Si-Backside Protection Circuits Against Physical Security Attacks on Flip-Chip Devices

Miki, Takuji ; Nagata, Makoto ; Sonoda, Hiroki ; Miura, Noriyuki ; Okidono, Takaaki ; Araga, Yuuki ; Watanabe, Naoya ; Shimamoto, Haruo ;…

(Citation)
IEEE Journal of Solid-State Circuits,55(10):2747-2755

(Issue Date)
2020-07-17

(Resource Type)
journal article

(Version)
Version of Record

(URL)
https://hdl.handle.net/20.500.14094/0100476386

Si-Backside Protection Circuits Against Physical Security Attacks on Flip-Chip Devices

Takuji Miki, *Member, IEEE*, Makoto Nagata, *Senior Member, IEEE*, Hiroki Sonoda, *Member, IEEE*, Noriyuki Miura, *Member, IEEE*, Takaaki Okidono, Yuuki Araga, *Member, IEEE*, Naoya Watanabe, *Member, IEEE*, Haruo Shimamoto, and Katsuya Kikuchi, *Member, IEEE*

***Abstract*— This article presents a cryptographic key protection technique from physical security attacks through Si-backside of IC chip. Flip-chip packaging leads to a serious security hole that allows emerging backside physical security attacks. The proposed backside buried metal (BBM) structure forming a meander wire pattern on the Si-backside detects unexpected disconnection of the meander and warns the malicious attempts to expose a vulnerable Si substrate. Moreover, the BBM meander also shields key information of cryptographic circuit from both passive side-channel attacks and active laser fault injection as well. Unlike other conventional laminate-based protection, this backside monolithic approach does not require frontside wiring resources or additional packaging layers, resulting in only 0.0025% size-overhead. The BBM meander was formed on the backside of a 0.13-μm CMOS cryptographic chip by wafer-level via-last BBM processing.**

***Index Terms*— Hardware security, laser fault injection (LFI), physical security attack, side-channel attack (SCA).**

I. Introduction

With the rapid growth of Internet of Things (IoTs) applications and devices, data security has been a major issue since IoT edge devices acquire confidential and privacy information and export it to the cloud network. The network data security is ensured by cryptography at the edge devices, based on digital encryption algorithms for data protection and digital signature algorithms for device authentication [1]. However, they are exposed to physical security attacks because malicious attackers can physically access to the distributed edge devices to steal a secret key by exploring side-channel information leakages, through passively measuring power supply noise or electromagnetic (EM) radiation [2], or actively injecting logical faults with laser or high-power EM irradiation [3]. These attacks target an IC chip rather than signal wiring on-board because it is necessary for attackers to extract a cryptographic key in order to steal or tamper with data instead of simply destroying it. To protect an IC chip from these attacks, various countermeasures have been reported. An active secure shield proposed in [4] detects physical intrusion inside the chip by monitoring encrypted signal-carrying wires on the top metal layers. A probing detection scheme reported in [5] also detects the physical approach by sensing capacitance variation. However, these techniques only counter the attacks from the frontside (surface) of an IC chip.

As the other feature of IoT devices, flip-chip packaging is often used since these devices prefer the smaller form factor even with more functionality and lower power. Flip-chip can be implemented with thin and almost chip scale packaging; however, it exposes the Si substrate to the surface of an IC chip, which leads a serious security hole. For example, side-channel noise to identify a key information is potentially leaked from the Si substrate, and laser also penetrates it and easily reaches the target core [6], [7]. Thus, a Si-backside protection technique is needed to defend the cryptographic core against the backside physical attacks. The active top-metal shield technique can also be used for backside protection by bonding two dies back-to-back [8] and, also, a breakable die with an exotic film lamination structure impedes backside physical attacks [9]. However, they require additional die or layer, which causes an increase in the size of an IC chip.

In this article, a chip-size-efficient countermeasure against backside physical attacks is presented [10]. A backside buried metal (BBM) structure forming a meander pattern is newly proposed to detect physical backside attacks such as laser-cutting, polishing, and milling without chip size-overhead. The BBM also protects a secret key of cryptography from side-channel information analysis with direct probing on Si-substrate by reducing substrate noise leakage. Since a laser cannot penetrate the Cu wiring, this structure can protect the cryptographic core from fault injection attack by laser irradiation. Since the BBM is fabricated by adding a few processes to a silicon via forming process, the manufacturing cost does not increase significantly. A prototype cryptographic chip with the meander BBM demonstrates secure characteristics against above attacks.

Manuscript received January 31, 2020; revised April 4, 2020; accepted May 19, 2020. Date of publication July 17, 2020; date of current version September 24, 2020. This article was approved by Guest Editor Atsushi Kawasumi. This work was supported in part by the Cabinet Office (CAO) through the Cross-Ministerial Strategic Innovation Promotion Program (SIP) "Cyber-Security for Critical Infrastructure" [funding agency: New Energy and Industrial Technology Development Organization (NEDO)]. *(Corresponding author: Takuji Miki.)*

Takuji Miki, Makoto Nagata, and Hiroki Sonoda are with the Graduate School of Science, Technology and Innovation, Kobe University, Kobe 657-8501, Japan (e-mail: miki@cs26.scitec.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.

Takaaki Okidono is with ECSEC, Tokyo 101-0054, Japan.

Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, and Katsuya Kikuchi are with the National Institute of Advanced Industrial Science and Technology, Tsukuba 305-8560, Japan.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSSC.2020.3005779

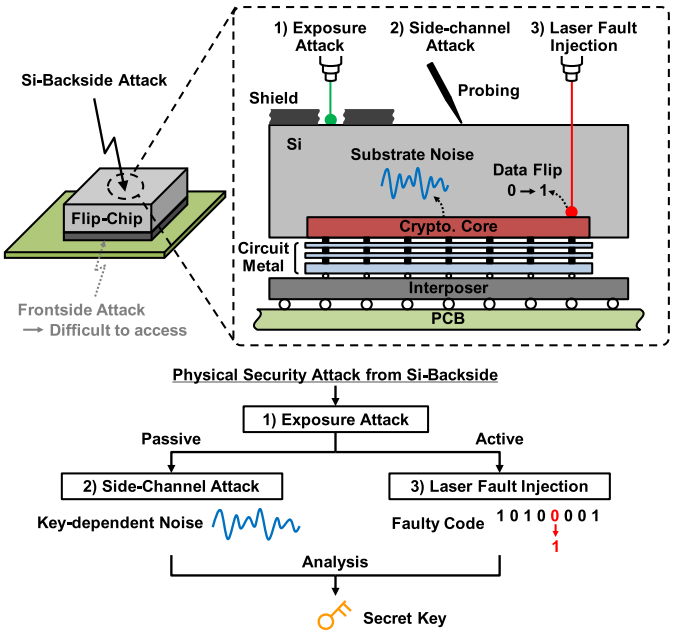

Fig. 1. Backside physical attacks on flip-chip.

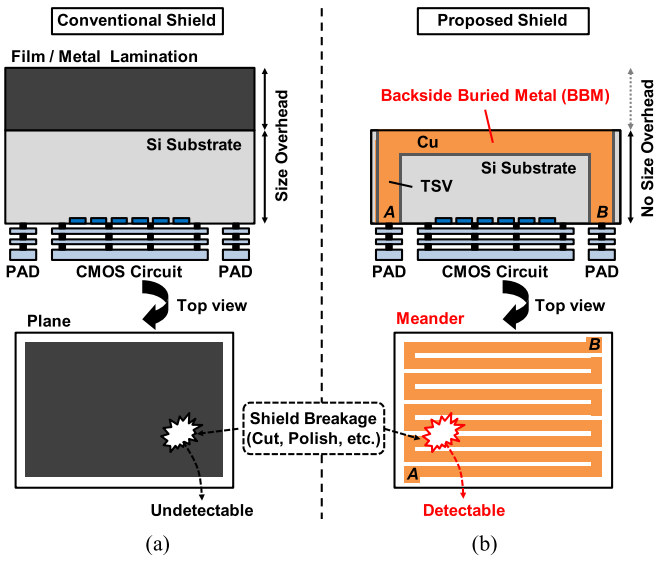

Fig. 2. Countermeasure against Si-backside physical attack. (a) Conventional and (b) proposed shield structure.

This article is an extension of [10], where the more detailed shield structure with manufacturing process and analysis for physical backside attack resistances are provided. Furthermore, the frontside CMOS circuit details and design guideline of BBM patterns are introduced. The rest of this article is organized as follows. Section II describes an overview of the physical security attacks from the Si-backside of IC chips. Section III presents the detail of the proposed protection structure and each mechanism of countermeasure against physical backside attacks including disconnection, side-channel attack (SCA), and laser fault injection (LFI). Section IV shows circuit design of a prototype chip. Experimental results for evaluation of each attack resistance are demonstrated in Section V. Finally, Section VI gives the conclusion.

II. Si-Backside Security Attacks

Fig. 1 shows the attacking scheme from the Si-backside of flip-chip ICs. The front side of IC chip has various obstacles to probing or laser irradiation such as unrelated circuit metals and an interposer board, which makes physical attacks from the top side of IC chip difficult. On the other hand, since there is nothing between the backside of the IC chip and the circuit transistors except for Si substrate, the attackers can directly access to the target core from the outside of the chip and easily steal the cryptographic key through Si substrate. Generally, the back of an IC chip is covered with a plastic package, and sometimes a chemical or metallic shield is also applied to prevent those attacks. Thus, attackers first need to remove them to expose Si substrate to the external surface of chip, for instance, by using a laser cutter. After removing the shield, there are two types of physical attacks. One is to passively probe an internal substrate noise during cryptographic operation and estimate secret key by analyzing the key-dependent noise, which is widely known as SCAs [2]. The other is to actively inject the fault such as data flip of registers by irradiating laser to the target flip-flops, and find the key using the faulty code for differential fault analysis [11]. This attack is called LFI. Both attacks are typically executed from the frontside of the chip; however, the backside SCA or LFI can be performed without interruption by circuit elements, which enhances the attack flexibility.

III. Protection Circuits Against Si-Backside Physical Security Attacks

To protect the cryptographic core from the serious backside attacks, a physical secure shield circuit is developed. In addition to the property that disables the backside SCA and LFI, the shield must be unremovable structure for a countermeasure against the exposure attack. However, malicious attackers can use a laser cutter system or mechanical polishing equipment to forcefully remove the shield, which makes difficult to develop physically unremovable structure. Thus, the proposed secure circuit has a function to detect the exposure attacks such as shield disconnection by cutting or polishing, and warn the malicious attempt to the user. Sections III-A–III-D describe the proposed shield structure as well as the operation details of countermeasure against the backside attacks including exposure, SCA, and LFI.

A. BBM Structure

Fig. 2 shows the shield structure for protection from the backside physical attacks. The conventional shield structures employ additional packaging materials, as shown in Fig. 2(a). The film lamination technique blocks laser [9], and metal or absorbing material coating techniques suppress noise emanating from the chip [12], [13]. These approaches increase the chip size by the thickness of the shield. It makes a non-negligible impact especially on IoT devices which are required to be as small as possible. Besides, a plane or

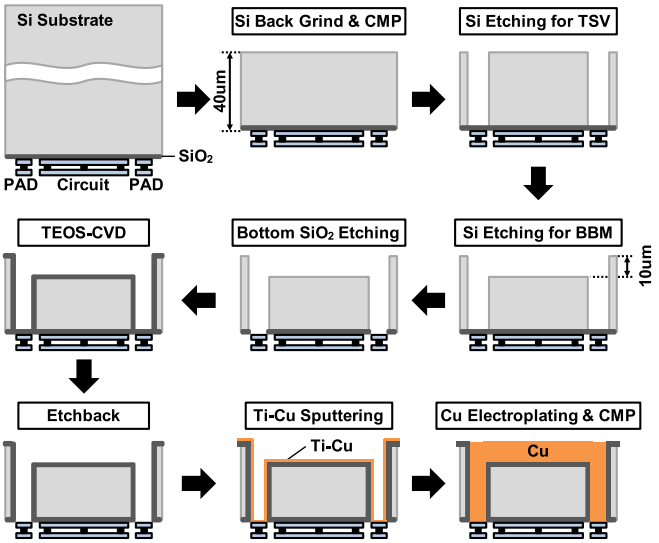

Fig. 3. Process flow of BBM and TSV.

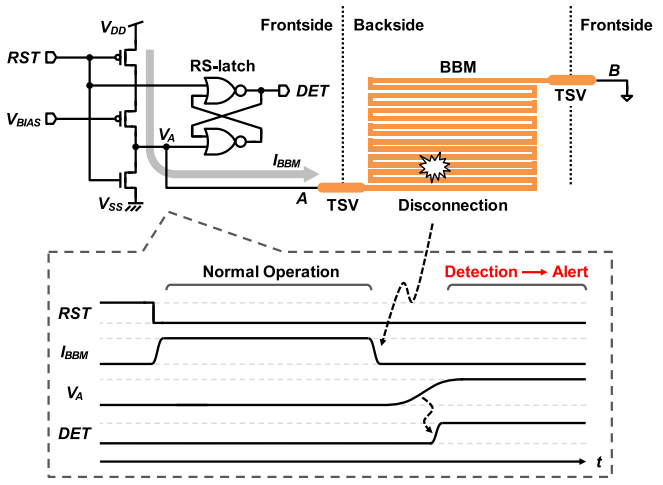

Fig. 4. Proposed disconnection detector circuit.

mesh pattern is often applied to the shield [13]; however, it cannot detect a breakage caused by attacker's malicious attempt to remove the shield using strong laser or focused ion beam (FBI) irradiation. Fig. 2(b) shows the proposed shield structure with BBM covering the backside of IC chip. Since Cu metal is buried in the existing Si substrate, there is no chip size overhead. The BBM forms a meander pattern and is connected to the surface CMOS circuit through Si vias (TSVs) under IO pads. A small current flows from the frontside CMOS circuit to the BBM meander, which enables to detect a disconnection by monitoring the current stop. Thus, the width of the current path should be narrow to be cut by the exposure attack. A meander pattern is, therefore, applied to the current path on BBM, not a plane or wide wiring pattern, to cover an entire chip and protect it from the physical attacks. Moreover, the BBM meander pattern can be drawn with fine pitch; thus, the monolithic shield structure remains the blocking effect of noise and laser. These details will be explained in Sections III-B–III-D.

The BBM and TSVs are fabricated with via-last process [14] as illustrated in the simplified flow of Fig. 3. Si substrate is generally thick enough with more than 300 μm even though it has no special circuit function. Thus, for the first process, the wafer is thinned down to 40 μm by Si back grinding and chemical mechanical polishing (CMP). Then, Si etching process is performed in two stages. After photolithography, the first Si etching is processed, and through holes for TSVs with 40 μm, depth is created. Next, Si is etched for BBM after ashing and photolithography. The thickness of etched Si for BBM forming is approximately 10 μm. After removing TSV bottom SiO_2 by etching, Tetraethoxysilane (TEOS)-Chemical Vapor Deposition (CVD) is executed for electrical isolation of Si substrate. Then, etch-back is carried out to remove the SiO_2 at the bottom of the TSVs and create an electrical contact between TSV and frontside CMOS circuit. Then, Ti–Cu sputtering is performed for a diffusion barrier between Cu and Si substrate. Finally, Cu electroplating is executed, and BBM is formed.

B. Backside Exposure Attack Detection

Fig. 4 depicts the circuit schematic and operation waveforms of the proposed disconnection detector. Only three transistors and one latch cell are used to detect the disconnection of BBM meander caused by the exposure attack. The detector circuit is connected through the TSVs to the BBM covering the entire area on the back of the chip with meander pattern. When the reset signal *RST* is "Hi," the detector is initial condition. After releasing the reset by setting the *RST* to "Lo," a driver starts to flow current I_{BBM} over the BBM meander. This current I_{BBM} keeps flowing during normal operation period to continuously monitor for attacks. When the BBM meander is disconnected by physical attacks, the current I_{BBM} stops immediately, and the voltage level of BBM V_{A} rises up to V_{DD}. Then, the Reset-Set (RS)-latch changes its internal logical state *DET* and warns the system for the advent of potential attacks. In this design, the current I_{BBM} is less than 150 nA thanks to the variable resistance controlled by V_{BIAS} and well isolated structure between Si substrate and BBM. Thus, the power dissipation due to the static current for monitoring is negligible especially for large-scale cryptographic ICs. Though the Cu BBM meander formed on the backside of IC chip has the potential to receive unwanted EM waves, the detector does not malfunction since the endpoint of meander wiring is connected to ground and the voltage level of BBM does not rise above the threshold of the latch. Note that while the power is not supplied, the detector does not work and the disconnection of BBM cannot be detected. However, such attacking scenario does not exist since SCA and LFI must be executed during crypto operation. Thus, even if the BBM is disconnected at power off, the detector can find the disconnection after the power is turned on.

Attackers may try to avoid the detection scheme by bypassing the meander as shown in Fig. 5(a). If the current path on meander BBM is intentionally shortcut to the output using a conductor, the current continues to flow even when the meander is disconnected, which disables the detection of the exposure attacks. To make countermeasures for such bypass attack, a dummy pattern of meander BBM can be inserted,

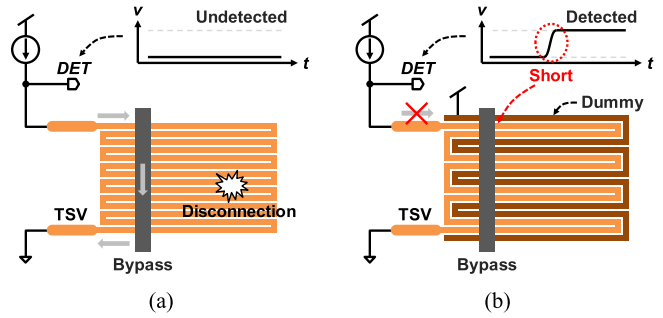

Fig. 5. (a) Bypass attack. (b) Its countermeasure with dummy pattern.

as illustrated in Fig. 5(b). The dummy BBM is supplied to high level with low impedance; thus, the voltage level of meander BBM will be high when the current path and dummy pattern are shorted by the bypass attack. It stops current flow and raises the detection signal *DET* to high. In this way, the detector with dummy BBM pattern can detect the unexpected short of BBM by bypass. Note that it is quite difficult to bypass only one wiring of BBM to avoid contact with dummy, thanks to the fine pitch of BBM meander. As the other attacking scenarios, the detector may be broken at the power off to stuck the detection signal to "Lo," which also disables the detection scheme. The detector can have toggling modes to confirm proper logical operations whenever the chip starts to be powered.

C. Backside SCA Resistance

The ground current caused by the switching operations of cryptographic circuit diffuses into Si substrate through contact taps and forms substrate current. This current produces substrate noise due to the resistive property of substrate. The waveform of this substrate noise is correlated with a secret key of cryptography. Thus, by probing Si-backside and capturing the substrate noise, a secret key can be identified by analyzing the key-dependent noise. This backside SCA enables the attackers to probe anywhere in the chip; thus, they can accurately measure the substrate noise in the closest points to the cryptographic circuit. It indicates that the backside SCA is even effective with the emerging countermeasure techniques for side-channel leakage suppression such as a current equalizing technique [15]. These countermeasures prevent a side-channel leakage on board and make it difficult to acquire the noise on power supply line. However, the backside SCA successfully works to find a correlation between obtained noise and key even under the countermeasure, since it can only use a local substrate noise generated by cryptographic operations. Fig. 6 illustrates the protection circuit using BBM from the serious backside SCA. The substrate noise coupled to the surface of BBM is inherently diminished owing to the resistive isolation of BBM from substrate node of circuits. The series resistor R_S, from the location of cryptographic circuits to the system ground, is considerably larger than the parasitic resistors R_P connecting to the nearby substrate taps. Therefore, the side-channel leakage on BBM V_{BBM} can be attenuated from the substrate noise V_{SUB}, according to the ratio of these

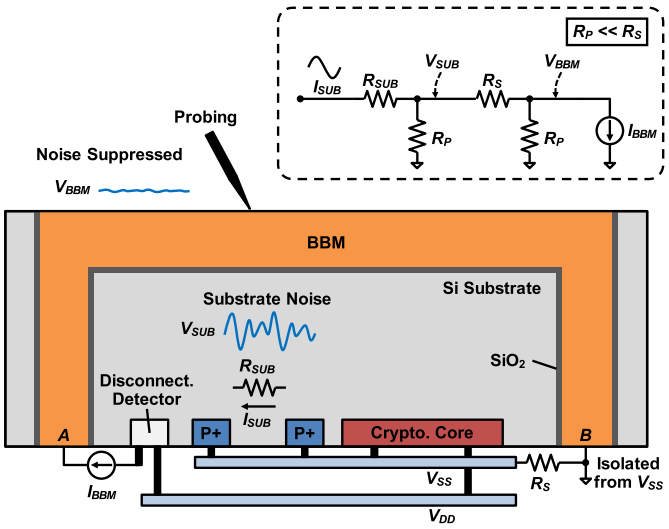

Fig. 6. Side-channel leakage suppression against direct probing attack on Si-backside.

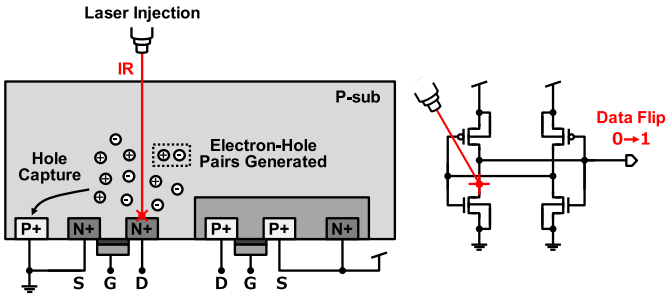

Fig. 7. LFI.

resistances as in the equivalent circuit of Fig. 6. In order to further isolate the BBM node from substrate and further suppress the noise, a resistance component may be provided between the ground and the end of meander. Although the meander pattern exposes silicon space between the BBM, this gap of 10 μm is narrow enough compared with the tip area of standard probe needle with more than 30 μm. Moreover, in future BBM process, much finer pitch of line and space will be possible; thus, it will be more difficult to probe only the silicon area between BBM.

D. Backside LFI Resistance

The laser of 1064 nm (infrared) wavelength passes through the Si substrate. When the IR laser is irradiated to the p-n junction area at the drain node of transistors, electron–hole pairs are generated, as shown in Fig. 7. The holes are collected to contact taps through the substrate, then photocurrent flows from the drain to substrate. If the laser is focused on cross-coupled inverters in flip-flops, the photocurrent potentially flips data held in a data register of a cryptographic cores. This fault-injected code is used for the subsequent analysis, such as differential fault analysis with both correct and faulty code, to estimate the secret key [16]. The LFI attack can be more efficient by irradiating from the Si-backside of IC chip, since the laser directly hits the target without being disturbed by

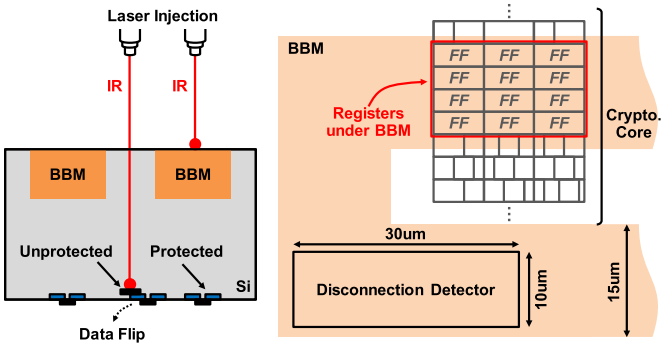

Fig. 8. Protection from LFI by BBM meander.

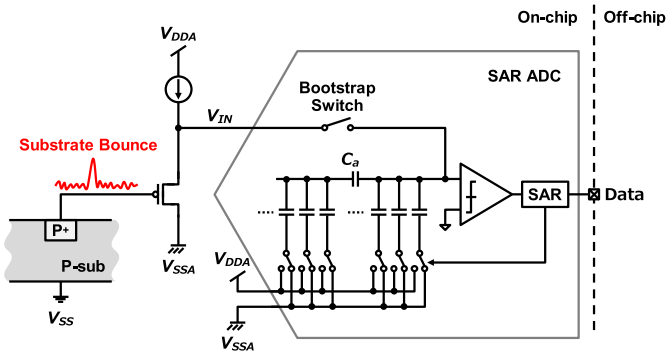

Fig. 9. On-chip substrate noise monitor.

circuit metals. The proposed BBM meander also prevents IR laser injection. This is because the thick Cu metal with more than 10 μm blocks the IR laser penetration. Thus, the target registers of accumulation circuits in the cryptographic core can be protected from LFI attack by hiding them under the Cu BBM, as shown in Fig. 8. Although IR laser can penetrate into the inside of a chip through the gap of BBM inherent to a meander pattern, the BBM linewidth of 15 μm is wide enough to cover the limited number of registers of cryptographic importance. Fig. 8 also shows the protection of the disconnection detector circuit itself from the breaking attacks which stuck the detection signal at "Lo." The detector can also be placed under BBM thanks to its simple configuration and small size of 10 μm $\times$ 30 μm. Thus, it can prevent malicious attack that destroys the detector before BBM breakage. The other possible LFI scenario is an attack targeted the aspect of the IC chip. However, the proposed structure with the substrate thinned to 40 μm and thick 10 μm BBM is also effective against such attack. It limits the path of irradiating the very small target flip-flops inside the large-scale cryptographic circuit from the side of the IC chip.

IV. Circuit Implementation

As a cryptographic circuit for edge devices, an elliptic curve digital signature algorithm (ECDSA) is designed. ECDSA is one of the digital signature techniques with a public key cryptographic algorithm which provides the different level of security from private key ones; however, it requires a large number of arithmetic operations. Thus, a dedicated hardware engine for acceleration of ECDSA is required to reduce power, area, and latency for edge operation. In this design, we implemented an ECDSA accelerator in 130-nm digital CMOS process, and its logic scale is approximately 200 k gate. Moreover, the disconnection detector composed of a few transistors is also embedded in the same single chip. The current path of the detector is connected to the BBM through the TSV under IO pad. The end of the current path on BBM meander is also connected to another TSV which is located to the opposite side of detector to contact with ground via isolation resistor.

Fig. 9 shows the circuit schematic of an on-chip substrate noise monitor to confirm the protection effects by the BBM meander. This monitor circuit acquires the substrate voltage bounce due to the photocurrent by an irradiation of IR laser, which helps us know whether LFI on BBM causes data flip or not. Besides, it can also be used to evaluate the potentiality of side-channel leakage from the chip by using on-chip measured substrate noise. The on-chip substrate noise monitor is composed of an input buffer and an analog-to-digital converter (ADC). A P+ contact tap is placed on Si substrate near the arithmetic registers of ECDSA circuit and its noise during operation is input to the buffer. A simple open-source follower is employed as an input buffer to drive the signal in a wide bandwidth. Though the voltage level of the target substrate is around V_{SS}, p-MOS source follower shifts the dc level up to the input range of subsequent ADC. A successive approximation register (SAR) ADC architecture is employed for a simple and energy-efficient configuration [17]. The resolution of the ADC is 11 bit, which is high enough to obtain the substrate bounce accurately. The ADC operates at 4 MS/s considering the response time of voltage at the laser injection. The capacitive digital-to-analog converter (DAC) inside the SAR ADC is divided into upper and lower DACs by connecting series capacitor C_a to reduce the size of sampling capacitor and expand the bandwidth. The ON-resistance of a sampling switch is also suppressed by using a bootstrap technique [18]. As the result, the bandwidth of the on-chip monitor achieves more than 1 GHz. Though the sampling frequency is much slower than the bandwidth, it can be covered by the equivalent sampling technique with under sampling, since the substrate noise caused by the laser injection or ECDSA operation can be synchronized with the sampling clock of ADC for evaluation.

The BBM circuit is also designed after the frontside CMOS circuit implementation. The specifications of BBM meander pattern such as linewidth, space, thickness, and area are determined according to the following design guidelines to improve security level. First, the space between BBM wirings is required to be as narrow as possible. This prevents the side-channel leakage by disabling the direct probing on only silicon area with probe needle. The width of BBM wiring should be also narrow to be cut by laser irradiation at the back-side exposure attack. However, as described in Section III-D, some registers of the cryptographic circuit must be placed under BBM wiring to protect them from the laser injection. Though the size of the standard cell depends on the technology node, the BBM width must be at least wider than the height

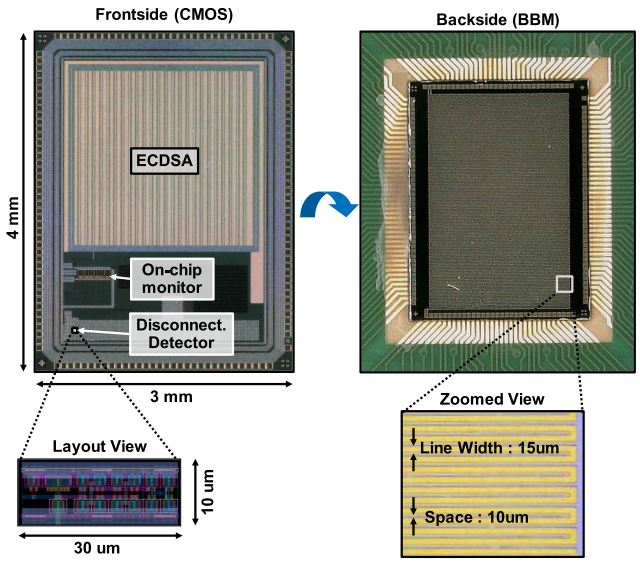

Fig. 10. Photographs of frontside and backside of prototype chip.

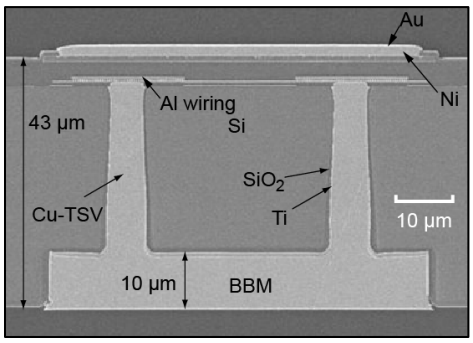

Fig. 11. SEM image of cross-sectional view of prototype chip.

of flip-flop cells. The depth of BBM is required to be thick enough to block the laser. The thicker BBM is also effective against LFI from the side of IC chip. Finally, the BBM meander is drawn with covering the entire chip to keep the attack points away from the target core.

V. Experimental Results

A Si test vehicle was developed with a 130-nm CMOS technology. Fig. 10 shows a die micrograph of both frontside and backside of the prototype chip. The chip size is 4 mm × 3 mm and the embedded cryptographic accelerator of ECDSA occupies 2 mm × 2 mm area and consumes 21.6 mA at the operation clock of 33 MHz. The on-chip substrate noise monitor and the disconnection detector with only 300 μm^2 as shown in the layout image of Fig. 10 are also implemented in a single chip. The wafer completed by the Si fab was then processed with the via-last, Cu BBM technology. The BBM forms meander pattern with the line and space of 15 and 10 μm, respectively, as shown in the zoomed-in view of the right picture in Fig. 10. In future process, the pitch of BBM will be much fine, which disables physical attacks even with an advanced equipment such as FIB. Fig. 11 shows the SEM image of the cross-sectional view around pad area of the prototype chip. It shows that the BBM meander and the TSVs to frontend circuits are seamlessly formed. The

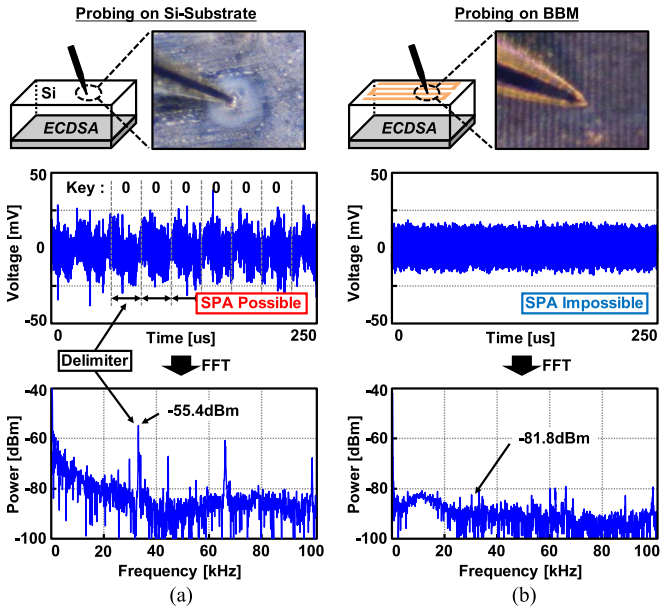

Fig. 12. Backside SCA on ECDSA chip (a) w/o BBM and (b) w/BBM.

thickness of the BBM meander is 10 μm, and the radius and height of TSVs are 5 and 43 μm, respectively. The prototype chip was mounted on a printed circuit board with flip-chip implementation.

First, the backside SCA on the prototype chip was experimented. The substrate noise during the operation of ECDSA at 33 MHz is directly acquired by probing on the Si-backside with a probing station and oscilloscope. To guess the key of ECDSA, a simple power analysis (SPA) is employed. This simply finds the correlation between the noise waveform and key information. Fig. 12 shows the results of the backside SCA on the silicon substrate and the BBM. When the Si substrate is directly probed without BBM, the key-dependent waveform is clearly shown in Fig. 12(a). It visibly discloses the number of clock cycles required for internal operation of scalar multiplications in the waveform, which enables key estimation. To evaluate how much side-channel information is leaked, we introduced the leakage power in the frequency of "delimiter" that indicates the processing time of scalar multiplications. In this experiment, the key of ECDSA is set to all 0 to make it easy to see the delimiter frequency with a single tone. The direct probing on the Si-substrate induces a peak power of −55.4 dBm at the 32-kHz delimiter frequency in fast Fourier transform (FFT) spectrum, which suggests the key estimation with SPA is very possible. On the other hand, when the direct probing is executed to the chip with BBM structure, the delimiter disappears in the waveforms and its power is sufficiently reduced to −81.8 dBm, as shown in Fig. 12(b). This is because the BBM meander is isolated from the Si substrate and the noise is not propagated, which makes SPA very impossible. The comparison of the delimiter power among Si-backside structures is given in Fig. 13. The delimiter leakage of −55.4 dBm is measured at the probing on Si-backside of ECDSA chip with the thickness of 40 μm. Although the thicker substrate of 350 μm attenuates −3.4 dB of the delimiter power, it still causes the key leakage.

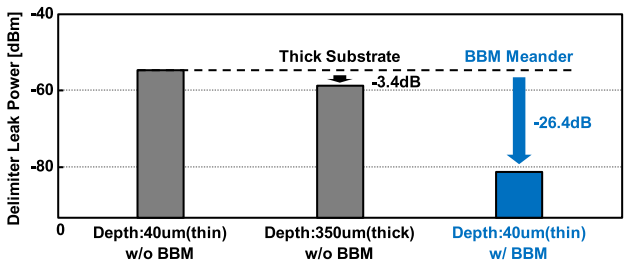

Fig. 13. Comparison of delimiter leak power among Si-backside structures.

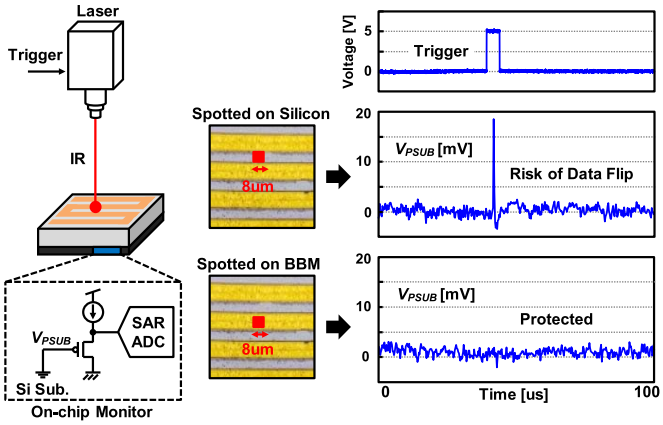

Fig. 14. Measured Si-substrate voltage bounces at IR laser irradiation on silicon and BBM.

However, the proposed BBM structure drastically reduces the delimiter leakage by −26.4 dB even while keeping the substrate thickness as thin as 40 μm. This is beneficial to low height packaging.

Fig. 14 shows the measured Si substrate voltage fluctuation at the laser irradiation. IR laser with the aperture size of 8 μm is irradiated on the silicon gap and on BBM. The Si substrate noise near the focused points is acquired and digitized by the wide-band on-chip monitor circuit embedded in the prototype chip. When the silicon between the BBM stripes is focused, the Si substrate voltage bounces due to electron–hole pair induction, which introduces the risk of data flip. On the other hand, when the laser is spotted on the BBM, the substrate voltage is not bounced at all because the laser is completely blocked by the thick Cu BBM. This experiment indicates that the core part of cryptographic accelerator can be effectively protected from laser irradiation by placing them under the BBM since the size of logic cells is much smaller than the widths of BBM stripe.

The protection against a laser cutting attack is testified as shown in Fig. 15. Once the Cu BBM meander is disconnected by the focused laser of 532 nm (green) wavelength, the detector immediately asserts the warning of physical attacks. This unification of the disconnection detector in a Si IC chip eliminates the need of additional protective structures in subsequent packaging and assembly stages. Note that "cut then restored" attack is invalid since the probing or LFI must be executed during circuit operation, thus the detector works at the moment when the BBM is disconnected.

Table I shows the comparison with the state-of-the-art countermeasures against backside physical attacks. The proposed

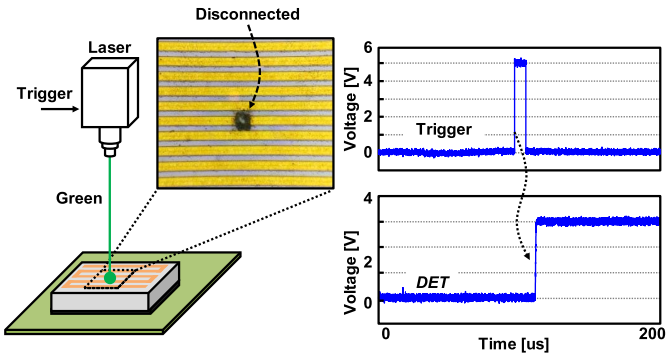

Fig. 15. Evaluation of laser disconnection attack on BBM.

TABLE I
COMPARISON WITH THE OTHER PROTECTION TECHNIQUES AGAINST BACKSIDE PHYSICAL ATTACKS

		[8]	[9]	This work
Structure		Top-metal shield + Back to back bond.	Breakable die + Film laminating	Backside Buried Metal (BBM)
Backside protection against	Probing	YES	YES	YES
	LFI	YES	YES	YES
	Disconnect (Cut, Polish)	YES	YES	YES
	Bypass	No	YES	YES
Overhead		+10% Si area Top metal occupied Two dies needed	+120μm thickness (Film layer)	+0.0025% Si area (Detector)

BBM meander can protect the cryptographic circuit from various backside physical attacks. Since the BBM and TSVs are formed in the existing backside Si-substrate and under IO pads, respectively, our technique only requires the additional area of the disconnection detector circuit with extremely small size of 300 μm^2, which is only 0.0025% of total chip area on the frontside. Compared with other works which require additional frontside physical layers, the proposed structure achieves less overhead while keeping backside physical attack resistances.

VI. CONCLUSION

The BBM Cu meander was monolithically unified with CMOS detector circuits to defend the cryptographic circuit against physical security attacks from vulnerable backside Si substrate. With this BBM circuit technique, the backside SCA does not disclose the key information of cryptography since the internal substrate noise is filtered out by the BBM and is not acquired by probing. Moreover, the backside LFI does not cause data flip due to the thick metal shield which the laser cannot penetrate. The proposed disconnection detector circuit finds the malicious attempts to expose the backside of IC chip by detecting the stop of current flow on BBM meander. The prototype chip fabricated in 130 nm successfully demonstrated the prevention of the physical security attacks including SCA and LFI, and also the detection of shield breakage, with little area overhead. The scheme is generally applicable to secure devices in diversified frontside technology nodes.

REFERENCES

[1] I. Verbauwhede, J. Balasch, S. S. Roy, and A. Van Herrewege, "24.1 circuit challenges from cryptography," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 428–429.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1666. Berlin, Germany: Springer, Aug. 1999, pp. 388–397.

[3] K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, "Information-theoretic approach to optimal differential fault analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 109–120, Feb. 2012.

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

[5] S. Manich, M. S. Wamser, and G. Sigl, "Detection of probing attempts in secure ICs," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust*, Jun. 2012, pp. 134–139.

[6] 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. 27–32.

[7] 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.

[8] J.-M. Cioranesco *et al.*, "Cryptographically secure shields," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 25–31.

[9] 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.

[10] T. Miki *et al.*, "A Si-backside protection circuits against physical security attacks on flip-chip devices," in *Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC)*, Nov. 2019, pp. 25–28.

[11] J. G. J. van Woudenberg, M. F. Witteman, and F. Menarini, "Practical optical fault injection on secure microcontrollers," in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr.*, Sep. 2011, pp. 91–99.

[12] W. Xiong, M. Jiang, M. Zhu, B. Zhu, and J. Lu, "Analysis of electromagnetic shielding of IC package with thin absorbing material coating inside in two different configurations," in *Proc. IEEE Int. Symp. Electromagn. Compat. IEEE Asia–Pacific Symp. Electromagn. Compat. (EMC/APEMC)*, May 2018, pp. 1216–1221.

[13] 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.

[14] 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.

[15] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2009, pp. 64–65.

[16] K. Matsuda *et al.*, "A 286F2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2018, pp. 352–353.

[17] B. P. Ginsburg and A. P. Chandrakasan, "500-MS/s 5-bit ADC in 65-nm CMOS with split capacitor array DAC," *IEEE J. Solid-State Circuits*, vol. 42, no. 4, pp. 739–747, Apr. 2007.

[18] A. M. Abo and P. R. Gray, "A 1.5-V, 10-bit, 14.3-MS/s CMOS pipeline analog-to-digital converter," *IEEE J. Solid-State Circuits*, vol. 34, no. 5, pp. 599–606, May 1999.

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.

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. He was an Associate Professor with Kobe University, Kobe, Japan, from 2002 to 2009, where he promoted to Full Professor in 2009 and is currently a Professor with the Graduate School of Science, Technology and Innovation. 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; 3-D system integration; and 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 from 2002 to 2009, the Custom Integrated Circuits Conference from 2007 to 2009, the Asian Solid-State Circuits Conference from 2005 to 2009, the International Solid-State Circuits Conference since 2014, the European Solid-State Circuits Conference since 2020, and many others. He has been the Chair of the Technology Directions Subcommittee for the International Solid-State Circuits Conference since 2018. He was a Technical Program Chair from 2010 to 2011, a Symposium Chair from 2012 to 2013, and an Executive Committee Member from 2010 to 2014 for the Symposium on VLSI Circuits. He was the Past Chair for the IEEE Solid-State Circuits Society (SSCS) Kansai Chapter from 2017 to 2018 and is currently an AdCom Member and a Distinguished Lecturer (DL) of the IEEE SSCS. He has been an Associate Editor of the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS since 2015.

Hiroki Sonoda (Member, IEEE) received the B.S. degree in engineering and the M.S. degree in science, technology, and innovation from Kobe University, Kobe, Japan, in 2018 and 2020, respectively, where he is currently pursuing the Ph.D. degree.

His research interest includes low-impedance packaging techniques 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, in 2003, 2005, and 2007, respectively.

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

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

Takaaki Okidono received the B.S. degree from Osaka Electro-Communication University, Neyagawa, Japan, in 1982.

He joined Semiconductor Business Unit, Miyoshi Electronics Corporation, Hiroshima, Japan, in 1982. He was also with the Semiconductor Packaging Development Group, Mitsubishi Electric Corporation, Hyogo, Japan. In 1988, he transferred to Wave Technology Inc., Hyogo, Japan, where he was involved in the design and development of semiconductor packages. Since 2017, he has been with ECSEC, Tokyo, Japan, focusing on advanced packaging technology.

Yuuki Araga (Member, IEEE) received the B.E., M.E., and Ph.D. degrees from the Department of Computer and System Engineering, Kobe University, Kobe, Japan, in 2008, 2010, and 2014, respectively.

He is currently a Researcher with the National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Japan. His present research focus is measurement and modeling techniques for 3-D integrated circuits.

Naoya Watanabe (Member, IEEE) received the M.S. and Ph.D. degrees in computer science and electronics from the Kyushu Institute of Technology, Fukuoka, Japan, in 2001 and 2004, respectively.

From 2004 to 2006, he was a Research Associate with the Kyushu Institute of Technology. From 2006 to 2008, he worked as a Researcher with Kumamoto Technology and Industry Foundation, Japan. In 2008, he joined Fukuoka Industry & Technology Foundation, Kumamoto, Japan, as a Researcher. In 2011, he joined the National Institute of Advanced Industrial Science and Technology, Tsukuba, Japan. He has been engaged in the study of 3-D stacking technology, 3-D stacked systems, and 3-D IC testing.

Dr. Watanabe is a member of the IEEE Components, Packaging, and Manufacturing Technology Society, the Japan Institute of Electronics Packaging (JIEP), the Japan Society of Applied Physics (JSAP), and the International Microelectronics Assembly & Packaging Society (IMAPS). He received the Best Paper Award from the IEEE CPMT Symposium Japan (ICSJ) in 2013.

Haruo Shimamoto received the B.S. and M.S. degrees from Osaka University, Suita, Japan, in 1978 and 1980, respectively.

He joined Semiconductor Business Unit, Miyoshi Electronics Corporation, Hiroshima, Japan. The former business unit was merged to Renesas in 2003 with Hitachi and in 2010 with NEC. He had been engaged about 28 years in the development of semiconductor packaging and mass production. In 2013, he joined the National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Japan, and is studying 3-D packaging technology. He is currently an Invited Researcher with the 3-D Integration System Group, Device Technology Research Institute, AIST.

Mr. Shimamoto is a member of the Japan Institute of Electronics Packaging (JIEP).

Katsuya Kikuchi (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Saitama University, Saitama, Japan, in 1996, 1998, and 2001, respectively.

He joined the National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Japan, in 2001, where he has been engaged in the research on 3-D integration system technologies. He is currently a Group Leader with the 3D Integration System Group, Device Technology Research Institute, AIST. His current research interests include the design and fabrication techniques toward 3-D integration systems with particular emphasis on power/signal integrity, testing, and diagnosis.

Dr. Kikuchi is a member of the Japan Institute of Electronics Packaging (JIEP), the Institute of Electronics Information and Communication Engineers (IEICE), the Japan Society of Applied Physics (JSAP), and the American Physical Society (APS).