Physical Attack Protection Techniques for IC Chip Level Hardware Security

Nagata, Makoto

Miki, Takuji

Miura, Noriyuki

(Citation)
IEEE Transactions On Very Large Scale Integration (VLSI) Systems,30(1):5-14

(Issue Date)
2022-01

(Resource Type)
journal article

(Version)
Version of Record

Physical Attack Protection Techniques for IC Chip Level Hardware Security

Makoto Nagata, *Senior Member, IEEE,* Takuji Miki, *Member, IEEE,* and Noriyuki Miura, *Member, IEEE*

(*Invited Paper*)

***Abstract*— Secure hardware systems are threatened by adversarial attempts on integrated circuit (IC) chips in a practical utilization environment. This article provides overviews of physical attacks on cryptographic circuits, associated vulnerabilities in an IC chip, and protection schemes in the vertical unification of systems, circuits, and packaging technologies. The design principles of on-chip monitoring circuits to sense the attackers' attempts are discussed and tested with Si demonstrators. Physical structures are explored for secure IC chips to establish protections against multimodal side-channel attacks. The backside buried metal (BBM) wirings in a Si substrate are unified with its frontside complementary metal–oxide semiconductor (CMOS) circuits to achieve avoidance, detection, and resiliency against electromagnetic and laser attacks.**

***Index Terms*— Backside metal wirings, cryptography, electromagnetic (EM) attack, hardware security, laser fault injection attack, on-chip monitoring, power delivery network, side-channel attack, Si substrate attack.**

I. Introduction

CRYPTOGRAPHIC devices have been innumerably penetrated in daily lives with the evolvement of Internet-of-Things (IoT) applications. Private data are wirelessly exchanged between edge nodes around the people of interest and cloud servers that exist remotely and even internationally. Here, the whole IoT network needs encryption and decryption of data for meeting security and privacy requirements.

Symmetric ciphers are often preferred in the communications of data and control codes since their encryption and decryption are attained at sufficiently high processing throughputs with a relatively smaller number of transistors. The advanced encryption standard (AES) [1] is the most popularly adopted and pursued for performance with integrated circuit (IC) technologies [2], [3] or even with field-programmable gate array (FPGA) devices [4], [5]. Also, a variety of lightweight ciphers has been developed [6] and evaluated in IC-chip level performance for more ubiquitous leverage of cryptography [7]–[9].

On the other hand, public-key ciphers realize the higher order security functionality demanded in IoT evolvements [10]–[11]. Examples include message authentications with digital signatures, attribute-based signatures, and encryption for group entities, homomorphic encryption without the need of decryption before calculation among encrypted data, and many other attractive possibilities. Continuous efforts have been devoted to implement such ciphers in semiconductor IC chips featured with low power and small footprint, along with high resiliency against implementation attacks [12], [13].

The adoption of cipher algorithms will be extended among highly reliable electronics to be integrated in autonomous driving vehicles, flying objects over populated towns, machine learning facilities with multi-modal analog sensor fusions, medical-healthcare devices, and many other systems. The necessity and mandatory requirements of the higher levels of security and safety have been argued and agreed among international frameworks and published in official documents [14]–[16].

Hardware security has been evolved with proactive research results widely in very large-scale integration (VLSI) systems and IC techniques toward the greater level of security in IoT applications [17]–[19]. Analog and mixed-signal circuits are also considered against security vulnerability [20]. Among the diversified scopes of hardware security, this article will be focused on IC-chip level protections against physical attacks for cryptographic circuits in IoT applications. The remaining part of this article is structured as follows. Section II overviews physical attacks. Section III provides protection techniques. Section IV addresses a concise conclusion.

II. Physical Attacks and Vulnerabilities

A. General Description

A variety of attempts have been made to derive secret key information from cryptographic circuits in operation. Passive attacks observe physically side effects such as power supply noise and electromagnetic (EM) wave emission during circuit operation, as known as side-channel (SC) attacks [21]–[23]. An external observer has a chance to deduce secret key bytes from power current waveforms, which are recorded by probing voltage variations at the power source terminal or receiving EM emanations over or around an IC chip.

Active attacks analyze the difference of erroneous outputs from originally correct outputs, after intentional fault injections in fault attacks [24]–[26]. The crypto processor produces

Manuscript received March 1, 2021; accepted April 5, 2021. Date of publication May 5, 2021; date of current version January 17, 2022. This work was supported in part by the Cabinet Office (CAO), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Cyber Physical Security for IoT Society," New Energy and Industrial Technology Development Organization (NEDO) under Grant JPNP18015. *(Corresponding author: Makoto Nagata.)*

Makoto Nagata and Takuji Miki are with the Graduate School of Science, Technology and Innovation, Kobe University, Kobe 657–8501, Japan (e-mail: nagata@cs.kobe-u.ac.jp).

Noriyuki Miura was with the Graduate School of System Informatics, Kobe University, Kobe 657–8501, Japan. He is now with the Graduate School of Information Science and Technology, Osaka University, Suita 565-0871, Japan (e-mail: nmiura@ist.osaka-u.ac.jp).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TVLSI.2021.3073946.

Digital Object Identifier 10.1109/TVLSI.2021.3073946

erroneous output bits once an observer intentionally injects faults by flipping 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.

These attacks explore the vulnerabilities of cryptographic circuits by looking into transistor-level operations digitally as well as through analog behaviors, which are therefore generally classified as physical attacks or implementation attacks. Those threats are essentially and inevitably present among the lowest entities of computing stack. The fault sensitivity attack is considered most efficient which directly relates the minimum power of intentional fault injection with the secret information in cryptographic circuits, by exploring the responsive surface of physical processes such as logic delay time variation, bit flipping, and power current consumption [27], [28].

Transactions in information processing share computing resources among microprocessor cores in a single system or even on the same die. This fact brings about another root of vulnerability against SC attacks at the high-level entities in computing hierarchy. Side-channel interactions happen among independent processes through the occupation of shared resources or even by the parasitic couplings among binary digital circuit components. Hardware performance counters were originally prepared for profiling the events of instruction executions as well as the usage statistics of hardware resources in a traditional microprocessor [29]. This has been exploited as the most reliable source of internal logic statistics for performance analysis while also considered attackable from the adversary viewpoint [30]. The interactions among processing threads are explored by attackers within a many-core CPU system on shared cache memories, shared memory buffers, or even translation lookaside buffers [31]–[33], although those resources are logically isolated and protected with hierarchical security walls. An example quantity to snoop is the probability of a cache hit and miss that can be differently measured by the number of clock cycles. The bits in the memory cells of interest in a row could be intentionally flipped by intentional and intensive read accesses to its adjacent cell rows [34]. The countermeasures have been actively developed by means of secure software coding and exploitation of secure hardware control.

There are emerging threats such as Hardware Trojans (HT) among modern electronics systems [35]. Crypto IC chips are unexpectedly made more vulnerable by HTs through malicious actions in diversified ways, where SC leakage properties such as power, delay, and EM waves are multiply explored [36]. The SC leakages have been challenged by HT circuits which are located within an IC chip [37] or even on a board [38], while also utilized for HT detection within an IC chip in the operation field [39] as well as during product testing [40].

B. IC Chip Level Vulnerabilities

Secure IC chips generally incorporate cryptographic functions, as shown in Fig. 1, where crypto circuits are surrounded with peripheral circuits. Plain and cipher texts are communicated through a digital data interface (I/F). The core power supply (core V_{DD}) voltage is regulated with respect to local ground (V_{SS}) voltage by power management circuits (PMCs) involving dc-dc converters and reference voltage generators. Also, a phase-locked loop (PLL) supplies clock frequencies. From an ideal viewpoint, the crypto circuits are therefore securely isolated from off-chip environment in signaling as well as powering. However, physical attacks potentially jeopardize hardware-level security by breaking those isolation walls [41]. Among the variety of attackable surfaces that can be assumed in an IC chip for an adversary, two essential constitutions of vulnerability at the transistor level are discussed in the following parts.

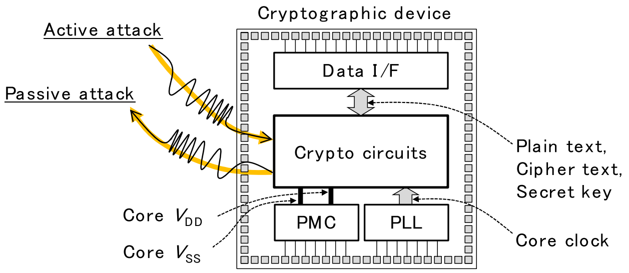


Fig. 1. Physical attack isolation at chip level [41].

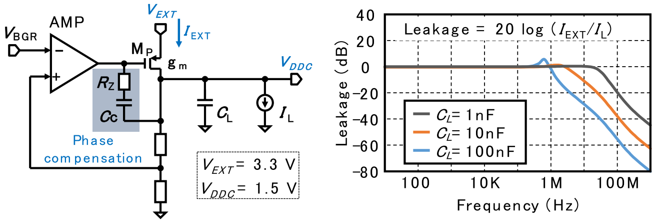


Fig. 2. LDO as an on-chip micro regulator.

1) Power Delivery Network: We have seen the vulnerability inherently attributes to the electrical property of power delivery networks (PDNs). The power current at the core V_{DD} dynamically varies with the progress of processing steps according to a cipher algorithm. A low-dropout linear regulator (LDO) is often provided for the micro regulation of the core V_{DD}, where the external power current, I_{EXT}, is sacrificed for the stabilization of internal core V_{DD} voltage within the low-pass bandwidth of an error correction feedback. The on-chip micro LDO circuit is typically depicted as in Fig. 2. The error feedback path includes on-chip *RC* components for the dominant pole compensation, instead of placing an off-chip (on-board) large-size capacitor for the stabilization of the core V_{DD} node [42]. This is desirable for fine-grained voltage regulation in a large IC chip among the core V_{DD} islands with different workloads, and also eliminates on-board explicit points to make the core V_{DD} voltage observable. However, I_{EXT} linearly copies the power consumption currents of digital circuits in the frequency bandwidth of the core V_{DD} regulation, which therefore never suppresses the power and EM SC leakage.

The crypto circuits implementing public-key crypto algorithms are more prone to the power SC leakage through LDO. Their leakage models attribute to the difference

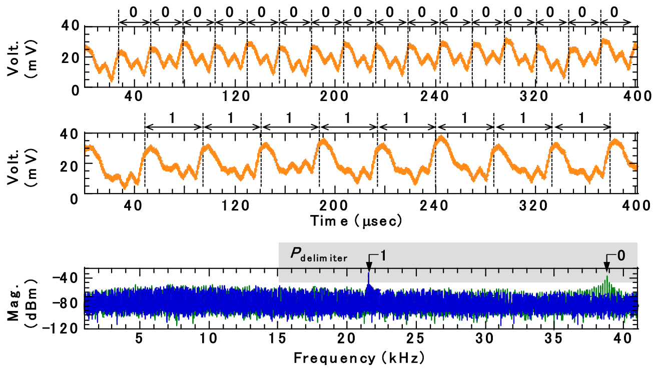


Fig. 3. EM signatures and frequency components measured on PCB from ECDSA engine at 50 MHz.

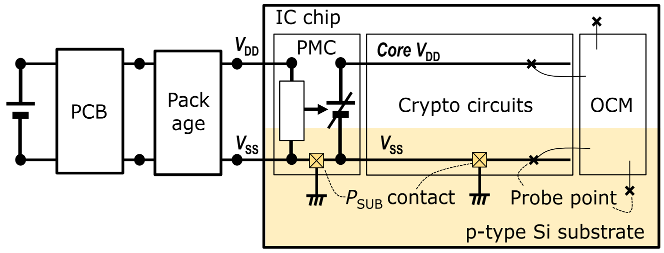


Fig. 4. Power delivery and Si substrate network.

in the number of clock cycles during arithmetic computation sequences. To adopt elliptic curve (EC) digital signature algorithm (ECDSA) for data authentication, for example, the arithmetic sequences are binarily grouped into the EC point doubling and EC point addition, where the operations are selected according to the conditional branch with the polarity of k_i which is the ith bit of a nonce, k. Once an adversary collects EM waveforms over the full lengths of EC computation, the signatures (envelope patterns) can emerge for the group of EC computation and consequently relate to k_i. The waveforms reflect internal logic structures of computation branches even with the adoption of Montgomery ladder method [43], [44]. Here, the number of clock cycles for each EC computation typically reaches the order of thousands. The frequency components of signatures can be therefore smaller than 100 kHz when an ECDSA core operates even at 100 MHz and stay within the low-pass bandwidth of LDO. This makes the SC leakage of public-key crypto circuits transparent throughout on- and off-chip PDN and visible around off-chip power supply (V_{EXT}) terminals at 3.3 V on a printed circuit board (PCB).

If the consecutive appearances of either "0" or "1" are set in a secret key, an ECDSA engine generates the regular presence of the signature by arithmetic operations, as experimentally shown in the EM waveforms of Fig. 3. The signature periods for the respective EC computations are roughly 47 and 26 μs. This results in the emergence of delimiter frequency component in the power spectrum and determines its power level, $P_{\text{delimiter}}$. This can effectively measure the security feature of crypto circuits with countermeasure algorithms and architectures, for instance, on EC-based ciphers. The frequency components at 21.5 and 39.0 kHz are the cases with the operating frequency at 50 MHz.

The statistical t-test method is generally applied to evaluate data dependence on power noise and EM waveforms, according to the test vector leakage assessment (TVLA) methodology [45]. The statistical significance, $|t| > 4.5$, suggests the presence of SC leakage.

In comparison, AES and lightweight private-key crypto circuits can prevent the leakage of I_{EXT} to a certain degree in the on-chip PDN. This is because their crypto processing completes typically in the order of 10 clock cycles with the clocking frequency of several 100 MHz, where I_{EXT} is located outside the low-pass bandwidth and thus attenuated with -20 dB/decade with frequencies. It is also noted in the size of circuits that the transistor count is smaller with the order of 10^3 in comparison to public-key crypto circuits. This also allows fine-grained power sourcing within crypto circuits so as to flatten I_{EXT}, by using capacitor-based charge equalization [46], [47] as well as digitally controlled power regulations in a variety of power converter topologies [48]–[51], [52]. Those designs have been actively explored up to the present, where the number of measurement traces to disclose the secret key bytes (MTD) is one of the key features to assess the security level of 128- or 256-bit AES circuits.

The research efforts remain needed to establish the design methodologies of secure PDNs for EC-based highly functional cryptographic circuits with the higher level of SC resiliency.

2) Si Substrate Network: A p-type doped Si substrate is the base material for CMOS devices. Crypto circuits are typically implemented on an IC chip using CMOS logic standard cells. The V_{SS} side of every logic cell is directly connected to the Si substrate through p^+ ohmic contact areas while the core V_{DD} one to n-type doped wells through n^+ areas, in order to bias the body voltage of n- and p-type MOS transistors, respectively [53]. This physical device structure forces the V_{SS} side of crypto circuits to be unified with the whole p-type Si substrate, as shown in Fig. 4, in a single V_{SS} domain as a part of on-chip PDN. The power current of crypto circuits is no longer hidden if an adversary looks into the V_{SS} side, even though their core V_{DD} side is isolated by the dedicated voltage regulators. It is known that the capacitive isolation of V_{SS} side can be accomplished by substrate engineering to include an intermediate silicon oxide layer. However, the attenuation factor is not much expected with the large area size of EC-based crypto circuits due to the reduction of capacitive impedance.

Fig. 5 demonstrates the on-chip measurements of V_{SS} voltage variations in an IC chip embedding AES circuits. The p-type Si node, V_{SUB}, is measured by on-chip voltage monitoring (OCM) circuitry and exhibits voltage waveforms almost identical to the internal V_{SS} node of the AES core, even with the distance of 1.7 mm. It has been shown that the waveforms on a Si substrate are applicable to the correlation power analysis (CPA) and deliver secret key bytes as similar as in the core V_{DD} side [54].

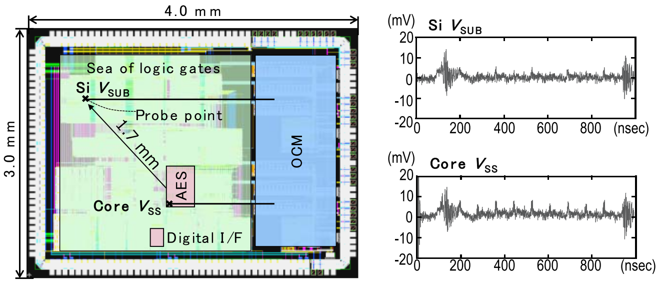
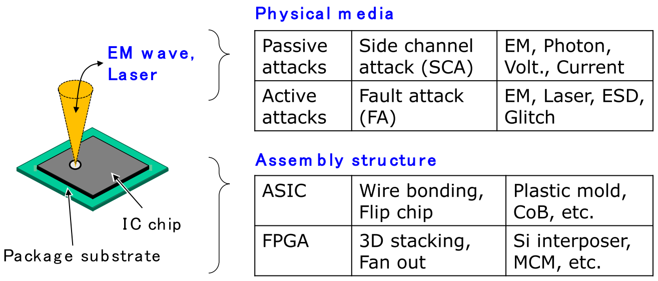


Fig. 5. On-chip waveform in crypto operation [41] and [54].



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

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

Fig. 6. Attack measures and packaging structures [41].

The Si substrate is therefore considered the unavoidable source of vulnerability against SC leakage in an IC chip implementation of any cipher algorithm. It is noted that the thickness of an IC chip is typically in the order of 350 μm or even thinner, which is smaller than the horizontal distance on a chip surface among circuits, for instance, between AES and LDO circuit blocks. As the advancement of IC chip packaging to minimize its form factor, the backside of a chip becomes more prominent for an attack surface particularly in flip-chip assembly [55].

C. IC Chip Packaging and Assembly

An adversary has the choice of physical attacks which are typically based on electromagnetism and optics, while thermal, acoustic, and mechanical properties are also explored. The packaging and assembly structures of a target IC chip need to be assessed from protection viewpoints, as outlined in Fig. 6. The EM measures are more flexible in selecting locations, angles as well as frequencies of interest, while spread over 100 μm or more in space, even without knowing surface materials. The optical measures are advantageous in localizing attacks in space and in time with the resolution of 1 μm and 10 ns, respectively, while needing decapsulation of an IC chip since resin materials for a laminate as well as molding are usually opaque.

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 transistors as the source of vulnerability. The higher level of cross-sectional complexity will help attackers to hesitate, while the more advanced reverse engineering techniques toward deep defect analysis can be utilized in high-end adversarial attempts.

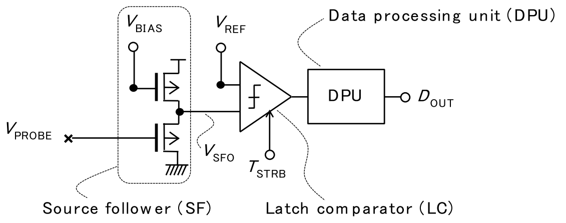


Fig. 7. OCM circuit schematic [41] and [53].

The third dimension has been explored for secure IC chip applications. The shielding layers on an IC chip use metal wiring channels densely in parallel with encrypted signaling on the topmost metal layer [56]. An additional chip having low-impedance PDN structures is placed on top of a secure IC die in the 3-D integration [57]. The shielding materials conformally formed in IC chip packaging are conductive to attenuate or magnetic to absorb EM radiations from the circuits [58]–[60]. An IC chip itself can be made fragile or use flexible materials for self-destruction on attack [61]. A variety of advanced packaging and assembly technologies have been exploited for the protection of IC chips from passive and active attacks [62].

The vulnerabilities against physical attacks can be mitigated by those measures at IC chip packaging and board-level assembly, only when they are co-designed with crypto circuits and associated protection schemes. This will be discussed in the remaining sections of this article. The challenge has been pursued not only on custom IC chips while also on cryptographic functionality on FPGA devices.

III. Protection Schemes

A. On-Chip Characterization

1) Power Side-Channel Leakage: The OCM of Fig. 7 provides unique features of in-place characterization of SC leakages within crypto circuits and detections of adversarial attempts. The on-chip voltage variation is measured locally at the probed points of interest among the core V_{DD} and V_{SS} wirings as well as V_{SUB} taps, where those measurements are localized and decoupled from the property of power supply regulation in global PDNs (Fig. 4). The OCM has been originally adopted to solve problems due to undesired power and substrate noise coupling [53]–[64] as well as electromagnetic compatibility (EMC), and then exploited toward the higher level of hardware security.

The voltage of interest, V_{PROBE}, is probed and sensed by a source follower (SF) at the input of OCM. 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} among the stepped V_{REF} is determined and output as the digital code of V_{REF}. The code is determined one after another for successive strobe timings through the 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.

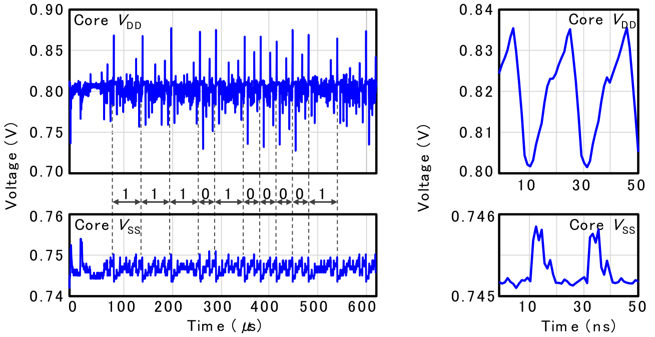


Fig. 8. On-chip measured voltage waveforms of ECDSA engine at 50 MHz.

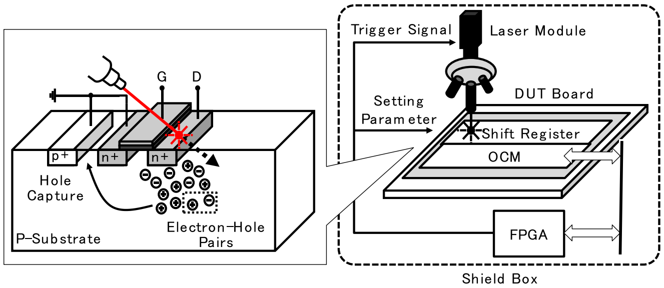


Fig. 9. LFI principle and experimental setup [66].

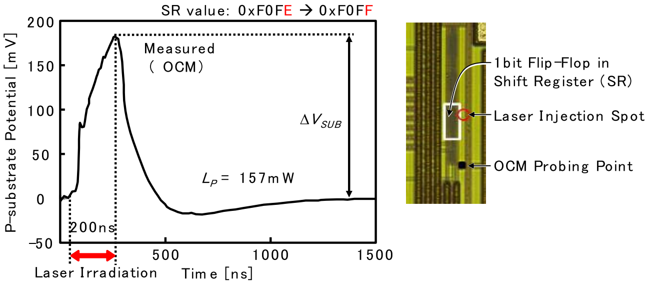


Fig. 10. Measured substrate voltage waveforms in laser irradiation [41].

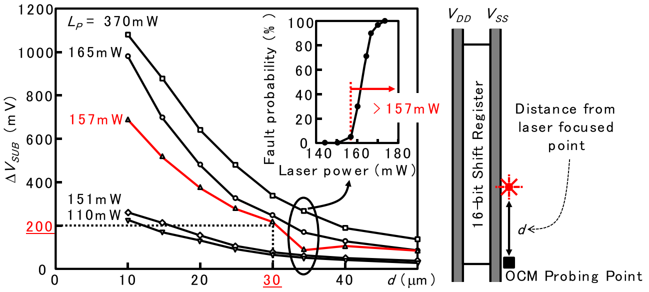


Fig. 11. On-chip characterization of LFI [41].

The measured in-place waveforms are analyzed for the potentiality of SC leakage from cryptographic processing. The OCM is equipped with a successive approximation register analog to digital converter (SAR-ADC) in the digitization stage of waveform capturing [65], for the acceleration to accommodate thousands of clock cycles in a public-key crypto algorithm. Fig. 8 exemplifies on-chip V_{DD} and V_{SS} waveforms of ECDSA crypto circuits operating at 50 MHz. The signatures for EC computations are clearly seen on both on-chip V_{DD} and V_{SS} domains with the dependence on secret key bits. Again, their frequency components are sufficiently within the low-pass bandwidth of an on-chip LDO and to be observable on PCB, as was shown in Fig. 3. The OCM is also capable of magnifying the voltage variations within a clock cycle of 20 ns in a high-time resolution setup. The offset dc voltages are due to n- and p-channel SF sensing the nominal V_{DD} and V_{SS} of 1.5 and 0.0 V, respectively.

The on-chip waveform measurements assess the presence of power SC leakage from crypto circuits and justify the SC leakage tolerant algorithms and architectures. The adoption of resilient packaging structures and attack detection capabilities is also motivated by the results.

2) Laser Fault Injection: On-chip characterization is applied to the laser illumination to circuits under operation, as depicted in Fig. 9 [66]. A near infrared (NIR) laser module is synchronized to the OCM and 16-bit shift register (SR) circuits on a device under test (DUT). 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. The electrons and holes are immediately separated to nearby electrodes that are biased at V_{DD} and V_{SS}, respectively, and creating substrate current and associated voltage bounce around the location of irradiation.

The laser fault injection is characterized by capturing on-chip V_{SUB} waveforms during and after the irradiation of NIR laser, with the laser power large enough to induce a single-bit failure. The laser beam is focused on an IC chip with the spot size of 2 μm at the intended x–y location in the resolution of 1 μm when we use an optical microscope having 50× magnification lens. The waveform given in Fig. 10 exhibits the maximum voltage increase of 180 mV when the LSB of SR flips from the originally stored value (0xF0F**E** → 0xF0F**F**). The dependence of substrate voltage variation (ΔV_{SUB}) on the distance along the SR from the point of laser irradiation is characterized for different laser powers as in Fig. 11, using the OCM with multiple probing points. The voltage variations induced at the point of laser irradiation spread concentrically on a Si substrate, where its radius is governed primarily by the resistivity. 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 on this particular CMOS technology. The measured results indicate that an IC chip can recognize the potentiality of laser attacks by measuring voltage bounce inside or surrounding positions to crypto circuits.

B. EM Attack Detection

The EM power can be straightforwardly delivered to the area of vulnerable nodes within the die through cables [67] or by the irradiation from the topside of a packaged IC chip to intentionally incur erroneous operation in crypto circuits in active fault injection attacks [68]. Those attempts are not necessarily using high-cost equipment, and more importantly,

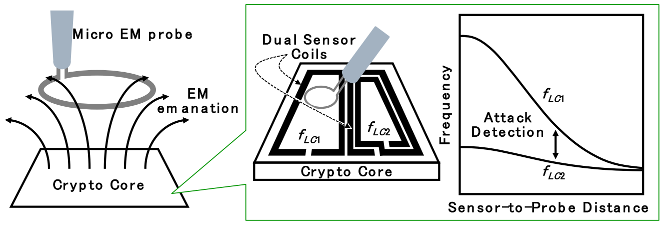


Fig. 12. LEMA sensing principle [71].

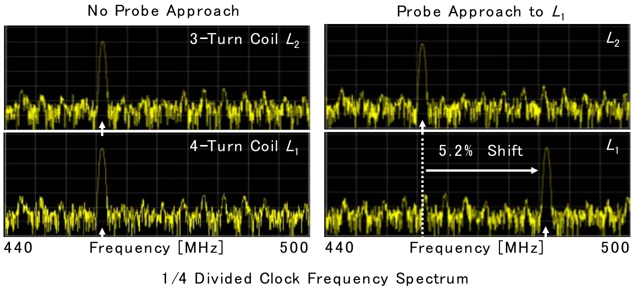
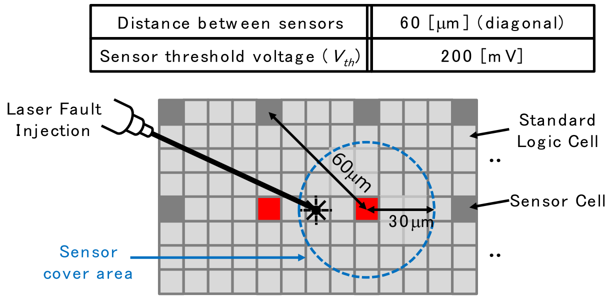


Fig. 13. Demonstration of EM probe detection [71].



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

Fig. 14. Design considerations of LFI sensors [41].

efficient than other invasive disturbances like voltage surges and clock glitches which can be potentially prevented by the power converter and PLL, respectively. On the other hand, a miniaturized micro antenna (μEM probe) is scanned over an IC chip in passive attacks to locate the highest level of EM side-channel leakage from a cryptographic processor, as in the local electromagnetic SC attack (LEMA) [69]. The finer resolution is expected with the careful removal of resins covering an IC chip.

The dynamic movement or even static placement of an antenna induces the change in the EM field nearby an IC chip and more or less interacts with the operation of circuits. These responses are inevitable in accordance with a physical law, even though the LEMA search itself is considered physically nonintrusive. An on-chip inductor (sensor coil) of Fig. 12 can sense the advent of adversary through magnetic coupling to its antenna (μEM probe), with the higher sensitivity for the more proximate positioning [70]. A pair of inductors (coils) with different shapes (e.g., the number of turns) are, respectively, used in *LC* oscillators, where their oscillatory frequencies uniquely respond to the nearby magnetic field, as demonstrated in Fig. 13. The inductors are formed only with wirings on the topmost metal layer and placed over the crypto circuits to protect. As the prevention mechanism against LEMA, the crypto function will be immediately halted or even detoured into a dummy state, when the placement of antenna is detected. The LEMA sensor features the on-chip calibration of *LC* oscillators against environmental variations of device parameters, power supply, and temperature (PVT), in order to retain its sensitivity to the weak displacements of proximate magnetic fields by passive attacks exploring EM SC leakage [71].

On the other hand, circuit-level interactions with EM waves have been exploited for the detection of adversarial high power irradiation intending fault injections even in FPGA devices. A variety of detector circuits use configurable logic elements in FPGA devices and successfully find unexpected glitches [72], gate-chain delay time variation [73], shifting self-oscillation frequencies, and relative phases among racing oscillators [74], [75], all caused by intentionally intensive EM irradiation.

The system-level response of secure IC chips will be utilized to analyze the output from the detectors and prioritize the symptoms for potentially being under passive as well as active EM SC attacks, and then immediately trigger evasive on-the-fly actions.

The detective capability becomes more fundamentally necessitated in security IC chips. The simulation techniques for EM radiation as well irradiation at the full-chip level [76], [77] promote the design of detector circuitry and rational placements in an IC chip. The technology developments for the higher level of EM attack detection will continue to grow.

C. Laser Attack Detection

The NIR laser spotted on an IC chip with the order of a few 1 μm induces voltage variation on a Si substrate with the spread radius of ten times or even larger. The OCM with multiple sensing frontend cells can detect the attempts, as conceptually sketched in Fig. 14, by thresholding abnormal magnitudes higher than 200 mV. The frontends are miniaturized by design and regularly distributed within the physical layout of crypto circuits. We can find design principles based on the body (bulk) current sensing, which was originally developed for detecting soft errors by high energy cosmic rays [78] and also exploited for finding laser fault injection [79]. The illumination from the backside of an IC chip should be detectable, which happens with the transparency of NIR light in a Si substrate.

The frontend with the post-layout area size of 286F^2/cell, which is almost same as the 2.6 equivalent gates of 2-input NAND logic cell, has been developed in a 0.18 μm standard CMOS technology, and embedded for 336 positions within a 128-bit AES circuits [80].

The body current by the laser irradiation can also be sensed through the change in self-oscillation frequencies, as similar to the EM sensing scheme, which is applicable to FPGA devices [81]. The laser-induced current is also assumed to flow in PDNs [82], which can be responded by power OCM circuits.

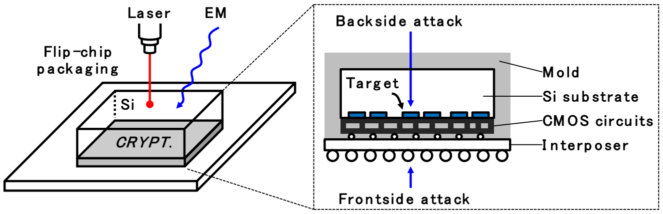


Fig. 15. Si backside as an attack surface.

D. Secure Packaging

The backside of an IC chip is open for adversarial attempts on a Si substrate, as shown in Fig. 15, in flip-chip packaging. Although an antenna senses and injects EM waves through resin coating or plastic molding of an IC chip, their removals will enhance the potentiality of attacks. Furthermore, an optical observation is performed on the emission of photons from actively operating transistors, or the laser irradiation into transistors creates body currents for incurring faulty operation. Those attempts need to decapsulate an IC chip to be naked in its backside and even to thin down as well as excavate the Si substrate from the backside. Focused ion beam (FIB) equipment for the finest reverse engineering is available to an adversary [83]. For the recognition of invasive attempts by an IC chip, photo current sensors may detect incoming lights after package opening [84].

The higher level of resiliency is newly challenged against multimodal and combinational physical attacks. Semiconductor packaging technologies have been so far continuously evolved for the higher performance, smaller footprint, and lower profile of an IC chip in mass production. However, the close cooperation of resilient packaging structures and detective circuit functionality will increase their values and provide unique ways to generally protect crypto circuits from invasive, noninvasive, passive, and active SC attacks. We have defined a secure packaging technology in this way.

A Si backside buried metal (BBM) technique has been developed for boosting power delivery performance in an IC chip [85] and exploited for secure packaging [86]. The BBM wirings are formed by Cu with the width and depth of 15 and 10 μm, respectively, in the backside of Si substrate of 40-μm thickness, and unified to CMOS circuits on the frontside with through Si via (TSV) connections.

The monolithic structures for attack prevention are sketched in Fig. 16, with variations of a single chip and 3-D chip stack. The frontend CMOS circuits include crypto circuits to be protected, voltage regulators for supplying crypto circuits, and OCM circuits for attack detection. When the IC chip is packaged in a flip-chip way, BBM wirings are exposed to the outside. The BBM stripes in a meander shape are biased at the shielding voltage of V_{SHD} which is isolated from V_{DD} and V_{SS} of an IC chip. The meander of Fig. 17 provides the functionality of EM shielding and laser blocking, and furthermore, forms a disconnection detector for intentional laser cutting. This is essentially advantageous over the single metal plate covering the full backside. Since the whole IC chip is covered by meanders, the entire public-key crypto circuits in a large Si area are protected.

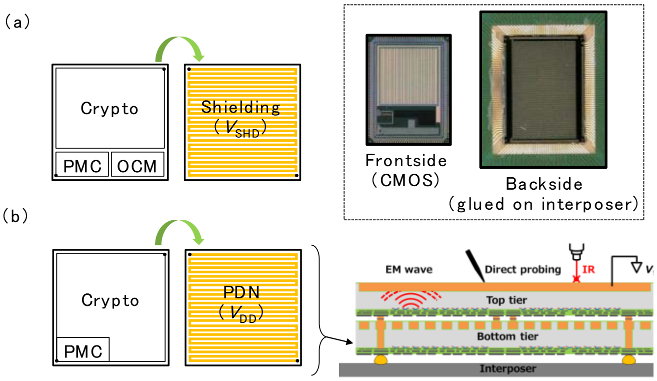


Fig. 16. Monolithic attack protection structure. (a) Single chip. (b) Secure 3D chip stack.

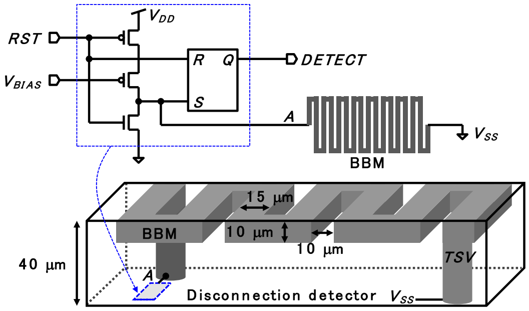


Fig. 17. Disconnection detection circuit using BBM.

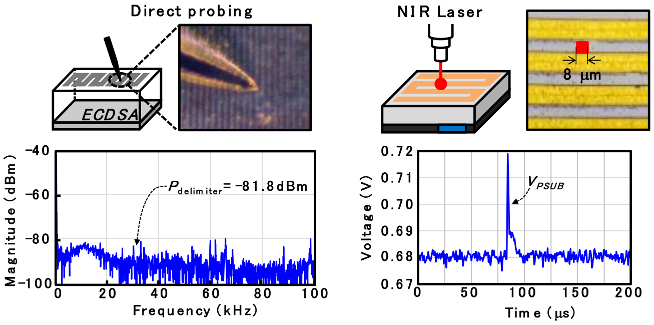


Fig. 18. Demonstration of BBM protections in passive (left) and active (right) attacks [86].

Fig. 18 shows experimental results of attack protection and die photographs of the BBM chip. The voltage probing directly on the backside Si substrate exhibits the suppression of $P_{\mathrm{delimiter}}$ for more than 25 dB in comparison to the regular IC chip without BBM. The laser irradiation is focused on the gap between BBM stripes, where the space of 10 μm was set in our experimental fabrication process. However, the resultant voltage variation on the frontside of an IC chip can be captured and recognized by the OCM. The BBM meander conceals circuit components from laser irradiations, and further detects an unexpected disconnection by the adversarial trial of metal removal by a laser cutter.

The BBM IC chips are stacked in 3-D packaging in Fig. 16(b). The bottom chip carries crypto circuits and designated power converters with PDNs supported by BBM stripes over the full backside area. While the frontside is faced down on a plastic interposer and assembled on a PCB, the backside is concealed by the top tier die. The top chip has the same structure as in the single die of Fig. 16(a) except for not incorporating crypto functions. This structure obviates SC leakages vertically by the BBM shielding effects while horizontally by the BBM distributed decoupling capacitors over the PDNs. The latter flattens the change of power currents locally among logic switching gates and therefore suppresses the power current dependence on arithmetic computation sequences in such as EC-based public-key crypto algorithms [87].

IV. Conclusion

Physical vulnerabilities and relevant attack methodologies were described from the IC chip viewpoint. Multimodal attempts by an adversary will become more prominent with the higher level of crypto analysis expertise and advanced technology utilization. Protection schemes need to be more sophisticated as well as diversified, and tailored to security functionality with chosen cipher algorithms.

A secure packaging technology that monolithically unifies the backside metal wirings and the frontside standard CMOS devices were exemplified. On-chip monitoring circuits were designed and implemented for sensing attempts and detecting attacks. The resiliency against multimodal attacks with EM emission and laser injection was demonstrated through system-level circuits-package interactions.

Hardware-level security in VLSI systems needs to feature detection, recognition, and obviation mechanisms. Physical protection technologies will continue to be explored with in-depth knowledge covering widely from material science, device, and packaging technologies to circuits and system architectures.

Acknowledgment

The authors thank to the present and past Ph.D. students who belonged to the Hardware Security and Safety Research Team (Secafy) at Kobe University.

References

[1] National Institute of Standards and Technology, *Advanced Encryption Standard (AES)*, Standard FIPS PUB 197, Nov. 2001.

[2] S. K. Mathew *et al.*, "53 Gbps native GF$(2^4)^2$ composite-field AES-encrypt/decrypt accelerator for content-protection in 45 nm high-performance microprocessors," *IEEE J. Solid-State Circuits*, vol. 46, no. 4, pp. 767–776, Apr. 2011.

[3] R. Ueno *et al.*, "High throughput/gate AES hardware architectures based on datapath compression," *IEEE Trans. Comput.*, vol. 69, no. 4, pp. 534–548, Apr. 2020.

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

[5] T. Good and M. Benaissa, "AES on FPGA from the fastest to the smallest," in *Proc. IACR CHES*, in Lecture Notes in Computer Science, vol. 3659. Springer, 2005, pp. 427–440.

[6] National Institute of Standards and Technology. *Computer Securrity Resource Center, Lightweight Cryptography*. Accessed: Mar. 1, 2021. [Online]. Available: https://csrc.nist.gov/projects/lightweight-cryptography

[7] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Proc. IACR CHES*, in Lecture Notes in Computer Science, vol. 4727. Springer, Sep. 2007, pp. 450–466.

[8] J. Borghoff *et al.*, "PRINCE—A low-latency block cipher for pervasive computing applications," in *Proc. IACR ASIACRYPT*, in Lecture Notes in Computer Science, vol. 7658. Springer, Dec. 2012, pp. 208–225.

[9] N. Miura *et al.*, "A 2.5ns-latency 0.39pJ/b 289μm^2/Gb/s ultra-light-weight PRINCE cryptographic processor," *Proc. Symp. VLSI Circuits*, Jun. 2017, pp. C266–C267.

[10] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ECC-based authentication scheme for Internet of Things (IoT)," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3440–3450, Sep. 2020.

[11] T. Matsumoto, M. Ikeda, M. Nagata, and Y. Uemura, "Secure cryptographic unit as root-of-trust for IoT era," *IEICE Trans. Electron.*, early access, Jan. 28, 2021, doi: 10.1587/transele.2020CDI0001.

[12] I. M. R. Verbauwhede, *Secure Integrated Circuits and Systems*. Cham, Switzerland: Springer, 2010.

[13] I. Verbauwhede, J. Balasch, S. S. Roy, and A. Van Herrewege, "Circuit challenges from cryptography," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 428–429.

[14] *Road Vehicles–Functional Safety*. Accessed: Mar. 1, 2021. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-2:v1:en

[15] UNECE. *World Forum for the Harmonization of Vehicle Regulations (WP.29)*. Accessed: Mar. 1, 2021. [Online]. Available: https://unece.org/transport/vehicle-regulations

[16] *Senior Officals Group Information Systems Security (SOGIS)*. Accessed: Mar. 1, 2021. [Online]. Available: https://www.sogis.eu/index_en.html

[17] M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*, M. Tehranipoor and C. Wang, Eds. Cham, Switzerland: Springer, 2012.

[18] N. Sklavos, R. Chaves, G. D. Natale, and F. Regazzoni, *Hardware Security and Trust, Design and Deployment of Integrated Circuits in a Threatened Environment*. Cham, Switzerland: Springer, 2017.

[19] C. H. Chang and Y. Cao, *Frontiers in Hardware Security and Trust; Theory, Design and Practice*. London, U.K.: IET, 2020.

[20] T. Miki, N. Miura, H. Sonoda, K. Mizuta, and M. Nagata, "A random interrupt dithering SAR technique for secure ADC against reference-charge side-channel attack," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 1, pp. 14–18, Jan. 2020.

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

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

[23] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Cham, Switzerland: Springer, 2007.

[24] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for fault," in *Proc. IACR EUROCRYPT*, in Lecture Notes in Computer Science, vol. 1233. Springer, May 1997, pp. 37–51.

[25] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *Proc. IACR CRYPTO*, in Lecture Notes in Computer Science, vol. 1294. Springer, Aug. 1997, pp. 513–525.

[26] D. Karaklajic, J.-M. Schmidt, and I. Verbauwhede, "Hardware Designer's guide to fault attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 21, no. 12, pp. 2295–2306, Dec. 2013.

[27] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in *Proc. IACR CHES*, in Lecture Notes in Computer Science, vol. 6225. Springer, Aug. 2010, pp. 320–334.

[28] 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," in *Proc. IACR CHES*, in Lecture Notes in Computer Science, vol. 6917. Springer, Sep. 2011, pp. 292–311.

[29] G. Ammons, T. Ball, and J. R. Larus, "Exploiting hardware performance counters with flow and context sensitive profiling," in *Proc. ACM SIGPLAN Conf. Program. Lang. Design Implement. (PLDI)*, May 1997, pp. 85–96.

[30] L. Uhsadel, A. Georges, and I. Verbauwhede, "Exploiting hardware performance counters," in *Proc. 5th Workshop Fault Diagnosis Tolerance Cryptography*, Aug. 2008, pp. 1–9.

[31] F. Liu, Y. Yarom, Q. Ge, G. Heiser, and R. B. Lee, "Last-level cache side-channel attacks are practical," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 605–622.

[32] P. Pessl, D. Gruss, C. Maurice, M. Schwarz, and S. Mangard, "DRAMA: Exploiting DRAM addressing for cross-CPU attacks," in *Proc. 25th USENIX Secur. Symp.*, Aug. 2016, pp. 565–581.

[33] B. Gras, K. Razavi, H. Bos, and C. Giuffrida, "Translation leak-aside buffer: Defeating cache side-channel protections with TLB attacks," in *Proc. 27th USENIX Secur. Symp.*, Aug. 2018, pp. 955–972.

[34] Y. Kim *et al.*, "Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors," in *Proc. ACM/IEEE 41st Annu. Int. Symp. Comput. Architecuture (ISCA)*, Jun. 2014, pp. 361–372.

[35] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Des. Test. Comput.*, vol. 27, no. 1, pp. 10–25, Jan. 2010.

[36] Y. Hayashi and S. Kawamura, "Survey of hardware trojan threats and detection," in *Proc. Int. Symp. Electromagn. Compat. (EMC Eur.)*, Sep. 2020, pp. 1–5.

[37] L. Lin, M. Kasper, T. Güneysu, C. Parr, and W. Burleson, "Trojan side-channels: Lightweight hardware trojans through side-channel engineering," in *Proc. IACR CHES*, in Lecture Notes in Computer Science, vol. 5747. Springer, Sep. 2009, pp. 382–395.

[38] M. Kinugawa, D. Fujimoto, and Y. Hayashi, "Electromagnetic information extortion from electronic devices using interceptor and its countermeasure," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2019, no. 4, pp. 62–90, Aug. 2019.

[39] S. Narasimhan *et al.*, "Hardware Trojan detection by multiple-parameter side-channel analysis," *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2183–2195, Nov. 2013.

[40] D. Fujimoto, M. Nagata, S. Bhasin, and J.-L. Danger, "A novel methodology for testing hardware security and trust exploiting on-chip power noise measurement," in *Proc. 20th Asia South Pacific Design Autom. Conf.*, Jan. 2015, pp. 749–754.

[41] M. Nagata, T. Miki, and N. Miura, "On-chip physical attack protection circuits for hardware security: Invited Paper," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Apr. 2019, pp. 1–6.

[42] I. P. Vaisband, R. Jakushokas, M. Popovich, A. V. Mezhiba, S. Köse, and E. G. Friedman, *On-Chip Power Delivery and Management*. Cham, Switzerland: Springer, 2016.

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

[44] K. Koiwa *et al.*, "Collision-based EM analysis on ECDSA hardware and a countermeasure," in *Proc. Joint Int. Symp. Electromagn. Compat., Sapporo Asia–Pacific Int. Symp. Electromagn. Compat. (EMC Sapporo/APEMC)*, Sapporo, Japan, Jun. 2019, pp. 793–796.

[45] J. Cooper, G. Goodwill, J. Jaffe, G. Kenworthy, and P. Rohatgi, "Test vector leakage assessment (TVLA) methodology in practice," in *Proc. Int. Cryptograph. Module Conf.*, Sep. 2013, pp. 1–13.

[46] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010.

[47] N. Miura, D. Fujimoto, R. Korenaga, K. Matsuda, and M. Nagata, "An intermittent-driven supply-current equalizer for 11x and 4x power-overhead savings in CPA-resistant 128bit AES cryptographic processor," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, Nov. 2014, pp. 225–228.

[48] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2017, pp. 142–143.

[49] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "128b AES engine with higher resistance to power and electromagnetic side-channel attacks enabled by a security-aware integrated all-digital low-dropout regulator," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2019, pp. 404–405.

[50] D. Das *et al.*, "EM and power SCA-resilient AES-256 in 65 nm CMOS through >350× current-domain signature attenuation," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2020, pp. 424–425.

[51] R. Kumar *et al.*, "A SCA-resistant AES engine in 14 nm CMOS with time/frequency-domain leakage suppression using non-linear digital LDO cascaded with arithmetic countermeasures," in *Proc. IEEE Symp. VLSI Circuits*, Jun. 2020, pp. 1–2.

[52] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "An EM/power SCA-resilient AES-256 with synthesizable signature attenuation using digital-friendly current source and RO-bleed-based integrated local feedback and global switched-mode control," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2021, pp. 500–501.

[53] M. Nagata, J. Nagai, T. Morie, and A. Iwata, "Measurements and analyses of substrate noise waveform in mixed-signal IC environment," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 19, no. 6, pp. 671–678, Jun. 2000.

[54] D. Fujimoto *et al.*, "Side-channel leakage on silicon substrate of CMOS cryptographic chip," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 32–37.

[55] M. T. Rahman and N. Asadizanjani, "Backside security assessment of modern SoCs," in *Proc. 20th Int. Workshop Microprocessor/SoC Test, Secur. Verification (MTV)*, Dec. 2019, pp. 18–24.

[56] X. T. Ngo *et al.*, "Cryptographically secure shield for security IPs protection," *IEEE Trans. Comput.*, vol. 66, no. 2, pp. 354–360, Feb. 2017.

[57] T. Miki *et al.*, "Over-the-top Si interposer embedding backside buried metal PDN to reduce power supply impedance of large scale digital ICs," in *Proc. Int. 3D Syst. Integr. Conf. (3DIC)*, Oct. 2019, pp. 1–4.

[58] N. Karim, J. Mao, and J. Fan, "Improving electromagnetic compatibility performance of packages and SiP modules using a conformal shielding solution," in *Proc. Asia–Pacific Int. Symp. Electromagn. Compat.*, 2010, pp. 56–59.

[59] J.-D.-V. Hoang, R. Darveaux, T. Lobianco, Y. Liu, and W. Nguyen, "Breakthrough packaging level shielding techniques and EMI effectiveness modeling and characterization," in *Proc. IEEE 66th Electron. Compon. Technol. Conf. (ECTC)*, May 2016, pp. 1290–1296.

[60] K. Watanabe *et al.*, "Magnetic composite sheets in IC chip packaging for suppression of undesired noise emission to wireless communication channels," in *Proc. 12th Int. Workshop Electromagn. Compat. Integr. Circuits (EMC Compo)*, Oct. 2019, pp. 1–3.

[61] S. Borel *et al.*, "A novel structure for backside protection against physical attacks on secure chips or SiP," in *Proc. IEEE 68th Electron. Compon. Technol. Conf. (ECTC)*, May 2018, pp. 515–520.

[62] W. Chen and W. R. Bottoms, *Heterogeneous Integration Roadmap*. Piscataway, NJ, USA: IEEE Press, 2019, ch. 19. Accessed: Mar. 1, 2021. [Online]. Available: http://eps.ieee.org/hir

[63] K. Noguchi and M. Nagata, "An on-chip multichannel waveform monitor for diagnosis of systems-on-a-chip integration," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 15, no. 10, pp. 1101–1110, Oct. 2007.

[64] T. Hashida and M. Nagata, "An on-chip waveform capturer and application to diagnosis of power delivery in SoC integration," *IEEE J. Solid-State Circuits*, vol. 46, no. 4, pp. 789–796, Apr. 2011.

[65] T. Wadatsumi, T. Miki, and M. Nagata, "A dual-mode successive approximation register analog to digital converter to detect malicious off-chip power noise measurement attacks," *Jpn. J. Appl. Phys.*, vol. 60, no. SB, Feb. 2021, Art. no. SBBL03.

[66] K. Matsuda, N. Miura, M. Nagata, Y.-I. Hayashi, T. Fujii, and K. Sakiyama, "On-chip substrate-bounce monitoring for laser-fault countermeasure," in *Proc. IEEE Asian Hardw.-Oriented Secur. Trust (AsianHOST)*, Dec. 2016, pp. 1–6.

[67] Y. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki, and H. Sone, "Non-invasive EMI-based fault injection attack against cryptographic modules," in *Proc. IEEE Int. Symp. Electromagn. Compat. (EMC)*, Aug. 2011, pp. 763–767.

[68] K. Sakiyama, Y. Sasaki, and Y. Li, *Security of Block Ciphers: From Algorithm Design to Hardware Implementation*. Hoboken, NJ, USA: Wiley, 2015.

[69] T. Sugawara, D. Suzuki, M. Saeki, M. Shiozaki, and T. Fujino, "On measurable side-channel leaks inside ASIC design primitives," in *IACR CHES*, in Lecture Notes in Computer Science, vol. 8086. Springer, Aug. 2013, pp. 159–178.

[70] N. Miura *et al.*, "A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor," in *Proc. Symp. VLSI Circuits Dig. Tech. Papers*, Jun. 2014, pp. 172–173.

[71] 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," *J. Cryptol.*, vol. 30, pp. 373–391, Dec. 2015.

[72] L. Zussa *et al.*, "Efficiency of a glitch detector against electromagnetic fault injection," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, 2014, pp. 1–6.

[73] D. El-Baze, J.-B. Rigaud, and P. Maurine, “An embedded digital sensor against EM and BB fault injection,” in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr. (FDTC)*, Aug. 2016, pp. 78–86.

[74] N. Miura *et al.*, “PLL to the rescue: A novel EM fault countermeasure,” in *Proc. 53rd ACM/EDAC/IEEE Design Automat. Conf. (DAC)*, Jun. 2016, pp. 1–6.

[75] J. Breier, S. Bhasin, and W. He, “An electromagnetic fault injection sensor using Hogge phase-detector,” in *Proc. 18th Int. Symp. Qual. Electron. Design (ISQED)*, Mar. 2017, pp. 307–312.

[76] A. Tsukioka *et al.*, “A fast side-channel leakage simulation technique based on IC chip power modeling,” *IEEE Lett. Electromagn. Compat. Pract. Appl.*, vol. 1, no. 4, pp. 83–87, Dec. 2019.

[77] M. Dumont, M. Lisart, and P. Maurine, “Modeling and simulating electromagnetic fault injection,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 4, pp. 680–693, Apr. 2021.

[78] E. H. Neto, I. Ribeiro, M. Vieira, G. Wirth, and F. L. Kastensmidt, “Using bulk built-in current sensors to detect soft errors,” *IEEE Micro*, vol. 26, no. 5, pp. 10–18, Sep. 2006.

[79] R. P. Bastos, F. S. Torres, J.-M. Dutertre, M.-L. Flottes, G. Di Natale, and B. Rouzeyre, “A bulk built-in sensor for detection of fault attacks,” in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, Jun. 2013, pp. 51–54.

[80] K. Matsuda *et al.*, “A 286 F2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack on cryptographic processor,” *IEEE J. Solid-State Circuits*, vol. 53, no. 11, pp. 3174–3182, Nov. 2018.

[81] W. He, J. Breier, S. Bhasin, N. Miura, and M. Nagata, “Ring oscillator under laser: Potential of PLL-based countermeasure against laser fault injection,” in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr. (FDTC)*, Aug. 2016, pp. 102–113.

[82] R. A. C. Viera, P. Maurine, J.-M. Dutertre, and R. Possamai Bastos, “Simulation and experimental demonstration of the importance of IR-drops during laser fault injection,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 6, pp. 1231–1244, Jun. 2020.

[83] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. S. Krissler, C. Boit, and J.-P. Seifert, “Breaking and entering through the silicon,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, Nov. 2013, pp. 733–744.

[84] D. Shahrjerdi, J. Rajendran, S. Garg, F. Koushanfar, and R. Karri, “Shielding and securing integrated circuits with sensors,” in *Proc. IEEE/ACM Int. Conf. Computer-Aided Design (ICCAD)*, Nov. 2014, pp. 170–174.

[85] Y. Araga *et al.*, “A thick Cu layer buried in Si interposer backside for global power routing,” *IEEE Trans. Compon., Packag., Manuf. Technol.*, vol. 9, no. 3, pp. 502–510, Mar. 2019.

[86] T. Miki *et al.*, “Si-backside protection circuits against physical security attacks on flip-chip devices,” *IEEE J. Solid-State Circuits*, vol. 55, no. 10, pp. 2747–2755, Oct. 2020.

[87] K. Monta *et al.*, “3-D CMOS chip stacking for security ICs featuring backside buried metal power delivery networks with distributed capacitance,” *IEEE Trans. Electron Devices*, vol. 68, no. 4, pp. 2077–2082, Apr. 2021.

Makoto Nagata (Senior Member, IEEE) 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.

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

Dr. Nagata is a Senior Member of IEICE. He has been a member of a variety of technical program committees of international conferences, such as the Symposium on VLSI Circuits (2002–2009), Custom Integrated Circuits Conference (2007–2009), Asian Solid-State Circuits Conference (2005–2009), International Solid-State Circuits Conference (since 2014), European Solid-State Circuits Conference (since 2020), and many others. He has been chairing the Technology Directions subcommittee for International Solid-State Circuits Conference since 2018. He was the Technical Program Chair (2010–2011), the Symposium Chair (2012–2013), and an Executive Committee Member (2014–2015) for the Symposium on VLSI circuits. He was the Past Chair of the IEEE Solid-State Circuits Society (SSCS) Kansai Chapter (2017–2018). He is currently an AdCom Member of the IEEE SSCS (since 2020), where he also serves as a Distinguished Lecturer (DL) of the society (since 2020). He has been an Associate Editor for IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS since 2015.

Takuji Miki (Member, IEEE) received the B.S. and M.S. degrees from Ritsumeikan University, Kyoto, Japan, in 2004 and 2006, respectively, and the Ph.D. degree from Kobe University, Kobe, Japan, in 2017.

From 2006 to 2016, he was with Panasonic Corporation, Osaka, Japan, where he was involved in the development of high-performance analog and mixed-signal integrated circuits for consumer and industrial applications. He is currently a Project Associate Professor with the Graduate School of Science, Technology and Innovation, Kobe University. His current research interests include data converters, sensor interface, and hardware security.

Noriyuki Miura (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Keio University, Yokohama, Japan.

From 2005 to 2008, he was a JSPS Research Fellow and an Assistant Professor (since 2007) with Keio University, where he developed wireless interconnect technology for 3-D integration. In 2012, he moved to Kobe University, Kobe, Japan, and he became a Professor at Osaka University, Suita, Japan, in 2020. He was also concurrently appointed as a JST PRESTO Researcher, and currently working on hardware security/safety and next-generation heterogeneous computing systems.

Dr. Miura is currently serving as a Technical Program Committee (TPC) Member of A-SSCC and Symposium on VLSI Circuits. He served as the TPC Vice Chair for 2015 A-SSCC. He was a recipient of the Top ISSCC Paper Contributors 2004–2013, the IACR CHES Best Paper Award in 2014, the IEICE Suematsu Yasuharu Award in 2017, and the Marubun Research Encouragement Award in 2019.