IEICE TRANSACTIONS

on Electronics

DOI:10.1587/transele.2022CDI0001

Publicized:2023/04/19

A PUBLICATION OF THE ELECTRONICS SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER Special Section on Solid-State Circuit Design − Architecture, Circuit, Device and Design Methodology

Design of Circuits and Packaging Systems for Security Chips (Invited)

Makoto Nagata, ***Senior Member***

SUMMARY Hardware oriented security and trust of semiconductor integrated circuit (IC) chips have been highly demanded. This paper outlines the requirements and recent developments in circuits and packaging systems of IC chips for security applications, with the particular emphasis on protections against physical implementation attacks. Power side channels are of undesired presence to crypto circuits once a crypto algorithm is implemented in Silicon, over power delivery networks (PDNs) on the frontside of a chip or even through the backside of a Si substrate, in the form of power voltage variation and electromagnetic wave emanation. Preventive measures have been exploited with circuit design and packaging technologies, and partly demonstrated with Si test vehicles.

key words: Hardware security, Secure packaging, Cryptography, Implementation attacks, Side channel leakage, CMOS integrated circuits.

1. Introduction

Internet-of-things (IoT) applications have proliferated everywhere on the globe. The nodes on the edge interact with surrounding environment through sensing and/or actuating frontends and then communicate digital data with cloud servers on the backend over backhauls. Every logical entity in this chain needs to maintain security and privacy, as depicted in Fig. 1, where semiconductor integrated circuit (IC) chips play crucial roles. Security chips are spread among IoT devices and featured by cryptography. The design, implementation and evaluation of IoT security were discussed in [1] with the variety of performance requirements on crypto functionality from the low-end lightweight to the high-end high throughput in response to respective definitions of systems and applications.

A crypto hardware core implements its associated cryptographic algorithm in digital ICs, which is called a crypto processor or abbreviated to a crypto core. A secret-key algorithm uses a common single key for both encryption of a given plain text and decryption of the cipher. A secret key is confidentially shared among the users through a secure communication channel. Advanced encryption standard (AES) is the most widely adopted [2][3][4]. On the other hand, a public-key algorithm uses a pair of keys, one is publicly opened and used for encrypting a plain text, while the other is privately kept and applied for decrypting the cipher. The pubic key is accessible to anyone, while only the person who creates the key pair and holds its secret key can extract information. Rivest–Shamir–Adleman (RSA) algorithm and elliptic curve cryptography (ECC) [5][6] are often used in this category. The use cases are versatile among secret-key and public-key crypto algorithms, and an IC chip for IoT security typically embed different crypto cores [7][8].

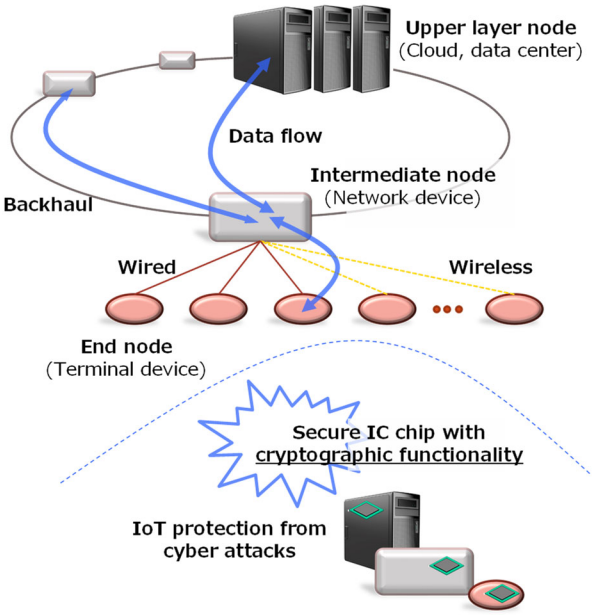

Fig. 1 IC chips for IoT security.

Modern crypto cores are mathematically proven for security by crypto analysts or tested for computational hardness of inverse processing. It is almost impossible to extract secret information from the collection of ciphers. However, there is another class of attacks exploring physical measures.

An edge device is physically placed nearby general users, in contrast to cloud servers that are remotely hold in a security-managed facility such as a data center. The IC chips in an edge device are therefore accessible by an adversary, and even worse, potentially decapsulated from package structures without a permanent damage, by chemically removing laminates or mechanically shaving or drilling resin moldings. This facilitates an adversary to locate an antenna or an electric needle and to probe crypto cores on an IC chip.

A side-channel (SC) leakage is generally known for the existing vulnerability of crypto cores against the attempts to steal secret information. The attempts are attributed to physical implementation of crypto cores even though their

The author is with the Graduate School of Science, Technology and Innovation, Kobe University, 1-1 Rokkodai, Nada, Kobe 657-8501, Japan.
Email: nagata@cs.kobe-u.ac.jp

crypto algorithms are theoretically proven for security, and then called implementation attacks [9][10][11]. The measurements of electromagnetic (EM) waves radiated from an IC chip during the operation of a crypto core, or the responses of a crypto core against high-power EM disturbances intentionally irradiated on to an IC chip [12][13][14], are the SC properties for an attacker to explore. These are categorized in passive and active SC attacks, respectively, and often combined with the IC-chip decapsulation techniques for the better resolution of experiments.

A variety of research efforts have been made on preventive measures against SC leakage, and importantly, we see it that the combination of their outcomes, vertically from systems to circuits, packaging structures and devices, will contribute to mitigate vulnerabilities more effectively than the adoption of a single solution. In this paper, we focus on the packaging solutions for security of crypto cores, which co-work with circuits and systems.

The remaining parts are configured as follows. Section II describes the attack opportunities utilizing SC leakages of an IC chip. Section III discusses the countermeasures to SC leakages from secure packaging viewpoints. Section IV provides conclusions and future works.

2. Attack surfaces – power and EM SC leakages

A secure IC chip with crypto processors is targeted by implementation attacks, as sketched in Fig. 2, once it is physically assembled in a package and operates on a printed circuit board (PCB). The SC leakages are searched by adversarial attempts about EM waves radiated from the chip or using infrared (IR) lasers irradiated on the chip. The architecture of a secure IC chip intends to horizontally protect crypto processors from attacks. Secure data interface (I/F) restricts digital data in a secure zone only for the information to be secured by crypto processors. Power converters in a power management control (PMC) unit regulates power current and attenuates power SC leakages. On-chip clocking by phase-locked loop (PLL) circuits eliminates undesired timing glitches and prevents from timing SC attacks. Crypto cores are also equipped by anti-tampering functionality or even provided with attack detection capabilities at the logic as well as at the circuit levels [15][16][17]. An IC chip can mitigate the threats of SC leakage, however, remains accessible to vertical attempts using EM and IR medias.

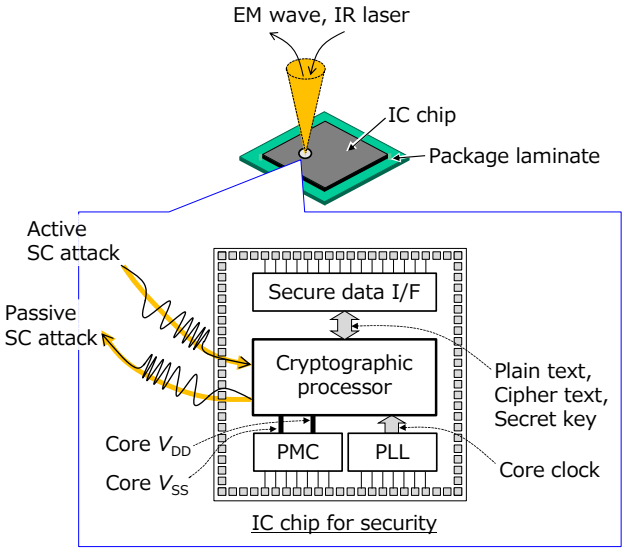

Fig. 2 Horizontal protection of IC chip and vertical vulnerability against SC leakages.

An IC chip with crypto cores is assembled on a PCB, using faced-up or flipped-chip packaging technologies (Fig. 3). A crypto core is directly accessed by vertical means on the frontside (circuit side) in a faced-up structure. The power and signal pads on the frontside IC chip are wire-bonded to the associated electrical lands on a package substrate. This structure has been traditionally chosen, matured, and popularly adopted in IC chip markets because of its lowest cost assembly. On the other hand, the core on a flipped chip is protected by package laminates from adversarial accesses from the frontside. This flipped-chip assembly becomes widely adopted in accordance with the demands of a lower profile and a smaller footprint of an electronic system, along with the emerging chip-sized packaging with use of membrane interposers [18][19][20].

Here, an IC chip in any packaging structure is vulnerable against SC attacks from the backside of its Si substrate (Si body of an IC chip), named Si-backside SC attacks, as exemplified in Fig. 4. The package and PCB laminates can be mechanically drilled to produce a hole for access to the Si-backside of an IC chip even in face-up packaging. On the

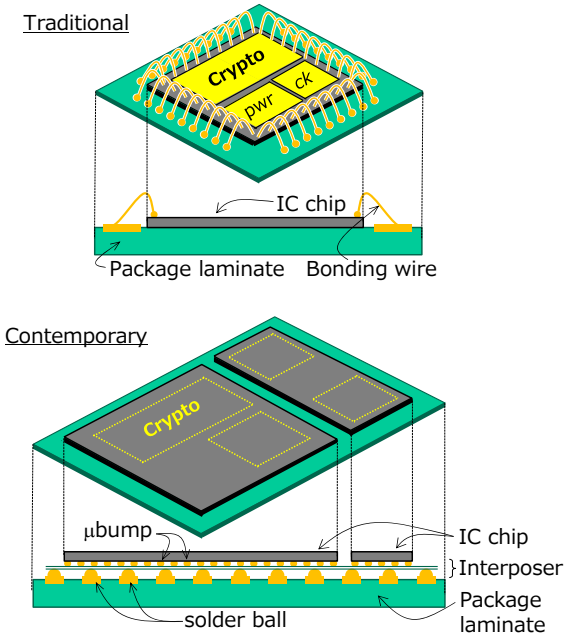

Fig. 3 Face-up and flip chip assembly.

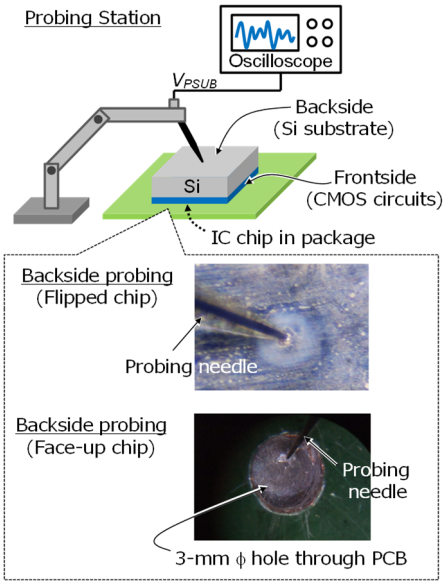

Fig. 4 Si-backside SC attack.

other hand, the whole Si-backside surface is open for an adversarial access in the case of flipped-chip packaging. It is of importance to address that the Si-backside is essentially inevitable as an attack surface for any secure IC chip, being accessible to either a voltage probe or an EM antenna.

Why SC leakages are observable from the Si backside – its answer is explained with a general sketch of a power delivery network (PDN) system shown in Fig. 5 [21]. An external power source supplies an IC chip, where power lines are in series connected through PCBs, packages, and IC chips. When digital switching takes place among logic cells of a crypto core, transient currents flow through power lines. This is in part decoupled among on-chip and off-chip parts of PDN by using power converters in a PMC unit, however, that is typically limited to the high voltage (V_{DD}) side. Every part in the ground (V_{SS}) side is straightforwardly connected, and importantly, with the Si substrate of an IC chip to stably bias the body voltage, in a typical semiconductor technology using p-type Si substrate as the base body. The dynamic power current, as the sum of transient currents from active logic cells, flows through power line parasitic impedances and induces the voltage variation over V_{DD} and V_{SS} domains. This can be observable on the Si substrate with direct voltage probing, or, through the EM wave radiation that is transparent to an antenna located on the Si-substrate backside [22].

Additionally, an on-chip voltage monitor (OCM) is equipped in an IC chip and measures voltage variations at the positions of interest over PDNs [23]. This helps to verify the design of crypto circuits for lower SCs and to provide the opportunity of detecting physical attack attempts [24].

Once the voltage or EM waves are captured, the measured data are subsequently analyzed for side-channel (SC)

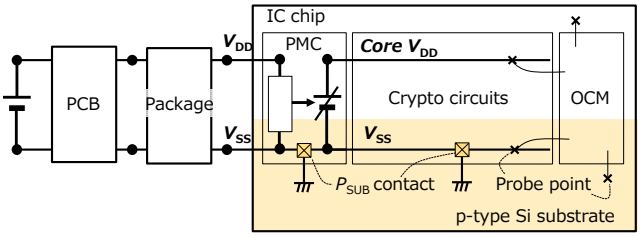

Fig. 5 Power delivery and Si substrate networks [21]. (Copyright 2022 IEEE)

leakage of secret information. The signal strength for measurements improves with the proper location of observation points on the backside once a die is decapsulated. This also facilitates to focus the intentional injection of intensive disturbance by EM or IR medias onto the area of vulnerability.

The voltage waveforms measured during the operation of crypto cores are shown in Figs. 6 and 7, for secret-key and public-key ciphers, respectively. The voltage waveforms are collected in the last round of AES operation for encrypting various plain texts, shown in Fig. 6, has the distribution of voltage drops that are very relevant to the number of bit flips happening in the data register, which is called Hamming distance. This inherent correlation of voltage drops or EM amplitudes to internal logic operations is the source of SC leakage for the design of AES in a round-based byte wise architecture. One metric of SC leakage tolerance is the number of measurement traces to presume the correct set of secret key bytes through the correlation analysis.

On the other hand, the time-domain voltage waveforms given in Fig. 7 includes “power signatures” in the internal arithmetic operations of ECDSA for a doubling, namely, two-time multiplication of the same data, or for a summation of two different data. The branch selection of arithmetic operations comes internally from key bits used in encryption (or decryption). This pattern-based analysis is effective for the class of public-key crypto algorithms. The number of clock cycles to complete these relevant arithmetic operations are typically of the order of a few thousands or even larger, and the associated frequency component is as low as 10 kHz when the core operates at 100 MHz in clock frequency. The example waveform in Fig. 7 exhibits 25 kHz frequency components, which is low enough to leak through a typical power converter, e.g., a low dropout voltage regulator (LDO) or a switching regulator (DC-DC converter). The size of discrepancy among the signatures, often represented in the magnitude of respective frequency components measured in dBm, can be the metric of resiliency against SC leakage.

These example waveforms were collected for the crypto cores without any countermeasure at the algorithm or at the circuit levels. The security metrics can be improved with sophisticated crypto architectures and algorithms. However,

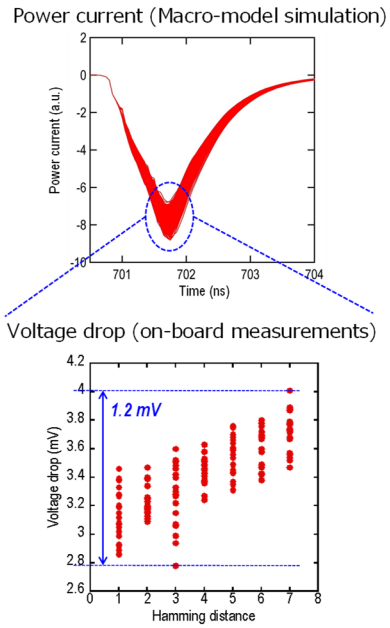

Fig. 6 Secret key crypto: power correlation attack.

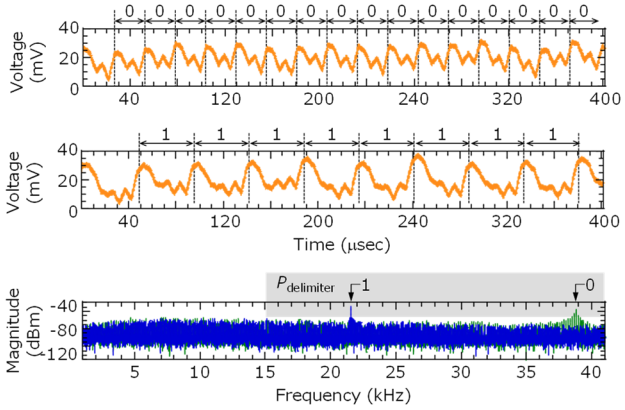

Fig. 7 Public key crypto: EM signature attack [21]. (Copyright 2022 IEEE)

the vertical access won't become negligible specially from the viewpoint of Si backside SC leakage, under adversarial attempts with the finer size of spotting by needles or antennas. The vertical protection is therefore needed.

3. Attack protections – secure packaging

Packaging and assembly technologies have evolved along with the development of semiconductor devices and integrated circuits. Security has also been always concerned. Multiple electronic cards were plastic molded in a single box and fully wrapped by an insulated nichrome wire, formed like a cocoon [25]. The internal card continuously measures the wire resistance and detects intrusions with cutting or shorting the cocoon. This technique was intended to protect a computing system from an unauthorized access, that was recognized as emerging th reats in compliance with computer downsizing toward a personal use, in the mid 80's. One can realize a historical analogy here in modern IoT devices. Multiple IC chips or chiplets are assembled on an interposer for packaging and to be protected from SC attacks or even physically intrusion attacks. A variety of engineering approaches have been proposed in packaging techniques for security [26][27][28].

The authors have developed the backside buried metal (BBM) technology outlined in Fig. 8 [29][30]. An IC chip has metal stripes monolithically buried on its Si substrate backside. Adversarial attempts on the Si backside are prevented by BBM structures, with shielding EM radiation or irradiation, blocking IR lasers to pe netrate, and tolerating physical intrusions such as cutting. Additionally, CMOS circuits on the frontside are electrically connected to BBM stripes with through Si vias (TSVs) and unified in electric systems such as intrusion detection as well as power delivery. The advantages of BBM structures over conventional membranes coated or sputtered on the backside are primarily found in the flexibility for structural exploration in vertical assembly and in the structural parameters such as the substrate thickness as thin as 50 μm or smaller and the metal thickness as thick as 10 μm or larger.

The post wafer BBM forming technology was evolved from the via-last manufacturing techniques, as shown in Fig. 9, in close collaboration with National Institute of Advanced Industrial Science and Technology (AIST). The prototype manufacturing was started from 0.13 μm CMOS 8-inch complete wafers carrying IC chips with security functionality. The wafers were thinned to 40 μm in thickness, and selectively dug for TSVs with 10 μm in diameter. The stripes with the pattern widths of 15 μm were processed in

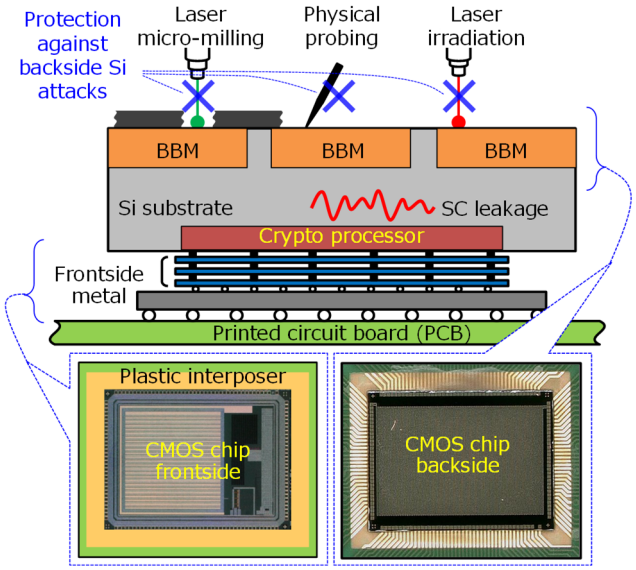

Fig. 8 Securing Si-substrate backside.

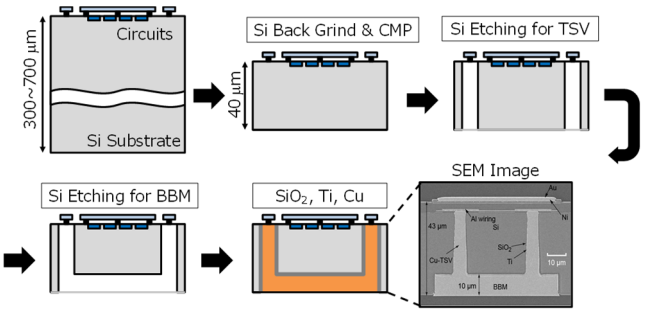

Fig. 9 Backside buried metal (BBM) technology [30]. (Copyright 2020 IEEE)

the depth of 10 µm. The TSVs and BBMs were coated by SiO_2 and Ti, and then filled with Cu. Further process details are given in [29].

The prototype IC chip was tested for the Si-backside SC leakage of ECDSA, similarly as in Fig. 7. The comparison between the prototype IC chip with the normal backside and that with BBM stripes is given in Fig. 10. The power signatures in the arithmetic operation with the successive key bits of "0" exhibit regular separations in a time-domain EM waveform and therefore induces a clear peak at the frequency of delimiters, in the normal CMOS IC chip with an open Si backside. In contrast, the delimiters become almost negligible for the prototype with BBM stripes, showing the attenuation factor of more than 24 dB that is equivalently less than 1/16 in power, measured in the frequency domain.

A conceptual sketch of the three-dimensional (3D) chip stacking with the BBM technology is given in Fig. 11. Each tier is inclusive of TSVs for tier-to-tier electrical as well as thermal connections, and accompanied by BBM stripes. CMOS circuits on the frontside utilize both the BBM stripes on its backside through TSVs and those on the immediate backside of an adjacent tier via area µbumps. The backside of the topmost tier will be used for shielding to protect a secure 3D stack against implementation attacks.

Power wirings are backed by BBM stripes throughout the PDN of a secure 3D stack. This takes the advantages of thick and wide Cu stripes when those are biased at the core V_{DD} and buried in the Si substrate at the system V_{SS}, as depicted in the equivalent circuit diagram of Fig. 12. Each crypto core in the tier is assumed to be locally supplied by a compact (micro) power regulator, µVRM.

By virtue of BBM stripes, the parasitic impedance in series to power wirings is reduced. In addition, the shunting capacitors, C_{BBM}, are formed between V_{DD} and V_{SS} and distributed over the whole PDN. The presence of these capacitors locally in each tier helps the operation of µVRM and well regulates the voltage of V_{DD} during active operation of crypto cores, in addition to, and more effectively than, the capacitors on a package, C_{PKG}.

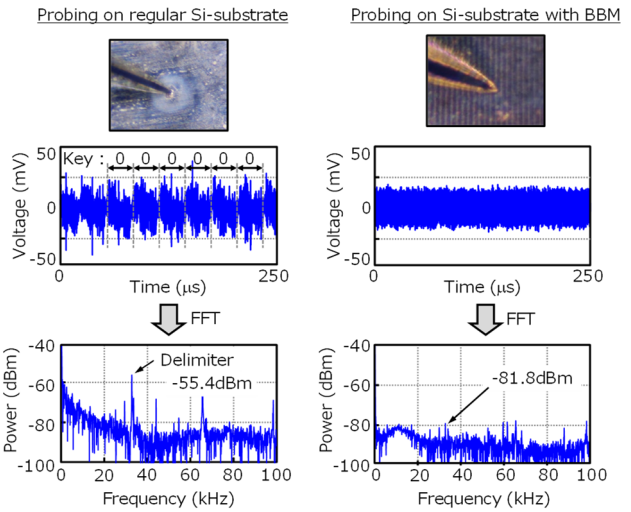

Fig. 10 Si substrate backside protection [30]. (Copyright 2020 IEEE)

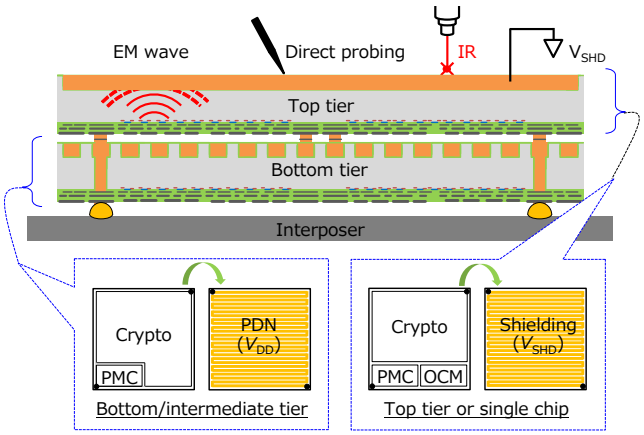

Fig. 11 Secure 3D IC chip stack using BBM [21].

A photo of prototype 4-tier 3D stacking is also given in Fig. 12. The TSVs (40 µm in depth) and BBM stripes (10 µm in thickness) are regularly placed on the Si substrate of every tier (Fig. 12 bottom left). Also, the part of wirings are vertically connected with an array of µbumps in the periphery of the die (Fig. 12 bottom right). This demonstrator exhibited 60% reduction of power noise over V_{DD} nodes, when on-chip measured by OCM, as explained in Fig. 5. In addition, the collection of EM waves on PCB was suggested the mitigation of power SC leakage [31].

4. Conclusions

An IC chip for security applications needs to be designed for resiliency against implementation attacks, typically through physically invasive, passive and active leakage SC explorations. This paper summarized the potentiality of on-chip protections against implementation attacks, with horizontal chip architectures and vertical packaging

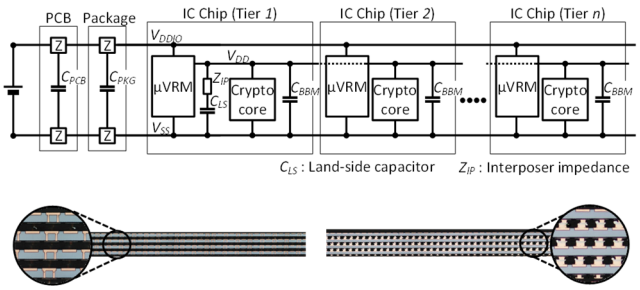

Fig. 12 3D CMOS PDN with BBM [21].

structures. The technological category of secure packaging was discussed for crypto-based secure systems and also extended for 3D integration. Cross-layer exploration of countermeasures is of obvious importance, that includes on-chip detection of attacks and proactive reactions to prevent from malicious attempts, which are left for future works in the research community of hardware security.

Acknowledgments

This work was in part supported by the Cabinet Office (CAO), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Cyber Physical Security for IoT Society”, JPNP18015 (funding agency: NEDO).

References

[1] T. Matsumoto, M. Ikeda, M. Nagata, Y. Uemura, "Secure Cryptographic Unit as Root-of-Trust for IoT Era," IEICE Trans. Electron. vol. E104-C, no. 7, pp. 262-271, Jul. 2021.

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

[3] S. K. Mathew, F. Sheikh, M. Kounavis, S. Gueron, A. Agarwal, S. K. Hsu, H. Kaul, M. A. Anders, and R. K. Krishnamurthy, “53 Gbps Native GF(2^4)^2 Composite-Field AES-Encrypt/Decrypt Accelerator for Content-Protection in 45 nm High-Performance Microprocessors,” IEEE Journal of Solid-State Circuits, vol. 46, no. 4, pp. 767-776, Apr. 2011.

[4] R. Ueno, S. Morioka, N. Miura, K. Matsuda, M. Nagata, S. Bhasin, Y. Mathieu, T. Graba, J-L. Danger, N. Homma, “High Throughput/Gate AES Hardware Architectures Based on Datapath Compression,” IEEE Transactions on Computers, vol. 69, no. 4, pp. 534-548, Apr. 2020.

[5] M. Tamura and M. Ikeda, “1.68µJ/signature-generation 256-bit ECDSA over GF(p) signature generator for IoT devices,” Proc. 2016 IEEE Asian Solid-State Circuits Conference, pp. 341-344, Nov. 2016.

[6] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, Y, Begriche, "A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT)," IEEE Systems Journal, vol. 14, no. 3, 3440-3450, Sep. 2020.

[7] “Secure Integrated Circuits and Systems,” I. Verbauwhede, Ed., Springer, 2010 (ISBN 978-0-387-71829-3).

[8] Frontiers in Hardware Security and Trust; Theory, Design and Practice,” C. H. Chang and Y. Cao, Eds, IET, 2020. (ISBN 978-1-785-61927-4)

[9] P. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” IACR CRYPTO 1996, Lecture Notes in Computer Science, vol. 1109, pp. 104–113, Aug. 1996.

[10] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” IACR CRYPTO 1999, Lecture Notes in Computer Science, vol. 1666, pp. 388–397, Aug. 1999.

[11] “Power Analysis Attacks – Revealing the Secrets of Smart Cards,” S. Mangard, E. Oswald, and T. Popp, Springer, 2007 (ISBN 978-0-387-38162-6).

[12] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," IACR CRYPTO, Lecture Notes in Computer Science, vol. 1294, pp. 513-525, Aug. 1997.

[13] A. Moradi, O. Mischke, C. Paar, Y. Li, K. Ohta, and K. Sakiyama, “On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attacks in a Combined Setting,” IACR CHES, Lecture Notes in Computer Science, vol. 6917, pp. 292-311, Sep. 2011.

[14] D. Karaklajić, J-M. Schmidt, and I. Verbauwhede, “Hardware Designer's Guide to Fault Attacks,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 21, no. 12, pp. 2295-2306, Dec. 2013.

[15] I. Verbauwhede, J. Balasch, S. S. Roy, and A. Van Herrewege, “Circuit Challenges from Cryptography,” IEEE ISSCC Dig. Tech. Papers, pp. 428-429, Feb. 2015.

[16] N. Homma, Y. Hayashi, T. Aoki, N. Miura, D. Fujimoto, and M. Nagata, “Design Methodology and Validity Verification for a Reactive Countermeasure Against EM Attacks,” IACR Journal of Cryptology, pp. 1-19, Online, Dec. 2015.

[17] K. Koiwa, R. Ueno, D. Fujimoto, Y. Hayashi, M. Nagata, M. Ikeda, T. Matsumoto, N. Homma, "Collision-Based EM Analysis on ECDSA Hardware and a Countermeasure," in Proc. the Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility (Joint EMC & APEMC 2019), pp. 793-796, Sapporo, Japan, June 2019.

[18] P. J. Tzeng *et al.*, “Process Integration of 3D Si Interposer with Double-Sided Active Chip Attachments,” in Proc. IEEE Electronic Components & Technology Conference (ECTC 2013), pp. 86-93, May 2013.

[19] “Heterogeneous Integration Roadmap,” Chapter 19: Security, 2019 Edition. http://eps.ieee.org/hir

[20] J. H. Lau, “Recent Advances and Trends in Multiple System and Heterogeneous Integration with TSV-Less Interposers,” IEEE Transactions on Components, Packaging and Manufacturing Technology, vol. 12, no. 8, pp. 1271-1281, Aug. 2022.

[21] M. Nagata, T. Miki, N. Miura, "Physical Attack Protection Techniques for IC Chip Level Hardware Security" IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 1, pp. 5-14, Jan. 2022.

[22] D. Fujimoto, D. Tanaka, N. Miura, and M. Nagata, “Side-Channel Leakage on Silicon Substrate of CMOS Cryptographic Chip,” in Proc. IEEE International Symposium on Hardware- Oriented Security and Trust (HOST 2014), pp. 32-37, May 2014.

[23] M. Nagata, J. Nagai, T. Morie, and A. Iwata, “Measurements and Analyses of Substrate Noise Waveform in Mixed Signal IC Environment,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 19, no. 6, pp. 671-678, 2000.

[24] T. Wadatsumi, T. Miki, M. Nagata, "A dual-mode successive approximation register analog to digital converter to detect malicious off-chip power noise measurement attacks," JSAP Japanese Journal of Applied Physics, vol. 60, no. SB, pp. SBBL03_1-9, Feb. 2021.

[25] S. H. Weingart, "Physical Security for the μABYSS System," IEEE Symposium on Security and Privacy, pp. 52-52, Apr. 1987.
[26] X. T. Ngo, J.-L. Danger, S. Guilley, T. Graba, Y. Mathieu, Z. Najm, S. Bhasin, “Cryptographically Secure Shield for Security IPs Protection,” IEEE Transactions on Computers, vol. 66, no. 2, pp. 354–360, Feb. 2017.
[27] S. Borel, L. Duperrex, E. Deschaseaux, J. Charbonnier, J. Cledière, R. Wacquez, J. Fournier, J.-C. Souriau, G. Simon, A. Merle, “A Novel Structure for Backside Protection Against Physical Attacks on Secure Chips or SiP,” in Proc. IEEE 68th Electronic Components and Technology Conference (ECTC 2018), pp. 515–520, May 2018.
[28] M. S. M. Khan, C. Xi, A. A. Khan, M. T. Rahman, M. M. Tehranipoor and N. Asadizanjani, "Secure Interposer-Based Heterogeneous Integration," in IEEE Design & Test, vol. 39, no. 6, pp. 156-164, Dec. 2022.
[29] Y. Araga, M. Nagata, H. Ikeda, T. Miki, N. Miura, N. Watanabe, H. Shimamoto, K. Kikuchi, “A Thick Cu Layer Buried in Si Interposer Backside for Global Power Routing,” IEEE Transactions on Components, Packaging and Manufacturing Technology, vol. 9, no. 3, pp. 502-510, Mar. 2019.
[30] T. Miki, M. Nagata, H. Sonoda, N. Miura, T. Okidono, Y. Araga, N. Watanabe, H. Shimamoto, K. Kikuchi, “Si-Backside Protection Circuits Against Physical Security Attacks on Flip-Chip Devices,” IEEE Journal of Solid-State Circuits, vol. 55, no. 10, pp. 2747-2755, Oct. 2020.
[31] K. Monta, H. Sonoda, T. Okidono, Y. Araga, N. Watanabe, H. Shimamoto, K. Kikuchi, N. Miura, T. Miki, M. Nagata, “3D CMOS Chip Stacking for Security ICs Featuring Backside Buried Metal Power Delivery Networks with Distributed Capacitance,” IEEE Trans. Electron Devices, vol. 68, no. 4, pp. 2077-2082, Apr. 2021.

Makoto Nagata received the B.S. and M.S. degrees in physics from Gakushuin University, Tokyo, Japan, in 1991 and 1993, respectively, and the Ph.D. degree in electronics engineering from Hiroshima University, Hiroshima, Japan, in 2001.

He was a Research Associate at Hiroshima University from 1994 to 2002, an Associate Professor at Kobe University, Kobe, Japan, from 2002 to 2009, where he was promoted to a Full Professor in 2009. He is currently a Dean and Professor with the Graduate School of Science, Technology and Innovation, Kobe University.

His research interests include design techniques targeting high-performance mixed analog, RF and digital VLSI systems with particular emphasis on power/signal/substrate integrity and electromagnetic compatibility, testing and diagnosis, three-dimensional system integration, as well as their applications for hardware security and safety, and cryogenic electronics for quantum computing.

Dr. Nagata is a Senior Member of IEICE. He has been a member of a variety of technical program committees of international conferences, such as the Symposium on VLSI Circuits (2002–2009), Custom Integrated Circuits Conference (2007–2009), Asian Solid-State Circuits Conference (2005–2009), International Solid-State Circuits Conference (2014-2022), European Solid-State Circuits Conference (since 2020), and many others. He chaired the Technology Directions subcommittee for International Solid-State Circuits Conference (2018-2022) and now serves for an Executive Committee Member. He was the Technical Program Chair (2010–2011), the Symposium Chair (2012–2013), and an Executive Committee Member (2014–2015) for the Symposium on VLSI circuits. He was the IEEE Solid-State Circuits Society (SSCS) Distinguished Lecturer (DL) (2020-2021) and also the IEEE SSCS Kansai Chapter Chair (2017–2018). He is currently an AdCom Member of the IEEE SSCS (since 2020), and an associate editor for IEEE Transactions on VLSI Systems (since 2015).