed based on the proposed information leakage sensor for high-availability secure information platforms.

Acknowledgments

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

ORCID iDs

Kohei Matsuda https://orcid.org/0000-0001-7713-4419
Yuichi Komano https://orcid.org/0000-0002-5121-3458
Takeshi Sugawara https://orcid.org/0000-0001-9356-534X
Mitsugu Iwamoto https://orcid.org/0000-0003-1092-8489
Kazuo Sakiyama https://orcid.org/0000-0002-4414-815X
Noriyuki Miura https://orcid.org/0000-0002-0072-6114

1) I. Verbauwhede, J. Balasch, S. S. Roy, and A. Van Herrewege, "Circuit challenges from cryptography," ISSCC Dig. Tech. Pap., 428–9 (2015).
2) P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *Advances in Cryptology* (Springer, Berlin, 1999) Lecture Notes in Computer Science, Vol. 1666, pp. 388–97.
3) E. Brier, C. Clavier, and F. Oliver, "Correlation power analysis with a leakage model," *Cryptographic Hardware and Embedded Systems* (Springer, Berlin, 2004) Lecture Notes in Computer Science, Vol. 3156, pp. 16–9.
4) D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for fault," *Advances in Cryptology* (Springer, Berlin, 1997) Lecture Notes in Computer Science, Vol. 1233, pp. 37–51.
5) E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," *Advances in Cryptology* (Springer, Berlin, 1997) Lecture Notes in Computer Science, Vol. 1294, pp. 513–25.
6) Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, Nov. 2001 [https://doi.org/10.6028/NIST.FIPS.197].
7) G. Piret and J. J. Quisquater, "A differential fault attack technique against SPN structures, with application to the AES and KHAZAD," Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (August, 2000) Vol. 2779, pp. 77–88.
8) K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, "Information-theoretic approach to optimal differential fault analysis," IEEE Trans. Inf. Forensics Security **7**, 109 (2012).
9) M. Tunstall, D. Mukhopadhyay, and S. Ali, "Differential fault analysis of the advanced encryption standard using a single fault Lecture Notes in Computer ScienceProc. Int. Workshop on Information Security Theory and Practices, June, 2011 (Springer), (Berlin) Vol. 6633, pp. 224–33.
10) J. Takahashi and T. Fukunaga, (2010), Differential fault analysis on AES with 192 and 256-bit keys IACR Cryptology ePrint Archive.
11) A. Moradi, M. T. M. Shalmani, and M. Salmasizadeh, "A generalized method of differential fault attack against AES cryptosystem," *Cryptographic Hardware and Embedded Systems* (Springer, Berlin, 2006) Lecture Notes in Computer Science, Vol. 4249, pp. 91–100.
12) Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," *Cryptographic Hardware and Embedded Systems* (Springer, Berlin, 2010) Lecture Notes in Computer Science, Vol. 6225, pp. 320–334.
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," *Cryptographic Hardware and Embedded Systems* (Springer, Berlin, 2011) Lecture Notes in Computer Science, Vol. 6917, pp. 292–311.
14) A. Moradi, O. Mischke, and C. Paar, "One attack to rule them all: collision timing attack versus 42 AES ASIC cores," IEEE Trans. Comput. **62**, 1786 (2013).
15) A. Barenghi, L. Breveglieri, L. koren, and D. Naccache, "Fault injection attacks on cryptographic devices: theory, practice and countermeasures," Proc. IEEE **100**, 3056 (2012).
16) S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," *Cryptographic Hardware and Embedded Systems* (Springer, Berlin, 2002) Lecture Notes in Computer Science, Vol. 2523, pp. 2–12.
17) T. G. Malkin, F. X. Standaert, and M. Yung, "A comparative cost/security analysis of fault attack countermeasure," Proc. Fault Diagnosis and Tolerance in Cryptography (FDTC), Sept. 2005, pp. 109–123.
18) 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. Pap., 274–5 (2011).
19) E. Trichina and R. Korkikyan, "Multi fault laser attacks on protected CRT-RSA," Proc. Fault Diagnosis and Tolerance in Cryptography (FDTC), Aug. 2010, pp. 75–86.
20) R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov, "Cryptographic processors—a survey," Proc. IEEE **94**, 357 (2006).
21) J. Woudenberg, M. F. Witteman, and F. Menarini, "Practical optical fault injection on secure microcontrollers," Proc. Fault Diagnosis and Tolerance in Cryptography (FDTC), Sept. 2011, pp. 91–99.
22) Renesas Technology Corporation, "IC Card System using Photo-Detectors for Protection," US Patent US7042752 B2.
23) K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y. Hayashi, M. Nagata, and N. Miura, "A 286F^2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack on cryptographic processor," IEEE J. Solid-State Circuits **53**, 3174–82 (2018).
24) K. Matsuda, S. Tada, M. Nagata, Y. Li, T. Sugawara, M. Iwamoto, K. Ohta, K. Sakiyama, and N. Miura, "An information leakage sensor based on measurement of laser-induced opto-electric bulk current density," Proc. Int. Conf. Solid State Devices and Materials (SSDM), 2019, pp. 501–502, M-1-03.
25) J. L. Wirth and S. C. Rogers, "The transient response of transistors and diodes to ionizing radiation," IEEE Trans. Nucl. Sci. **11**, 24 (1964).
26) D. H. Habing, "The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits," IEEE Trans. Nucl. Sci. **12**, 91 (1965).
27) C. Roscian, J. M. Dutertre, and A. Tria, "Frontside laser fault injection on cryptosystems—application to the AES last round," Proc. IEEE Hardware-Oriented Security and Trust (HOST), Jun 2013, pp. 119–124.
28) R. Baumann, "The impact of technology scaling on soft error rate performance and limits to the efficacy of error correction," Tech. Dig. Int. Electron Devices Meeting, Dec. 2002, pp. 329–332.
29) E. H. Neto, I. Ribeiro, G. Wirth, F. Kastensmidt, and M. Vieira, "Using bulk built-in current sensors to detect soft errors," IEEE Micro **26**, 10 (2006).
30) 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-induced currents," Proc. IEEE Int. On-Line Testing Symp. (IOLTS), Jul. 2015, pp. 150–155.
31) A. Sarafianos, O. Gagliano, M. Lisart, V. Serradeil, J.-M. Dutertre, and A. Tria, "Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90 nm technology," Proc. IEEE Int. Reliability Physics Symp. (IRPS), Apr. 2013, pp. 5B.5.1–5B.5.9.
32) E. W. Enlow and D. R. Alexander, "Photocurrent modeling of modern microcircuit pn junctions," IEEE Trans. Nucl. Sci. **35**, 1467 (1988).
33) R. A. C. Viera, P. Maurine, J.-M. Dutertre, and R. P. Bastos, "Simulation and experimental demonstration of the importance of IR-drops during laser fault-injection," IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. (2019).
34) K. Matsuda, N. Miura, M. Nagata, Y. Hayashi, T. Fujii, and K. Sakiyama, "On-chip substrate-bounce monitoring for laser-fault countermeasure," Proc. IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Dec. 2016, pp. 1–6.
35) B. Bhuva, "Soft error trends in advanced silicon technology nodes," Proc. IEEE Int. Electron Devices Meeting (IEDM), Dec. 2018, pp. 34.4.1–34.4.4.
36) P. C. Kocher, "Leak-resistant cryptographic indexed key update," US Patent US6539092B1.
37) M. Medwed, F.-X. Standaert, J. Großschädl, and F. Regazzoni, "Fresh re-keying: security against side-channel and fault attacks for low-cost devices," *International Conference on Cryptology in Africa* (Springer, Berlin), Lecture Notes in Computer Science, Vol. 6055, pp. 279–96.
38) C. Dobraunig, F. Koeune, S. Mangard, F. Mendel, and F.-X. Standaert, "Towards fresh and hybrid re-keying schemes with beyond birthday security Lecture Notes in Computer ScienceInt. Conf. on Smart Card Research and Advanced Applications, Vol. 9514, pp. 225–41.
39) Y. Komano and S. Hirose, "Re-keying scheme revisited: security model and instantiations," Appl. Sci. **9**, 1002 (2019).
40) M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," Inf. Process. Lett. **97**, 52 (2006).