Si Substrate Backside—An Emerging Physical Attack Surface for Secure ICs in Flip Chip Packaging

Nagata, Makoto

Miki, Takuji

(Citation)
IEEE Open Journal of the Solid-State Circuits Society,4:365-375

(Issue Date)
2024-11-18

(Resource Type)
journal article

(Version)
Version of Record

(URL)
https://hdl.handle.net/20.500.14094/0100492887

IEEE Open Journal of the
Solid-State Circuits Society

Received 2 September 2024; revised 11 November 2024; accepted 12 November 2024. Date of publication 18 November 2024;
date of current version 7 January 2025.

Digital Object Identifier 10.1109/OJSSCS.2024.3499967

Si Substrate Backside—An Emerging Physical Attack Surface for Secure ICs in Flip Chip Packaging

MAKOTO NAGATA (Senior Member, IEEE), AND TAKUJI MIKI (Member, IEEE)

The Graduate School of Science, Technology and Innovation, Kobe University, Kobe 657-8501, Japan

CORRESPONDING AUTHOR: M. NAGATA (e-mail: nagata@cs.kobe-u.ac.jp)

This work was in part by the New Energy and Industrial Technology Development Organization (NEDO) under Grant JPNP23013, and in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI under Grant JP22H04999.

ABSTRACT Semiconductor integrated circuit (IC) chips are regularly exposed to physical attacks and faced to the compromise of information security. An attacker leverages Si substrate backside as the open surface of an IC chip in flip-chip packaging and explores the points of information leakage over the entire backside without being hampered by physical obstacles as well as applying invasive treatments. Physical side channels (SCs), e.g., voltage potentials, current flows, electromagnetic (EM) waves, and photons, are transparent through Si substrate and attributed to the operation of security ICs. An attacker measures SCs using probes as well as antennas and correlates them with secret information, such as secret key bytes, used in a cryptographic processor or analog quantities at the frontend of Internet of Things (IoT) gadgets. This article defines and elucidates the emerging threats of Si-substrate backside attacks on flipped IC chips, demonstrates attacks and proposes countermeasures.

INDEX TERMS Advanced packaging, cryptography, hardware security, integrated circuits (ICs), secure packaging, side channel (SC) attack.

I. INTRODUCTION

A SECURITY integrated circuit (IC) chip is challenged by an adversary with malicious attempts to steal secret information or to overwrite or falsify data in a system. A cryptographic processor could be vulnerable to so called side channel (SC) attacks, once a crypto algorithm with theoretically proven for security is implemented in digital hardware and/or software, and even potentially with architectures toward the higher level of resiliency. SC information leakage essentially attributes to the physical quantities among digital circuits that exhibit the correlation with cryptographic processing. The insights of SC leakages and SC attacks should be referred to the literature, such as [1], [2], [3], [4], [5], [6], [7], and [8], along with their historic discoveries as well as scholarly evolvements. Since the earliest reports on the SC leakage among semiconductor IC chips with passive eavesdropping models [1], [2] as well as active fault injection models [4], [5], IC chips have continuously explored and leveraged the design methodology toward SC tolerance up to now [3], [6], [7], [8]. In response to the compilation of SC knowledge, the standardized frameworks for security assurance, such as the common criteria for information technology security evaluation (CC) [9], that is equivalent to ISO/IEC18045, and the security requirements for cryptographic modules (FIPS 140-3) [10] that refer to ISO/IEC 19790, mentions the vulnerability associated with SC attacks. More visibly, the vulnerability assessment (AVA) class of evaluation assurance level (EAL) in CC defines the level of attack potential by a potential adversary, which is regularly updated according to reported SC attacks.

The attack methods and the prevention measures have been scientifically investigated and enthusiastically competed from respective angles. Design for security has been vertically pursued across the design hierarchies of a crypto processor. For combatting passive SC leakage, the masking architecture uses random numbers to decorrelate power consumption and sensitive information among logical operation at transistor-level cells [11], [12]. The place and route algorithms are tuned specially for camouflage, hiding and balancing of power consumption in the core part of crypto processing at the physical-layout level [13], [14]. Power converter circuits are designed for the flatness of power current against load

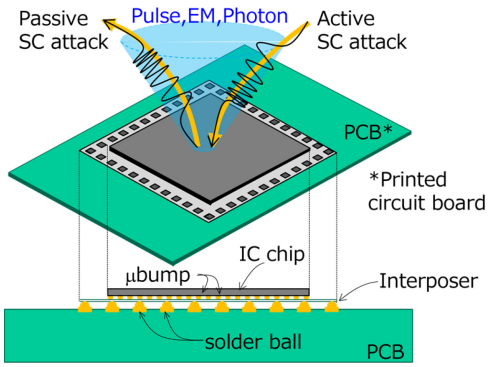

FIGURE 1. IC chip flipped packaging. Physical medias of pulse, EM, and photon are possibly emitted as well as injected, for use in passive and active SC attacks, respectively.

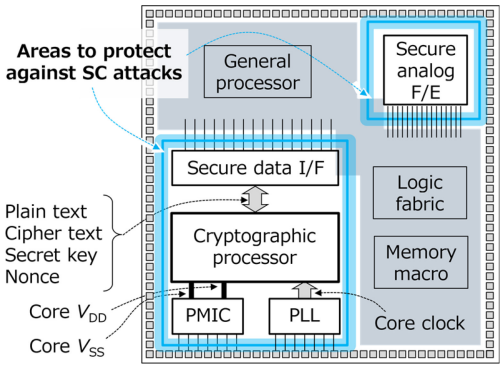

FIGURE 2. Security IC chip floorplan.

variations [15], [16], [17], [18] or for the equalization of load current [19], [20]. The advent of more efficient active SC attacks [21], [22], [23] urges to exploit prevention structures in IC chips [24], [25]. An attacker leverages those knowledges and explores attack trials across spaces wider than concerned by IC designers.

Analog information processing, on the other hand, is also no longer unrelated to SC attacks [26]. Analog to digital (A/D) or digital to analog (D/A) converters at the frontend of sensors or actuators, respectively, are potentially compromised for analog quantities. It is noted that analog information is not protected by digital cryptography, naturally before A/D conversion or immediately after D/A conversion, respectively, and therefore the measures to avoid physical attacks at the location of analog signaling are necessary. With the scenario of stealing analog information at the input of a successive approximation register (SAR) A/D converter, which is most often adopted by the Internet of Things (IoT) gadgets these days, an attacker measures the voltage noise on analog power rails (V_{DD}, V_{SS}) or analog reference voltage (V_{REF}) as analog SC voltages, although which are to be ideally fixed at DC voltage over the operation of A/D conversion. Then the attacker associates the analog SC voltages with the sampled voltage of an analog signal at its input, by virtue of template matching as well as machine learning with neural networks. The demonstration has been successfully reported [27], [28], [29], even for estimating the magnitudes and the signs of analog inputs in a high-speed asynchronous and high-resolution differential SAR A/D converter [30].

Research efforts have been continuously made in the last decades to solve SC information leakage problems, as partly addressed in the previous statements, and very much diversified among a variety of attack surfaces as well as attack targets. The former exploits insecure behaviors from systems to devices, more concretely, software codes, hardware data transactions, circuit operations, and device-level physical interactions. The latter spreads across disparate features, such as digital cryptography, analog information processing, and device-based unclonable authentication. These problems are fundamental to security IC systems and will remain unsolved even with advanced transistor technologies. We need more in-depth understanding of physical mechanisms behind those SC problems within IC chips.

In this article, the SCs over the Si backside of an IC chip will be focused on different physical medias, with a particular consideration of flip-chip packaging structures. The remaining part of this article is constructed as follows. Threat models and SC attacks will be detailed in Section II from both passive and active approaches including Silicon experiments. The countermeasure techniques will be discussed in Section III before a brief conclusion given in Section IV.

II. SIDE CHANNEL ATTACKS

A. THREAT MODELS

An IC chip is flipped down and faced to a fine-pitch interposer in the flip chip packaging of Fig. 1. This is often the case with advanced IC chips [31], [32], [33]. The area pads are densely populated on its frontside (circuit side) and bonded to the interposer as well as printed circuit board (PCB) with bumps and balls, respectively, with the preferable advantages of accommodating a large number of pins and the shorter connection lengths, in comparison to the traditional bond-wire-based face up packaging. Security ICs are hidden from an attacker by the compositions on the frontside of such flipped-chip packaging. However, the backside of an IC chip, more precisely, the Si substrate backside, is now accessible or traceable by an attacker to observe (in passive attacks) or to impose (in active attacks) the voltage variation on Si backside, electromagnetic (EM) waves, as well as photons through Si substrate, as sketched in Fig. 1.

A general floorplan of a security IC chip is depicted in Fig. 2, where the digital area is divided into secure zones and universal areas which are interfaced by secure walls (blue lines in the figure.) The digital data of security importance are screened by secure interface (I/F) when coming to or outgoing from the secure zone. A cryptographic (crypto) processor that encrypts or decrypts the digital data is supplied by a power management IC (PMIC) and prevented from voltage glitches within the zone. Similarly, clock signals are routed from a phased locked loop (PLL)-based signal synthesizer, which eliminates intentional timing glitches. The

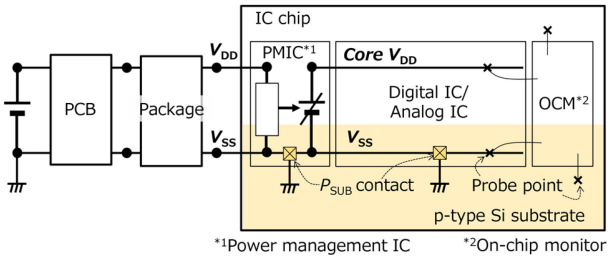

FIGURE 3. General schematic of PDN.

analog functionality for security is also logically protected by using a crypto processor. While this architecture prevents security ICs from horizontal attacks, the vulnerability remains for the attacks perpendicular to ICs. The security threats of SC attacks over Si substrate backside emerge from this fact will be detailed as follows.

The general schematic of a power delivery network (PDN) is given in Fig. 3. An IC chip has V_{SS} (ground side) paths common to every circuit for power current flowing from V_{DD} (high side). The p-type Si substrate (P_{SUB}), very often used as a base Si substrate in manufacturing transistors, is globally tied with V_{SS} with distributed $p+$ contacts. This is a resistive material that can convey voltage variations, transparent for infrared (IR) photons and EM waves.

Digital circuits for security, e.g., crypto processors, and analog circuits handling secure information, e.g., security sensors, can be individually supplied by PMIC at different supply voltage, however, commonly connected to V_{SS}. Power current of any circuit induces voltage variations on V_{SS} nodes, which become measurable at any point over P_{SUB} once probed on Si backside by an external entity, or potentially by an adversary. The voltage variation is attributed to the distributed parasitic impedance over V_{SS} wires and P_{SUB} networks, and therefore additive among circuits and transmittable across the areas of security (defined only on the frontside) over the entire Si substrate.

Additionally, a secure IC chip embeds on-chip monitoring (OCM) circuits to probe V_{DD}, V_{SS}, and P_{SUB} nodes within the chip and to measure and store voltage waveforms at the respective nodes [34]. These waveforms are post-evaluated to characterize SC leakage as well as to detect SC attacks.

B. PASSIVE ATTACKS

Physical variables that are measurable on Si substrate backside and exemplified in Fig. 4, are correlated with information handled by circuits. An adversary makes attempts to distinguish secret key bytes in the key spaces of 128 bits or larger, by exploiting the large set of measurement traces during the operation of a crypto processor. Similarly, analog information is deduced from the measurement traces over the conversion procedures between analog values and digital codes or vice versa. An observer assumes the algorithm, architecture, and implementation (physical placements, clock cycles, and/or timing diagrams) of the Target of Evaluation (ToE) for collecting measurement traces and analyzes the information risen up from them according

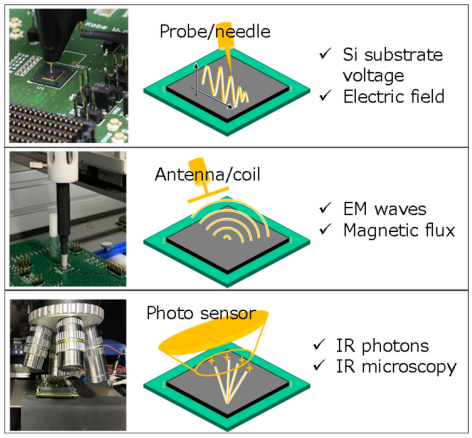

FIGURE 4. Passive SCs on Si backside.

to the leakage models associated with the measurements. The procedure is passively executed by an automatic analyzer with searching the position of interest on the surface of an IC chip as well as on the time axis of circuit operation. The phenomena and processes are called SC information leakage and passive SC attacks, respectively. The properties of each variable physically measurable on Si backside (Fig. 4) are outlined as follows.

1) Si substrate voltage is directly probed on its surface by a conductive needle, and its time-domain waveforms are captured by an oscilloscope. This is the most straightforward observation of physical variables associated with circuit operation, where the power current flows through V_{SS} wires and induces voltage variations among P_{SUB} nodes (V_{PSUB}). This V_{PSUB} electrically propagates to the backside surface of Si substrate through its resistive/capacitive network. When we assume that ToE is a crypto processor of advanced encryption standard (AES) in a plain design (no SC countermeasure) with a 128-bit secret key, the V_{PSUB} traces exhibit SC leakage and the number of V_{PSUB} waveforms in the order of 10k reveal the key bytes through correlation power analysis (CPA). Measurements and analysis details are referred to [35].
2) EM wave emanates from metal wires within ICs in operation and is sensed by an antenna nearby Si backside of the IC chip. Si substrate is transparent to EM waves. The set of EM traces is exploitable for SC leakage with the model of correlation EM analysis (CEMA). A small coil straightforwardly measures the magnetic flux induced by the power current of ToE flowing through metal wires. References are, such as [36] and [37].
3) Photons are emitted from Si-based transistors, e.g., MOSFETs though microscopic processes of generation and recombination of electron–hole pairs. This limitedly happens among the transistors involved in the switching operation of logic gates, where such electrons are highly energized by the drain electric field (hot electrons) or vertically penetrate into a gate oxide

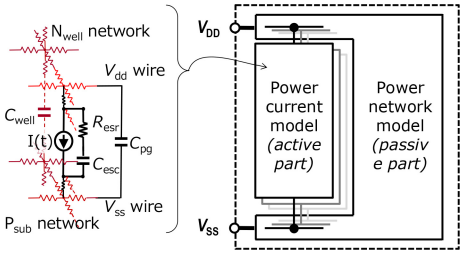

FIGURE 5. Power current simulation models.

layer according to the gate electric field (tunneling electrons). Those photons are lower in energy than the Si bandgap and then transmissive through Si substrate, and perpendicularly emitted out from the Si backside surface. An array of photo detectors captures the location, pattern, and timing of photo emissions during the operation of logic circuits of ToE. In particular, the set of optical snapshots of a crypto processor is associated with its internal operation, by the correlation-based photo emission analysis (CPEA). The examples are given in [38] and [39].

The physical properties of Fig. 4 independently convey SC information, which originate uniquely from the power current of ToE. It is noted that the power current itself is observable at the power pads on the frontside as well as at the power pins on PCB, however, their frequency components are limited by the low-pass nature of PMIC as well as parasitic impedances to PDN. Similarly, thermal patterns of an IC chip reflect the heating from active parts of ICs and therefore behave as another source of SC leakage [40], [41], however, respond only to low-frequency transition of power currents. Si substrate backside facilitates the exploitation of SC leakages passively, in parallel, in a wide bandwidth and even at multiple points over the backside surface.

C. SIMULATION MODEL OF PASSIVE ATTACKS

The passive SC leakages on Si substrate stem mainly from power current of ToE. We have established a simulation framework that utilizes the power current model shown in Fig. 5 [42]. The model contains two submodels of active power current and passive power network. The former uses a power library and is derived in the time domain per an active operation of ToE, e.g., a crypto processor, with a given test vector or an operation scenario. The latter uses a process design kit (PDK) and is extracted statically from the physical design of ToE with respect to the impedance network of PDN.

The power current signatures (piecewise linear time-domain waveforms) are simulated for every logic element in a given logic cell library with all possible input/output conditions according to its truth table and recorded in a power library. For the higher level of accuracy, the logic element is designed at the transistor level and assumes the parametric variations of input skew, input slew, output fanout, as well as the natural variations of power supply voltage, temperature, and device parameters, in the collection of power current signatures using an industry-standard circuit simulator, e.g., SPICE. The parasitic passive components surrounding transistors, associated with p-type (P) and n-type (N) wells and P/N junctions are involved. The power library is reusable and called in the calculation of a power current waveform for a logic design with a given input test vector, according to the toggle records among gate elements derived in gate-level logic simulation in the time domain.

The power current simulation, using the power library, is universally helpful for pre-Silicon evaluation of SC leakages over Si substrate backside.

First, V_{PSUB} waveforms are obtained by a circuit simulator with the combined netlist of power current and power network models. Here, V_{DD} and V_{SS} domains additionally involve multiple layers with resistive and capacitive parameters that are discretized and calculated from the impurity profile associated with the Si substrate. The V_{PSUB} waveforms among the points of interest on the Si backside surface are processed for CPA of SC leakage.

Second, the magnetic flux density, $B(r)$, is computed from the current density, I, flowing over the metal wires of PDN, following to Biot–Savart law, at the point of r in the proximate space to the Si backside surface. The power current simulation provides I_i on each fragment i of PDN and brings about $B(r)$ by integrating the contributions of I_i over the entire PDN. The distribution in space and the direction of vectors are characterized for $B(r)$ and related with CEMA of SC leakage [43], [44], [45].

Third, the power current is further resolved into the channel current of each transistor, I_{DS}, and then related with photon emission rates. The assumptions are made with the bremsstrahlung of the channel hot electron as the primary mechanism of photon emission [46] and the pixel size, such as 10 μm $\times$ 10 μm for the detectability of integrated photons by an image sensor. The resultant distribution and intensity of photon emissions penetrated out on the Si backside surface are used for CPEA of SC leakage [47].

Power current simulation is widely leveraged by the pre-Silicon evaluation of ToE for passive SC leakages with multiple physical properties observable on Si substrate backside. The simulation framework is built into the design environment of security IC chips and particularly helpful in exploring countermeasures at the physical design level.

D. ACTIVE ATTACKS

Security IC chips are exposed to active attacks through Si substrate backside, as depicted in Fig. 6. An adversary attempts to create bit flips or change analog values within ToEs. The vulnerability is known to some crypto algorithms against the analysis between the cipher correctly encrypted and the faulty cipher once a single bit or certain number of bits is intentionally changed. The analysis of difference among pairs of correct and faulty ciphers narrows the search space for secret key bytes, according to differential fault analysis (DFA). The active attempt is strongly advantageous for an adversary since there is no need of analog measurements

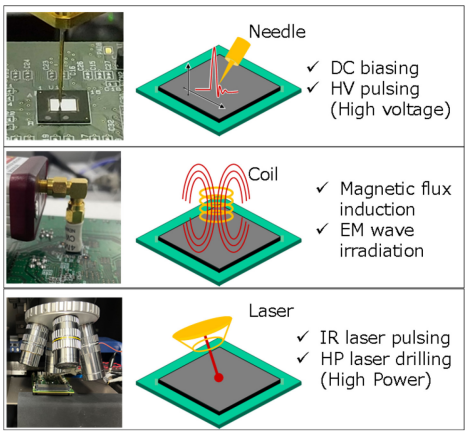

FIGURE 6. Active SCs on Si backside.

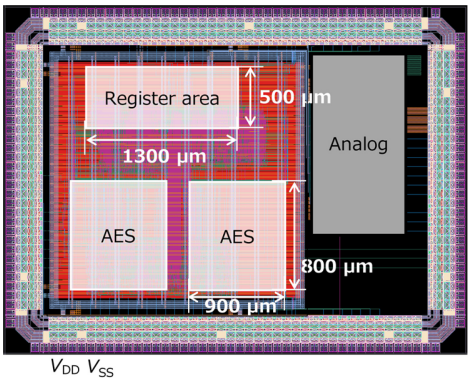

FIGURE 7. Test chip for HV pulsing on Si backside.

or characterization of physical properties. Once a faulty bit is injected in some physical methods (Fig. 6), the difference in output is available from digital interface. The fault injection attack (FIA) becomes more seriously concerned threats on security IC chips.

1) A conductive needle is attached on the surface of Si substrate backside and intentionally imposes DC voltage for biasing, AC voltage for modulation, or high-voltage (HV) pulses for disturbance. One can scan the point of injection over the full area of Si backside and see any change in digital output. The injected voltage travels through Si substrate to the area of transistors on the frontside and modulates the body voltage or induces the transient current flowing through P/N wells and junctions. This alters the threshold voltage of a transistor or the bias point of a circuit node.
2) An antenna or a coil is placed nearby the surface of Si substrate backside and irradiates EM wave with the high amplitude. One can change the position of antenna around the Si backside and see any change in digital output. The EM wave propagates through Si substrate to metallic interconnects on the frontside and induces current on wires. This current alters the bias point of a circuit node or influences the operation of circuits.

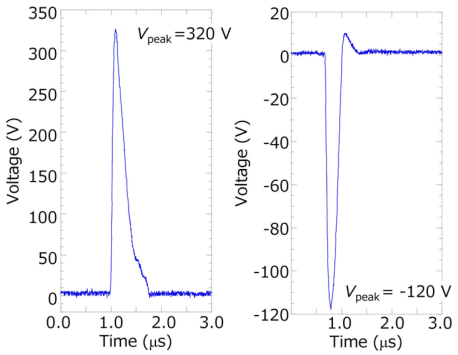

FIGURE 8. Waveforms of HV pulsing on Si backside.

3) IR laser is illuminated from the surface of Si substrate backside. One can change the angle and position of illumination and see any change in digital output. The IR ray penetrates to the transistors and creates hole–electron pairs at P/N wells and junctions. The resultant hole current and electron counterpart are, respectively, absorbed by either grounded or positively biased taps, flow into circuit nodes and affects the operation of circuits.

It is essentially attainable for a backside attack to create some changes proximately at the transistors of interest within ToE, thanks to the transparency of Si substrate, and the avoidance of obstacles from Si backside. Although physical medias are different, the faulty operation of circuits can be induced and makes FIA executable. The locality of focus, the efficacy and controllability of injection, and the cost of equipment are diversified. It is noted that the simulation model needs to be responsive for circuits to differently react against injected physical medias, therefore becomes more complex for active attacks than that for passive ones.

E. EXAMPLES OF ACTIVE ATTACKS

This section exemplifies some attack attempts with Si experiments.

1) HV pulsing is enabled by a switched capacitor-based electrical discharger and is tested over an IC chip of Fig. 7, using a 0.18-μm CMOS technology. The electronic charges on a capacitive storage flow into the primary coil of a transformer in an instant time, and the induced current on the secondary coil is then guided to the conductive needle either in the positive or in the negative direction [48]. The voltage at the attached point on the Si backside is observed by an oscilloscope, showing the voltage peak, V_{peak} of $+320$ and -120 V for the positive and negative direction, respectively, as plotted in Fig. 8. The duration of pulsing is around 500 ns. The magnitude of pulsing is mainly controlled by the charging voltage, V_{charge}, however, strongly affected by the parasitic contact impedance. HV pulsing was applied on Si backside within the area of registers, shown in Fig. 9, at the tap point chosen in the left center, middle center, and right

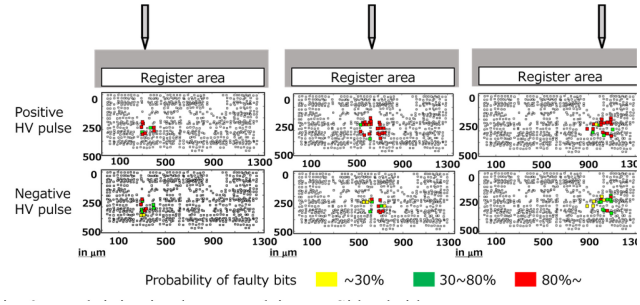

FIGURE 9. Fault injection by HV pulsing on Si backside.

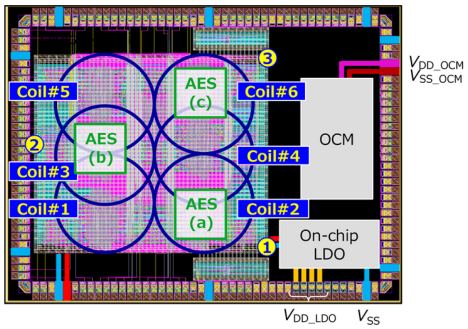

FIGURE 10. Test chip for EM irradiation on Si backside.

center of the area of 1300 μm in X-direction and 500 μm in Y-direction. The registers consist of flip flops with input signal and output signal chains. The clock signal was halted when pulsing was triggered. The rate of occurring faulty bits is calculated among flip flops after recursive measurements. The results are overlayed for each flip flop on the physical layout of register area. The locality of erroneous flip flops is confirmed for the respective tap positions, and similarly observed for both positive and negative HV pulsing. The tap point was set with the precision X-Y positioner on the area of crypto processors (128-bit AES cores) and searched for the position where the error is limited solely to a single byte among 16 bytes in the ninth clock cycle of AES operation. We have found such tapping positions differently for either positive or negative HV pulsing and finally disclosed all the 16 bytes of a secret key by DFA, as detailed in [49] and [50]. This proves the focused positioning of HV pulsing and the threat of Si backside FIA.

2) EM irradiation uses a solenoid that has either clockwise (CW) or counterclockwise (CCW) windings and connects to a pulse current generator for injecting magnetic flux. EM irradiation is experimented over another IC chip of Fig. 10 that integrates an array of three 128-bit AES cores. This chip is equipped with OCM to evaluate the voltage variation of V_{DD} nodes at the three different probed points on PDN, respectively, located nearby the AES cores of interest. The EM irradiation from the Si backside was performed at the six positions distributed over the digital area, with CW and CCW solenoids with the controlled voltage for pulse current generation of 300 and 350 V, respectively. The voltage variation induced on the PDN mesh was on-chip measured as in the plot of Fig. 11. It is of interest to note that the voltage waveform exhibits a negative-drop shape and supposed similarly to be a very large IR drop on V_{DD} nodes. The drop has the width of roughly 50 ns while widely varies for the height from the almost negligible level to more than 1 V (CW 300 V) or 0.5 V (CCW 350 V), without clear dependence on the position of a solenoid. The distribution of occurring faulty ciphers (bit errors) is given in Fig. 12 among the three AES cores. While the AES in the left middle exhibits errors with CW 300 V for all the solenoid positions, the other AES in the right top indicates them with CCW 350 V again among all the positions. Overall, the EM irradiation induces wide-area effects in terms of FIA and less position sensitive for DFA, particularly for Si backside attacks. The analytical understanding of EM coupling to CMOS devices remains actively investigated [51].

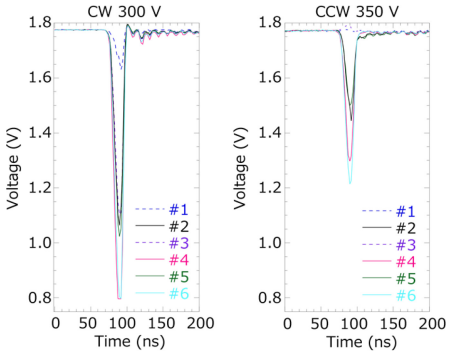

FIGURE 11. On-chip voltage waveforms induced by EM irradiation on Si backside.

3) Near infrared (NIR) exposure from Si backside was demonstrated with the OCM measurements of V_{PSUB} and V_{NWEL} on the front side of an IC chip. The drop height reaches as large as 500 mV or even larger (Fig. 19), depending on the power density of NIR exposure. The detailed measurements will be discussed in the next section.

III. COUNTERMEASURES

A. ATTACK PROTECTION

The buried PDN is investigated on Si backside among very advanced semiconductor technology nodes [52]. This allows power metals to be placed on Si backside and to avoid congestions on the frontside densely populated with signal wirings. This 3-D monolithic structure is expected to boost logic performance [53]. In contrast, Nagata et al. [25] have investigated the concurrent use of Si backside for PDN improvement as well as SC protection, as explained in the following two structures, which justifies the introduction of post-wafer (via-last) through Si via (TSV) manufacturing processes.

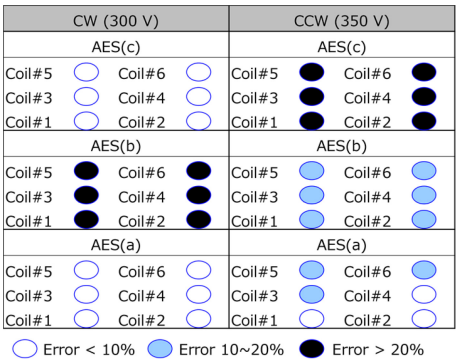

FIGURE 12. Fault injection by EM irradiation on Si backside.

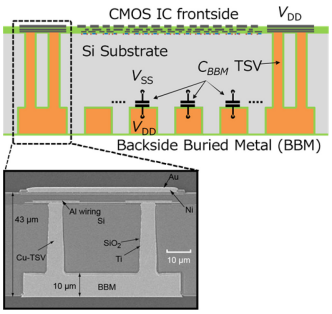

FIGURE 13. Si BBM structure.

It is also stated here that Si substrate voltage variations in the order of 20 mV enabled the correlation-based passive SC attacks among 10 000 waveforms. In contrast, the peak voltage magnitude reached several hundreds of mV around circuits for active Si backside injections for a single shot experiment. The large deviation in Si substrate voltage complicates the design of secure IC chips for tolerance against SC attack and prompts the deployment of advanced packaging as well as on-chip sensing for security.

1) The backside buried metal (BBM) structure of Fig. 13 [54] improved power delivery performance of a 3-D logic chip stack, with capacitors formed and distributed on the backside of Si substrate in each tier of the stack. The BBM structure also prevents secure IC chips from backside SC attacks [55].
2) The backside of Si substrate is bonded by a Si interposer having buried metal stripes, as shown in Fig. 14, for protection from backside SC attacks. We name this structure the backside bonded and buried metal stripes (triple b), TBM [56]. The geometry of meander stripes is patterned on Si interposer, through deeply perpendicular etching, oxide coating on the carved surface and followed by barrier metal formation, and then Cu plating to fill the stripes. The frontside of Si interposer with Cu stripes is glued to the backside of CMOS wafer through oxide-oxide direct bonding. Here, CMOS wafer is thinned and machined by TSV process with Cu filling, which enables to electrically connect the metal wires on the frontside of CMOS wafer and Cu meander strips by TBM. The meander is connected to the system ground via the frontside pads with bumps/balls. It is advantageous for a meander covering the whole die area that the cut of line at any place is detectable by sensing the flow of current through the meander. This is not possible with solid or mesh patterns.

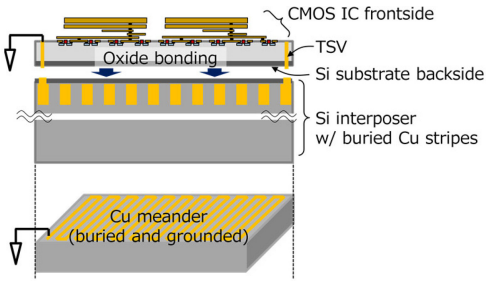

FIGURE 14. Si backside bonded and buried metal (TBM) structure.

BBM depth	10 μm
BBM width	15 μm
BBM space	10 μm
Si substrate thickness	40 μm

TBM depth	50 μm
TBM width	20 μm
TBM space	20 μm
Si interposer thickness	350 μm
Si substrate thickness	20 μm

FIGURE 15. Structural parameters of (a) BBM and (b) TBM.

The typical structural parameters are compared between BBM and TBM as in Fig. 15. For BBM, the two-step etching from Si backside and Cu plating monolithically form TSVs and stripes on CMOS wafer backside. Here, the depth of BBM is essentially limited and smaller than the thickness of a thinned Si substrate. In contrast, the structural parameters of TBM are decoupled from the geometry of TSVs on CMOS wafer, which allows the deeper and denser stripes. Further, TBM wafer with the larger thickness by bonding makes it easier than BBM thinned wafer to be handled in packaging and assembly processes.

The advantage of TBM over BBM is given in Fig. 16 for protection against IR irradiation from the Si backside. Since IR ray has directness, Cu stripes block the penetration when the direction of IR is normal to Si backside. While the regions on the frontside underneath Cu stripes are protected, the other regions not covered by Cu stripes are unprotected. Although this is the natural consequence of IR exposure, a designer could carefully utilize the protected areas in physical design. One example is to place the secure circuit components, e.g., key registers and state counters in the areas of backside Cu stripes.

The oblique incidence of IR ray shrinks the protectable regions. In contrast to BBM, the deeper and denser TBM stripes mitigate this effect of oblique incidence and tolerate even for multiple reflections on their sidewalls.

The cross section of TBM sample is given in Fig. 17. CMOS wafer with TSV is bonded by Si interposer with TBM. The thickness of CMOS wafer and Si interposer is 20 and 375 μm, respectively, and the total thickness of

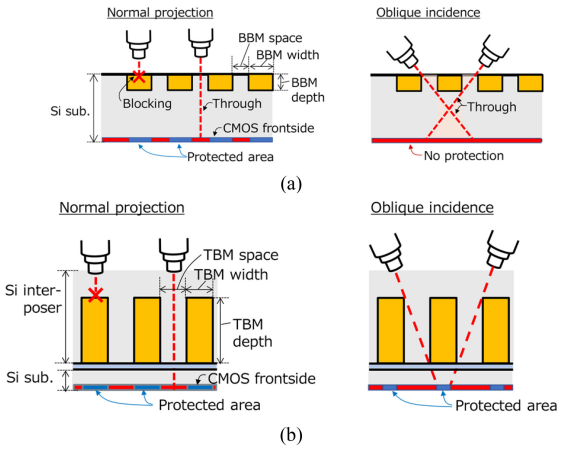

FIGURE 16. Blockage of IR laser exposure. (a) BBM. (b) TBM.

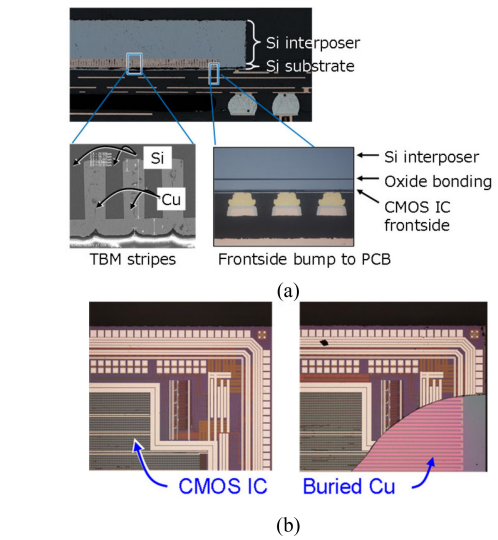

FIGURE 17. TBM demonstrator: (a) Cross-sectional and (b) horizontal photos.

roughly 400 μm facilitates post-wafer assembly with bumps to a plastic interposer and balls to PCB. We only see CMOS circuits on the frontside photo, however, TBM meander appears when CMOS chip is broken. The thinned CMOS is fragile and hampers the attempts of reverse engineering.

B. ATTACK DETECTION

OCM captures voltage variations on V_{DD} and V_{SS} of PDN and V_{SUB} of the entire chip. The trends in time and the distribution in space are evaluated to find anomalous behaviors potentially associated with adversarial attempts. Chip-level measurements of induced voltage by HV pulsing and by NIR exposure are directly measured by OCM. Digital monitors [57], [58] use the variation of logic timings within the digital leaf cells in series, in response to power voltage changes induced similarly by such exposures. Once the chip detects undesired voltage variations, the security functionality will become halted or move to an emergency mode with randomized outputs.

OCM measurements of V_{NWEL} provide waveforms under NIR exposure from Si backside, as in the experimental setup

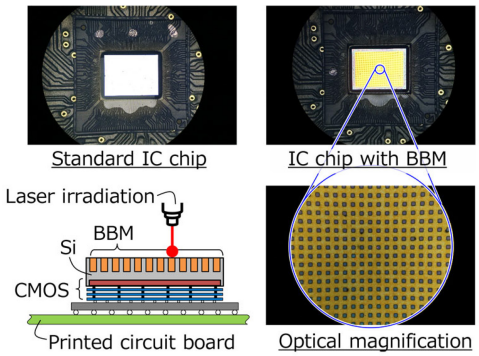

FIGURE 18. NIR exposure on Si backside and blockage by BBM.

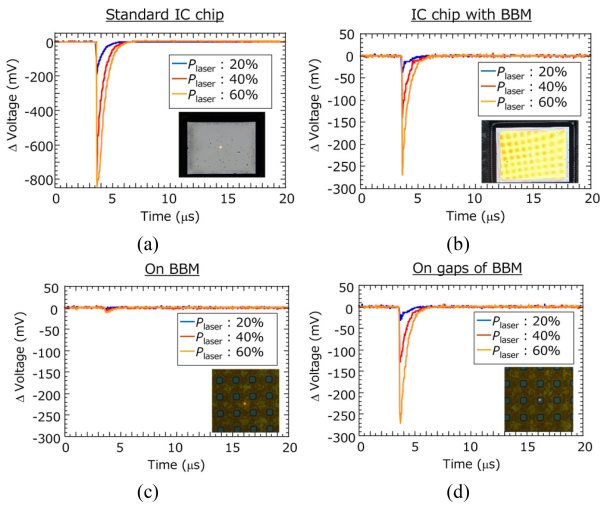

FIGURE 19. On-chip voltage waveforms induced by NIR exposure on Si backside with (a) and (b) wide aperture and (c) and (d) narrow aperture.

of Fig. 18. The voltage drop induced on V_{NWEL}, which is nominally biased at V_{DD}, becomes larger for the higher level of NIR power density. In comparison to the conventional CMOS chip [Fig. 19(a)], the drop is roughly 65% attenuated for the chip having the mesh of BBM stripes [Fig. 19(b)], where the entire chip is widely exposed by NIR laser. The drop is blocked by BBM stripes [Fig. 19(c)] once NIR aperture is narrowed to the width of BBM stripes. The drop enlarges when NIR laser spots the gap of BBM stripes [Fig. 19(d)] to the similar level when the entire chip is exposure.

TBM meander is not seen by visible lights from the backside of Si interposer. An adversary may approach, drill or grind the Si backside without looking, and then cut the stripe to make holes. The embedded line-cut sensor of Fig. 20 detects the attempt, according to the time chart in the figure. The physical implementation is outlined in Fig. 21. The capacitors are created by using the sidewall capacitances of TBM stripes. The circuit components of the detector are placed on CMOS chip within the protected regions under the TBM strips, so as not being broken by laser exposures.

The operation of line-cut sensor is summarized as follows.

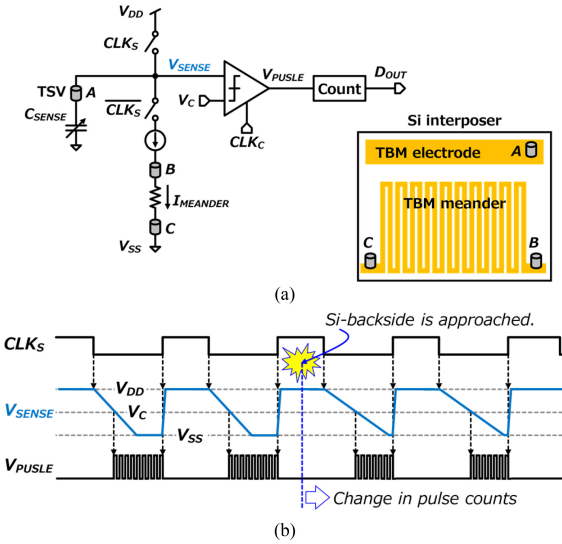

FIGURE 20. Si-backside approach and line-cut detector using TBM capacitor and TBM meander, (a) circuit schematic and (b) timing diagram.

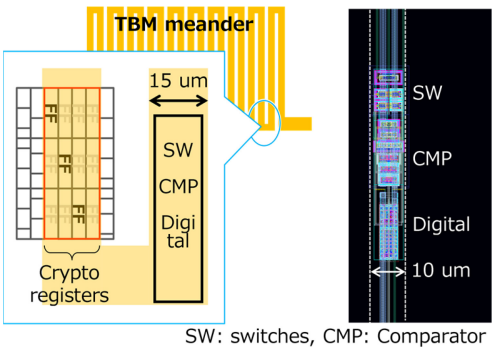

FIGURE 21. Physical layout hidden by TBM.

1) The capacitor C_{SENCE} is charged to V_{DD} when the system clock CLK_S is high.
2) The capacitor C_{SENCE} is discharged with the constant drain current when CLK_S is low.
3) The voltage level of V_{SENCE} reduced and becomes below the reference level of V_C of the comparator working with the comparator clock CLK_C.
4) The number of output pulses from the comparator is calculated.

The output code is stably constant in normal environment, as sketched in Fig. 20(b) and also in Fig. 22. Once an adversary approaches, the stray and coupling capacitance alters the effective size of C_{SENCE} and the output code starts to deviate. Further, once an adversary cut the meander, the output code is fixed at the lowest. These are detectable by seeing the output. In addition, TBM meander and capacitor shield outgoing and incoming EM waves and mitigate passive and active EM SC attacks.

IV. CONCLUSION

It is imperative to protect security IC chips from passive and active SC attacks. IC chips in advanced packaging expose Si backside to adversarial attempts using voltage probing, EM waves, and NIR lasers. The attack mechanisms and equipment are detailed and exemplified with Silicon demonstrators. Attack protection and detection use 3-D monolithic structure, such as BBM and TBM, which is generally effective against the SC attacks in passive and active manners with voltage pulse, EM and photons. Further experiments will be pursued.

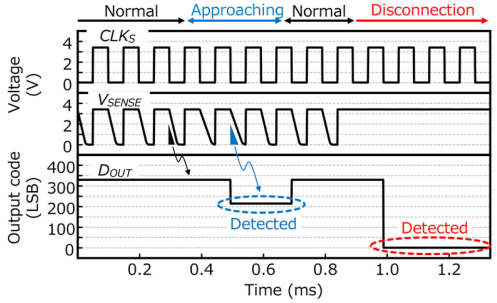

FIGURE 22. Simulated waveforms of operation.

ACKNOWLEDGMENT

The authors thank Dr. Kazuki Monta, Mr. Takuya Wadatsumi, and Mr. Rikuu Hasegawa for scientific discussions.

REFERENCES

[1] P. Kocher, "Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems," in *Proc. Annu. Int. Cryptol. Conf.*, Aug. 1996, pp. 104–113.
[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. IACR CRYPTO*, 1999, pp. 388–397.
[3] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks—Revealing the Secrets of Smart Cards*. New York, NY, USA: Springer, 2007.
[4] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for fault," in *Proc. IACR EUROCRYPT*, May 1997, pp. 37–51.
[5] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *Proc. IACR CRYPTO*, Aug. 1997, pp. 513–525.
[6] I. Verbauwhede, *Secure Integrated Circuits and Systems*. New York, NY, USA: Springer, 2010.
[7] N. Sklavos, R. Chaves, G. D. Natale, and F. Regazzoni, Eds., *Hardware Security and Trust, Design and Deployment of Integrated Circuits in a Threatened Environment*. Cham, Switzerland: Springer, 2017.
[8] C. H. Chang and Y. Cao, Eds., *Frontiers in Hardware Security and Trust; Theory, Design and Practice*. London, U.K.: IET, 2020.
[9] "The common criteria." Accessed: Nov. 1, 2024. [Online]. Available: https://www.commoncriteriaportal.org/index.cfm
[10] "Security requirements for cryptographic modules." Accessed: Nov. 1, 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/140-3/final
[11] S. Nikova et al., "Threshold implementations against side-channel attacks and glitches," in *Proc. Int. Conf. Inf. Commun. Secur.*, 2006, pp. 529–545.
[12] H. Gross et al., "Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order," ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2016/486, 2016.
[13] K. Tiri et al., "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. IEEE DATE*, 2004, pp. 246–251.
[14] K. Tiri and I. Verbauwhede, "A digital design flow for secure integrated circuits," *IEEE Trans. Comput.-Aided Design Integr Circuits Syst.*, vol. 25, no. 7, pp. 1197–1208, Jul. 2006. doi: 10.1109/TCAD.2005.855939.
[15] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," *IEEE J. Solid-State Circuits,* vol. 53, no. 8, pp. 2399–2414, Aug. 2018. doi: 10.1109/JSSC.2018.282269.

[16] D. Das et al., "EM and power SCA-resilient AES-256 through >350× current-domain signature attenuation and local lower metal routing," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, Jan. 2021. doi: 10.1109/JSSC.2020.3032975.

[17] R. Kumar et al., "A time-/frequency-domain side-channel attack resistant AES-128 and RSA-4K crypto-processor in 14-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 56, no. 4, pp. 1141–1151, Apr. 2021. doi: 10.1109/JSSC.2021.3052146.

[18] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-STELLAR: An EM/power SCA-resilient AES-256 with synthesis-friendly signature attenuation," *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, Jan. 2022. doi: 10.1109/JSSC.2021.311333.

[19] 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, Dec. 2009. doi: 10.1109/JSSC.2009.203408.

[20] N. Miura, D. Fujimoto, R. Korenaga, K. Matsuda, and M. Nagata, "An intermittent-driven supply-current equalizer for 11× and 4× power-overhead savings in CPA-resistant 128bit AES cryptographic processor," in *Proc. IEEE Asian Solid-State Circuits*, Nov. 2014, pp. 225–228, doi: 10.1109/ASSCC.2014.700890.

[21] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in *Proc. IACR CHES*, Aug. 2010, pp. 320–334.

[22] 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*, Sep. 2011, pp. 292–311.

[23] A. Beckers, S. Guilley, P. Maurine, C. O'Flynn, and S. Picek, "(Adversarial) electromagnetic disturbance in the industry," *IEEE Trans. Comput.*, vol. 72, no. 2, pp. 414–422, Feb. 2023, doi: 10.1109/TC.2022.3224373.

[24] D. Karaklajić, 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. doi: 10.1109/TVLSI.2012.223170.

[25] M. Nagata, T. Miki, and N. Miura, "Physical attack protection techniques for IC chip level hardware security," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 1, pp. 5–14, Jan. 2022. doi: 10.1109/TVLSI.2021.307394.

[26] M. Nagata, N. Miura, and T. Miki, "Analog techniques for digital security," *IEEE Solid-State Circuits Mag.*, vol. 15, no. 1, pp. 25–31, Jan. 2023. doi: 10.1109/MSSC.2022.321978.

[27] 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, doi: 10.1109/TCSII.2019.2901534.

[28] T. Jeong, A. P. Chandrakasan, and H.-S. Lee, "S2ADC: A 12-bit, 1.25-MS/s secure SAR ADC with power side-channel attack resistance," *IEEE J. Solid-State Circuits*, vol. 56, no. 3, pp. 844–854, Mar. 2021, doi: 10.1109/JSSC.2020.3027806.

[29] M. Ashok, E. V. Levine, and A. P. Chandrakasan, "Randomized switching SAR (RS-SAR) ADC for power and EM side-channel security," *IEEE Solid-State Circuits Lett.*, vol. 5, pp. 247–250, 2022, doi: 10.1109/LSSC.2022.3211705.

[30] R. Takahashi, T. Miki, and M. Nagata, "An analog side-channel attack on a high-speed asynchronous SAR ADC using dual neural network technique," *IEICE Trans. Electron.*, vol. E106.C, no. 10, pp. 565–569, Oct. 2023, doi: 10.1587/transele.2022CTS0002.

[31] J. H. Lau, "Recent advances and trends in multiple system and heterogeneous integration with TSV-less interposers," *IEEE Trans. Compon., Packag. Manuf. Technol.*, vol. 12, no. 8, pp. 1271–1281, Aug. 2022. doi: 10.1109/TCPMT.2022.319437.

[32] J. H. Lau, "Recent advances and trends in multiple system and heterogeneous integration with TSV interposers," *IEEE Trans. Compon., Packag. Manuf. Technol.*, vol. 13, no. 1, pp. 3–25, Jan. 2023. doi: 10.1109/TCPMT.2023.323400.

[33] M. Nagata, "Design of circuits and packaging systems for security chips," *IEICE Trans. Electron.*, vol. E106.C, no. 7, pp. 345–351, Jul. 2023. doi: 10.1587/transele.2022CDI000.

[34] 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. doi: 10.1109/43.848088.

[35] D. Fujimoto et al., "Side-channel leakage on silicon substrate of CMOS cryptographic chip," in *Proc. IEEE Int. Symp. Hardw., Oriented Security Trust (HOST),* May 2014, pp. 32–37, doi: 10.1109/HST.2014.6855564.

[36] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Proc. Int. Workshop Cryptogr. Hardw. Embed. Syst. (CHES)*, 2001, pp. 251–261, doi: 10.1007/3-540-44709-1_21.

[37] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side—Channel(s)," in *Proc. Int. Workshop Cryptogr. Hardw. Embed. Syst. (CHES)*, 2003, pp. 29–45, doi: 10.1007/3-540-36400-5_4.

[38] S. Tajik et al., "Photonic side-channel analysis of arbiter PUFs," *J. Cryptol.*, vol. 30, pp. 550–571, Apr. 2017, doi: 10.1007/s00145-016-9228-.

[39] J. Di-Battista, J. C. Courrege, B. Rouzeyre, L. Torres, and P. Perdu, "When failure analysis meets side-channel attacks," in *Proc. Int. Workshop Cryptogr. Hardw. Embed. Syst. (CHES)*, 2010, pp. 188–202, doi: 10.1007/978-3-642-15031-9_1.

[40] J. Brouchier, T. Kean, C. Marsh, and D. Naccache, "Temperature attacks," *IEEE Security Privacy*, vol. 7, no. 2, pp. 79–82, Mar./Apr. 2009, doi: 10.1109/MSP.2009.5.

[41] N. Chang et al., "ML-augmented methodology for fast thermal side-channel emission analysis," in *Proc. 26th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2021, pp. 463–468, doi: 10.1145/3394885.343164.

[42] 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. doi: 10.1109/LEMCPA.2020.297862.

[43] D. Poggi, T. Ordas, A. Sarafianos, and P. Maurine, "Checking robustness against EM side-channel attacks prior to manufacturing," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 5, pp. 1264–1275, May 2022. doi: 10.1109/TCAD.2021.309229.

[44] D. Das et al., "EM SCA white-box analysis-based reduced leakage cell design and presilicon evaluation," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 11, pp. 4927–4938, Nov. 2022. doi: 10.1109/TCAD.2022.314436.

[45] K. Monta et al., "Silicon-correlated simulation methodology of EM side-channel leakage analysis," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 19, no. 1, pp. 1–23, Jan. 2023. doi: 10.1145/356895.

[46] S. Tam and C. Hu, "Hot-electron-induced photon and photocarrier generation in silicon MOSFET's," *IEEE Trans. Electron Devices*, vol. 31, no. 9, pp. 1264–1273, Sep. 1984. doi: 10.1109/T-ED.1984.2169.

[47] H. Li et al., "Photon emission modeling and machine-learning assisted pre-silicon optical side-channel simulation," in *Proc. IEEE Int. Symp. Hardw. Oriented Security Trust (HOST)*, May 2024, pp. 107–111, doi: 10.1109/HOST55342.2024.1054541.

[48] T. Wadatsumi et al., "Experimental exploration of the backside ESD impacts on an IC chip in flip chip packaging," *IEICE Trans. Electron.*, vol. E106.C, no. 10, pp. 556–564, Oct. 2023. doi: 10.1587/transele.2022CTP000.

[49] T. Wadatsumi et al., "Chip-backside vulnerability to intentional electromagnetic interference in integrated circuits," *IEEE Trans. Electromagn. Compat.*, vol. 66, no. 5, pp. 1556–1566, Oct. 2024, doi: 10.1109/TEMC.2024.344091.

[50] Y. Hayashi, R. Hasegawa, T. Wadatsumi, K. Monta, T. Miki, and M. Nagata, "Fault injection attacks exploiting high voltage pulsing over Si-substrate backside of IC chips," in *Proc. IEEE Fault Diagn. Toler. Cryptogr. (FDTC)*, Sep. 2024, pp. 44–52.

[51] R. Hasegawa, K. Monta, T. Wadatsumi, T. Miki, and M. Nagata, "On-chip evaluation of voltage drops and fault occurrence induced by Si backside EM injection," in *Proc. Int. Workshop Constr. Side-Channel Anal. Secure Design (COSADE)*, Apr. 2024, pp. 22–37, doi: 10.1007/978-3-031-57543-3_.

[52] D. Prasad et al., "Buried power rails and back-side power grids: Arm® CPU power delivery network design beyond 5nm," in *Proc. IEEE Int. Electron Devices Meeting (IEDM)*, Dec. 2019, pp. 19.1.1–19.1.4, doi: 10.1109/IEDM19573.2019.8993617.

[53] M. O. Hossen, B. Chava, G. Van der Plas, E. Beyne, and M. S. Bakir, "Power Delivery Network (PDN) modeling for backside-PDN configurations with buried power rails and μ TSVs," *IEEE Trans. Electron Devices*, vol. 67, no. 1, pp. 11–17, Jan. 2020. doi: 10.1109/TED.2019.2954301.

[54] 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. doi: 10.1109/TED.2021.305822.

[55] 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. doi: 10.1109/JSSC.2020.300577.

[56] T. Wadatsumi, R. Hasegawa, K. Monta, T. Okidono, T. Miki, and M. Nagata, "A Si-interposer with buried Cu metal stripes and bonded to Si-substrate backside for security IC chips," in *Proc. IEEE Electron. Compon. Technol. Conf. (ECTC)*, Jun. 2023, pp. 951–954, doi: 10.1109/ECTC51909.2023.0016.

[57] M. T. H. Anik, J.-L. Danger, S. Guilley, and N. Karimi, "Detecting failures and attacks via digital sensors," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 7, pp. 1315–1326, Jul. 2021, doi: 10.1109/TCAD.2020.3020921.

[58] M. Ebrahimabadi et al., "DELFINES: Detecting laser fault injection attacks via digital sensors," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 43, no. 3, pp. 774–787, Mar. 2024, doi: 10.1109/TCAD.2023.3322623 .

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 with Hiroshima University from 1994 to 2002, an Associate Professor with Kobe University, Kobe, Japan, from 2002 to 2009, where he was promoted to a Full Professor in 2009. 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, 2.5-D and 3-D system integration, as well as their applications for hardware security and hardware safety, and cryogenic electronics for quantum computing.

Dr. Nagata chaired the Technology Directions subcommittee for International Solid-State Circuits Conference (2018–2022) and has been serving as an Executive Committee Member since 2023. He was the Technical Program Chair (2010 and 2011), the Symposium Chair (2012 and 2013), and an Executive Committee Member (2014 and 2015) for the Symposium on VLSI circuits. He is the Conference General Chair for AsianHOST 2024. He was the IEEE Solid-State Circuits Society AdCom Member (2020–2022), the Distinguished Lecturer (2020, 2021, and since 2024), and has been serving as the Chapters Vice Chair since 2022 of the society. He has been an Associate Editor for IEEE Transactions on VLSI Systems since 2015. 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 (2014–2022), European Solid-State Circuits Conference (2020–2022), and many others. He is a Senior Member of IEICE, and currently the President of Electronics Society, IEICE (2024).

TAKUJI MIKI (Member, IEEE) received the Ph.D. degree from Kobe University, Kobe, Japan, in 2017.

From 2006 to 2017, he was with Panasonic Corporation, Osaka, Japan, where he was involved in the development of analog and mixed-signal integrated circuits for consumer and industrial applications. He is currently an Associate Professor with the Graduate School of Science, Technology and Innovation, Kobe University. His current research interests include data converters, and hardware security and cryogenic CMOS circuits for quantum computers.

Dr. Miki is currently serving as a member of technical program committees for the IEEE Asian Solid-State Circuits Conference and the IEEE European Solid-State Circuits Conference.