3-D CMOS Chip Stacking for Security ICs Featuring Backside Buried Metal Power Delivery Networks With Distributed Capacitance

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

***Abstract*—3-D stacks of complimentary metal–oxide–semiconductor (CMOS) integrated circuit (IC) chips for security applications monolithically embed backside buried metal (BBM) routing with low series impedance and high decoupling capability in a power delivery network (PDN), thanks to distributed capacitances over a full-chip backside area. The 3-D Si demonstrator integrating cryptographic engines was fabricated in a 0.13-μm CMOS technology with post-Si wafer-level BBM Cu processing with 10, 15, and 10 μm of thickness, linewidth, and space, respectively, along with through Si vias (TSVs) with 10 and 40 μm of diameter and depth, respectively. The capacitance of 0.18 nF/mm^2 in the effective backside area of 71 mm^2 suppressed dynamic IR drops in 10% and 59% for the single chip and four chip stack samples, respectively, during the operation of a 3.9 M-gate crypto core at 30 MHz. On-chip power noise monitoring (OCM) was applied in these measurements. The 3-D BBM PDN also effectively reduces power side channel information leakage, which is evaluated by 14$\times$ increase in the number of externally observed electromagnetic (EM) noise waveforms to attain the *t*-test value of larger than 4.5.**

***Index Terms*—Cryptographic engine, electromagnetic (EM) compatibility, on chip monitoring, power signal integrity, power supply noise (PSN), Si substrate backside, side channel leakage.**

I. Introduction

POWER and signal integrity (PSI) has been elaborately accomplished to sustain homogeneous as well as heterogeneous evolvements of very large scale integrated (VLSI) systems. Capacitors essentially contribute to bring stable and capable power delivery for high-performance circuit operation and also to prevent unexpected intercircuit interference due to power noise coupling. Those capacitors are desirably embedded in a system with the higher density and larger total capacitance, the more compact footprint and lower profile, and the higher voltage tolerance and smaller electrical impedance. Their leverage toward system performance prompts the advancement of Si wafer processing as well as post-Si packaging technology platforms.

On-die high-density capacitors have metal–insulator–metal (MIM) thin-layered structures within a metal stack or involve deeply etched trenches with dielectric and metal fillings. Package capacitors usually deploy multilayer ceramic capacitor (MLCC) surface mount discrete (SMD) components, which are located on the backside shadow of an integrated circuit (IC) chip or adjacent to it, called a land side capacitor (LSC) or a die side capacitor (DSC), respectively. On-die as well as package capacitors recently start to be embedded within a packaging interposer of high-performance large IC chips in high volume production, e.g., a microprocessor [1] and field-programmable gate array (FPGA) [2]. This aims at the very large total capacitance and efficiently decoupled utilization of semiconductor manufacturing sites with different technology nodes. Adopted technology platforms among literature include thin-film multiple layers within a plastic interposer [3], MIM and deep trench (DT) capacitors processed on a Si interposer [4], [5], DT capacitors by wafer-to-wafer bonding [6], and so forth. The suppression of power supply noise (PSN) is evaluated as general benefits, along with the improvements on clock jitters and delay time of critical logic paths.

While those capacitor technologies are primarily for 2.5-D interposer assembly [7], further developments are expected for PSI in 3-D VLSI systems [8]–[10]. This article describes BBM capacitors distributed over the whole 3-D complimentary metal–oxide–semiconductor (CMOS) chip stack. In addition to PSN suppression, we will introduce another measure of 3-D embedded capacitance on the benefits from hardware-security perspectives.

The backside of a Si substrate is an open space for passive elements to be integrated, which are almost free of

Manuscript received November 17, 2020; revised December 27, 2020; accepted January 31, 2021. Date of publication February 22, 2021; date of current version March 24, 2021. This work was based on results obtained from a project, JPNP16007, commissioned by the New Energy and Industrial Technology Development Organization (NEDO). This article is an extended version of a paper presented at IEDM 2020. The review of this article was arranged by Editor T. Grasser. *(Kazuki Monta and Hiroki Sonoda contributed equally to this work.) (Corresponding author: Kazuki Monta.)*

Kazuki Monta, Hiroki Sonoda, Takuji Miki, and Makoto Nagata are with the Graduate School of Science, Technology and Innovation, Kobe University, Kobe 657-8501, Japan (e-mail: monta@cs26.scitec.kobe-u.ac.jp).

Takaaki Okidono is with the Electronic Commerce Security Technology Research Association (ECSEC) Laboratory Inc., Tokyo 101-0054, Japan.

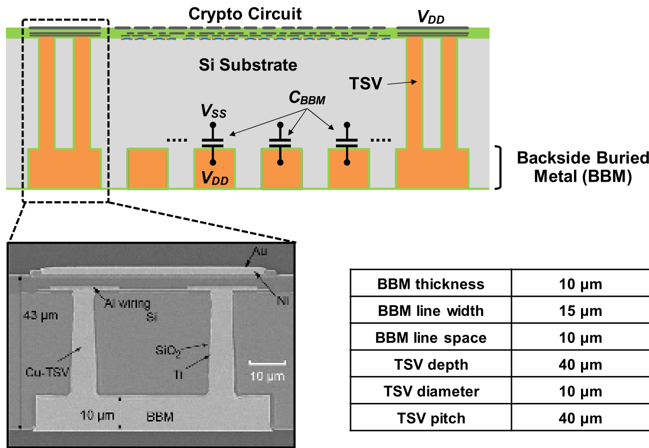
Yuuki Araga, Naoya Watanabe, Haruo Shimamoto, and Katsuya Kikuchi are with the National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba 305-8560, Japan.

Noriyuki Miura is with the Graduate School of Information Science and Technology, Osaka University, Osaka 565-0871, Japan.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TED.2021.3058226.

Digital Object Identifier 10.1109/TED.2021.3058226

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/



BBM thickness	10 µm
BBM line width	15 µm
BBM line space	10 µm
TSV depth	40 µm
TSV diameter	10 µm
TSV pitch	40 µm

Fig. 1. BBM structure (SEM photo from [13]).

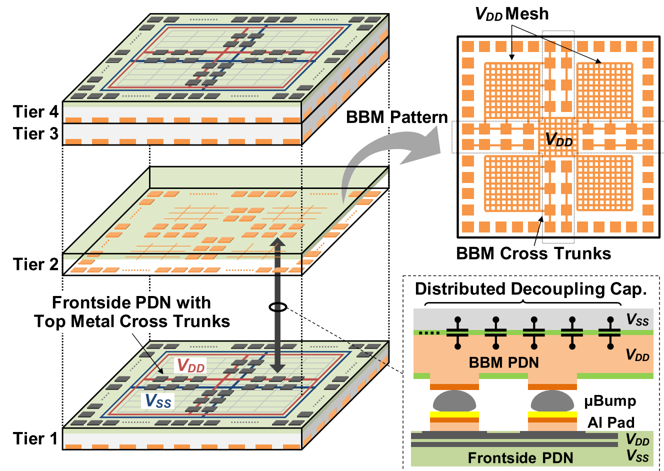


Fig. 2. Proposed 3-D stack with BBM PDN.

design constraints posed by transistor technology nodes on its front side. The BBM technique in a post CMOS wafer-level processing way has been developed to form thick and wide Cu stripes buried from the backside of Si [11]. The back- and front-side metal stacks are electrically connected by TSVs at the periphery of a die or in the area of high-voltage analog circuits to avoid keep out zones in a core logic area. This dual-side metallization has realized a passive Si interposer placed over a CMOS chip for in-package low-impedance power delivery [12] and a monolithic CMOS chip with backside attack protection circuits [13]. The Si backside technologies are in the trend of technology developments of near-core power supply functionality, as reported for monolithic PDNs in a very scaled technology toward 3-nm node [14], [15]. Another proposal is also given for the functionally integrated in-package magnetic core inductor [16].

In this article, we demonstrate the use of backside Si for integrated passives and routings for power delivery in a secure 3-D CMOS chip stack typically with cryptographic functions [17]. The next section describes PDN architecture using BBM. Section III details a demonstrator fabricated through wafer-level processing and assembled in a system. Measurement results will be described in Section IV. A brief summary will be given in Section V.

II. CMOS Power Delivery With BBM

The BBM routing in the cross-sectional view of Fig. 1 is formed through wafer-level post CMOS processing. In digital ICs consisting of conventional CMOS logic cells, the ground side (V_{SS}) nodes are strongly tied up on a p-type Si wafer through Si substrate contacts. With this reason, the whole BBM routing is dedicated to the power supply (V_{DD}) side of PDN, aiming at side and bottom wall capacitances distributed over the full-chip backside, C_{BBM}, for chip-wide PSN suppression. The BBM PDN is connected to the front-side counterpart by TSVs processed only at the position of I/O pads in the die periphery, so as not to interfere with layout of the core transistors in a logic cell array. The BBM PDN has the dimensions given in Fig. 1, featured by more than ten times thicker and wider Cu in comparison with typical front-side top-layer metal wirings. The BBM PDN reduces the on-chip PDN impedance, which is very much desirable to a large-area digital IC chip embodying such as public-key cryptographic algorithm.

In the 3-D evolution of BBM PDN in Fig. 2, the backside of an upper tier provides V_{DD} and V_{SS} BBM cross trunks that are directly contacted with surface μbumps on the front side of adjacent bottom tier. The μbumps are stacked on area Al pads and aligned in sequence respectively for V_{DD} and V_{SS} top metal cross trunks in the middle part of the CMOS front side. The remaining BBM portions fully belong to the V_{DD} domain and densely form meshes for PDN capacitance against Si substrate biased at V_{SS}. The V_{DD} and V_{SS} domains are, respectively, unified by the BBM cross trunks and TSVs in periphery for tier-to-tier vertical PDN interconnections, and, therefore, the BBM PDN capacitance is evenly distributed over the whole 3-D stack.

Flip-chip ball grid array packaging is adopted for assembly. The first (bottom) chip is faced to a fine-pitch plastic interposer, where μbumps on the periphery pads are directly contacted on Al lands of an interposer. The subsequent chips are homogeneously stacked. Fig. 3 shows the structural view and cross-sectional photos of a four-tier stack test sample. The BBM on the top tier is visible if the stack is decapsulated. It can be isolated from the PDN and biased to an externally applied clean voltage (e.g., V_{SHD}, for EM shielding).

III. Silicon Demonstrator Details

A. Power Delivery

A single chip implementation of BBM PDN is represented by the equivalent circuit of Fig. 4(a). A digital core is supplied by an on-chip micro voltage regulator module (μVRM) where the capacitance on the BBM meshes, C_{BBM}, is formed on the core V_{DD} against V_{SS} and serves as the immediate decoupling capacitor. Cryptographic engines are integrated in a digital core of the Si demonstrator in this article. To maximize the power delivery efficiency, the chip is flipped down and assembled on a plastic interposer where land-side capacitors, C_{LS}, can be additionally integrated on or within its laminates; however, the series impedance parasitic to routing and contacts (Z_{IP}) is unavoidable.

In a 3-D stack as given in Fig. 4(b), the identical chips with BBM and TSVs are cascaded in a flipped 3-D stack, aiming for

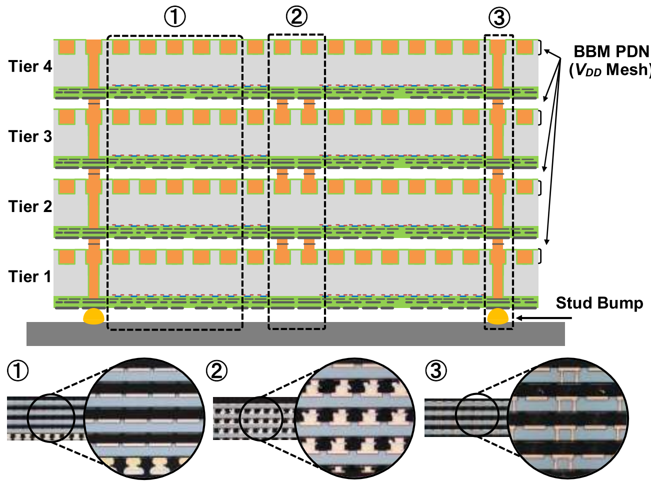


Fig. 3. Photos of 3-D stacking structure with BBM PDN.

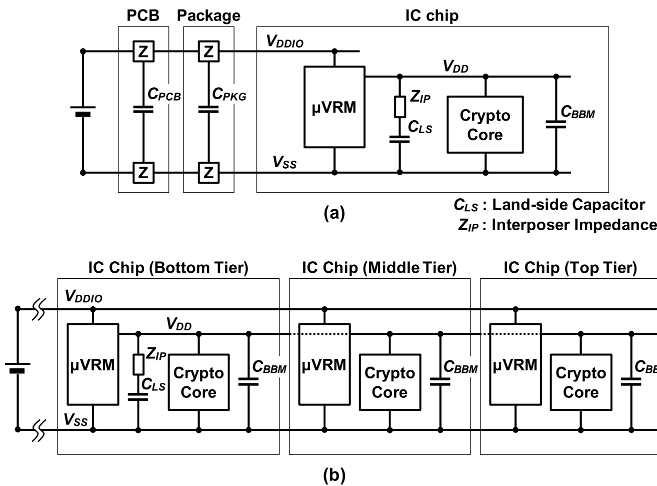
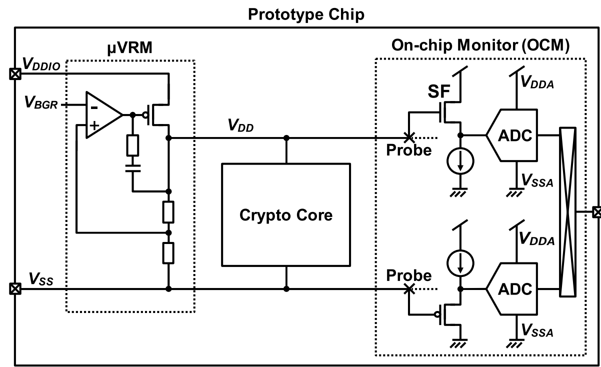


Fig. 4. Equivalent circuit of (a) single chip with BBM PDN, and (b) 3-D stacked chip with BBM PDN.



Chip Name	Crypto Algorithm	Chip Size	Num. of Logic Gates	μVRM	OCM	BBM Mesh (Line / Space)
Public Key Crypto #1	ECC*1	12 mm x 8 mm	2.9 M	O	O	15 μm / 35 μm
Public Key Crypto #2	ECC*1	12 mm x 8 mm	3.9 M	O	O	15 μm / 35 μm
Public Key Crypto #3	ECC*1	12 mm x 8 mm	4.3 M	O	O	15 μm / 35 μm
Private Key Crypto	AES*2	4 mm x 3 mm	203.5 K	O	O	15 μm / 10 μm
Digital TEG Chip	-	4 mm x 3 mm	70.8 K	O	O	15 μm / 10 μm
Analog TEG Chip	-	4 mm x 3 mm	0.1 K	-	-	15 μm / 10 μm

*1 Elliptic Curve Cryptography *2 Advanced Encryption Standard

Fig. 5. Circuit configuration of prototype chips.

the energy efficiency of parallelized crypto transactions. It is noted that the explicit capacitance of C_{BBM} for V_{DD} is inserted in every tier, while C_{LS} is accommodated only on the first one. C_{BBM} is not deteriorated by the series impedance between adjacent tiers thanks to distributed vertical PDN connections.

While V_{SS} is unified over the whole 3-D stack, V_{DD} on a respective tier is regulated by the μVRM or even halted in a power-down mode for logic circuits. Here, the V_{DD} voltage is generated with respect to V_{SS} as the global reference voltage. The BBM then lowers parasitic impedance primarily on the V_{DD} domain and consequently improves the capacity of power delivery in the whole 3-D chip stack.

B. Functionality

We have developed the prototype IC chip of Fig. 5 in a 0.13 μm six layer metal CMOS technology. A few derivatives of cryptographic algorithms are embodied as listed in the table. Public-key crypto cores are based on elliptic curve cryptography and differently designed with the number of 2-input NAND equivalent gates from 2.9 to 4.3 million in the same chip size of 12 $\times$ 8 mm^2. The digital cores are nominally supplied at 1.5 V by either a single μVRM or dual μVRMs, which are located on the left top and the right bottom corners of the chip, according to test scenarios. In addition, the small-scale chips of 4 $\times$ 3 mm^2 with some test circuits are prepared for the comparison of BBM capacitance.

On-chip power noise monitoring (OCM) function is equipped in each chip for the measurements of voltage variations on V_{DD} and V_{SS} nodes [9], [12]. The OCM channel includes a source follower (SF) to sense the voltage of interest at its input and a subsequent 11-bit successive approximation register (SAR) analog-to-digital converter (ADC) for on-chip voltage digitization. The SF with n- and p-channel MOSFET is prepared for the core V_{DD} nominally at 1.5 V and V_{SS} at 0.0 V voltages, in order to provide the negative and positive offset DC voltages at its output, respectively. This makes power noise voltages match the input voltage range of the ADC.

The photographies of front-side CMOS and backside BBM on the same die are shown in Fig. 6, along with magnified views around the center of die area showing cross trunks with μbump areas and BBM PDN meshes.

IV. Measurement Results

A. Passive Impedance Measurements

The capacitance of each chip in a standalone (not stacked), generally defined as the total capacitance between V_{DD} and V_{SS}, is measured with and without the BBM PDN, as shown in Fig. 7. The capacitance of Fig. 7 includes the parasitic caps to frontend circuitry and C_{BBM}. The capacitance per area of C_{BBM} are then dissolved through linear regression and summarized in Fig. 8. The density of BBM meshes differs among the small and large size chips and provides the capacitance of 0.25 and 0.18 nF/mm^2, respectively. The BBM capacitor in total of 12.8 nF (in average among the large area chips) is distributed over the full-chip backside.

In comparison with typical in-circuit structures such as metal-on-metal (MOM) and MIM capacitors, the capacitance

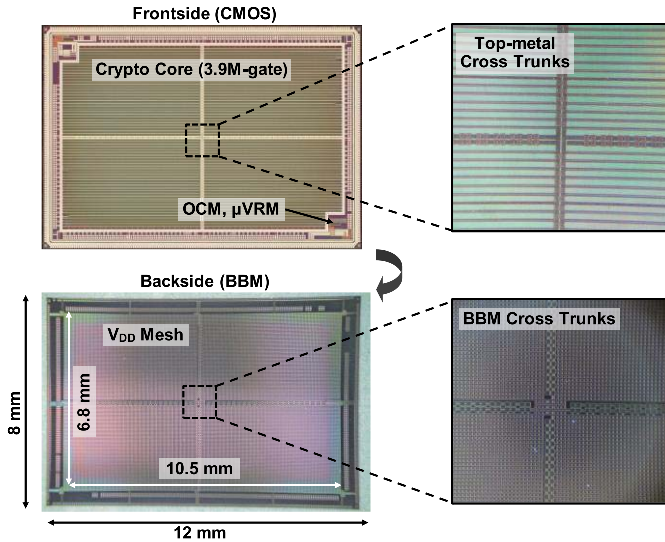


Fig. 6. Photos of front-side CMOS and backside BBM of fabricated chip (public key crypto #2).

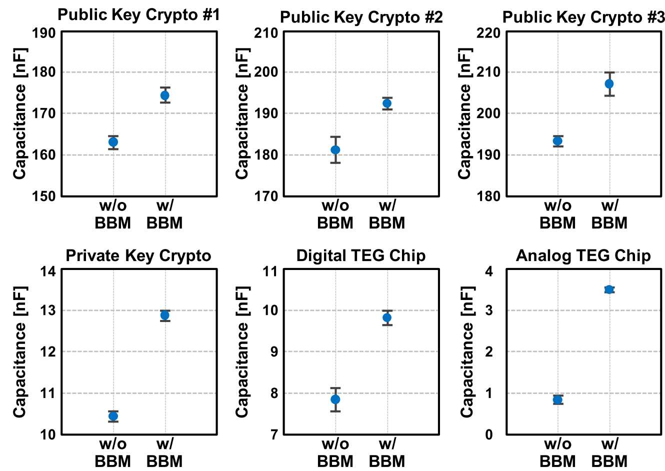


Fig. 7. Measured BBM capacitance of single chip.

Element	BBM	MOM	MIM	Gate Cap.
Unit Capacitance	Mesh #1 L=15 μm S=35 μm 0.18 fF/μm²; Mesh #2 L=15 μm S=10 μm 0.25 fF/μm²	≈ 1 fF/μm²	≈ 2 fF/μm²	≈ 4.2 fF/μm²
Density	≈ 100 % (Filled with meshes)	< 90 %	< 70 %	< 20 %
Capacitance per 1mm²	Mesh #1: 0.18 nF/mm²; Mesh #2: 0.25 nF/mm²	0.9 nF/mm²	1.4 nF/mm²	0.84 nF/mm²
Area Overhead	No area-overhead	All metal and device layers occupied	Top 2 metal layers occupied	M1 and device layers occupied

Fig. 8. Summary of BBM capacitance and comparison with other capacitive elements.

of BBM is roughly from 4× to 8× smaller. However, it is of importance to note that the BBM capacitor eliminates the sacrifice of front-side core areas. On the contrary, although the transistor gate electrode exhibits the largest capacitance, it imposes the highest area overheads associated with contacts and wirings and reduces the area efficiency. Those comparisons are executed with manual layouts and simulations according to physical design kits and rules of the given technology.

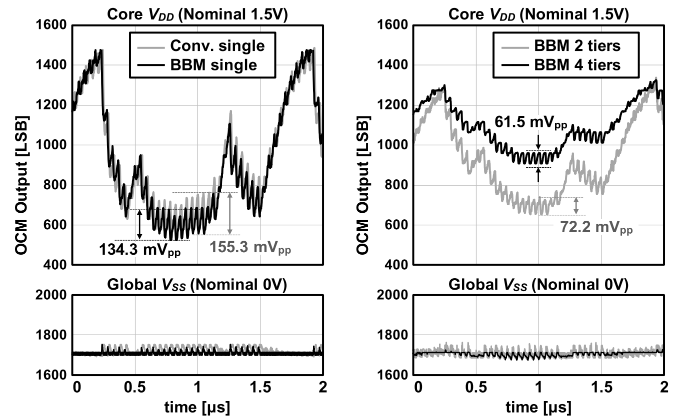


Fig. 9. Measured VDD and VSS waveforms during operation of public key crypto #2.

B. Active IR Drop Measurements

PSN is measured by the OCM during the operation of a cryptographic engine (public-key crypto algorithm #2) on the first tier. The waveforms are measured on V_{DD} and V_{SS} nodes as given in Fig. 9, among demonstrators with and without BBM. The measurements are also explored for a single chip as well as in 3-D chip stacks with two and four tiers. The vertical axis shows the voltage as measured in the step of least significant bit (LSB) of ADC, which is approximately 0.73 mV/LSB, and also includes the DC offset voltage of the SF. The horizontal time axis is resolved by the sampling interval of 1.0 ns, controlled by an external data timing generator.

The periodic voltage variations on V_{DD}, called dynamic IR drops, are synchronous to clocking and associated with the internal operation of addition and multiplication of binary data with the width of 256 bits or even larger. The huge number of logic gates is continuously toggling for each clock cycle during the arithmetic operations, which limits the maximum clock frequency at 30 MHz. The low-frequency droops, which continue for approximately 1.5 μs, follow to the evolvement of logic activities associated with mathematic expressions in crypto algorithm. It is shown that both periodic and low-frequency voltage variations are more suppressed with the larger number of tiers in a 3-D stack. On the other hand, the voltage among V_{SS} nodes is very stable around the nominal ground voltage, reflecting the strong unification of V_{SS} networks in the stack. The full use of BBM stripes on V_{DD} domains is, therefore, proven to be effective. There is no recognizable discrepancy among tested 3-D IC chip samples in cryptographic operation and in total power consumption.

The peak-to-peak voltage variation is derived from the waveforms and summarized in Fig. 10 for comparison between conventional and BBM stacks. The reduction of dynamic IR drops on V_{DD} nodes reaches 59% if the four-tier stack embeds BBM capacitors, which is 14% more efficient than in the conventional 3-D stack.

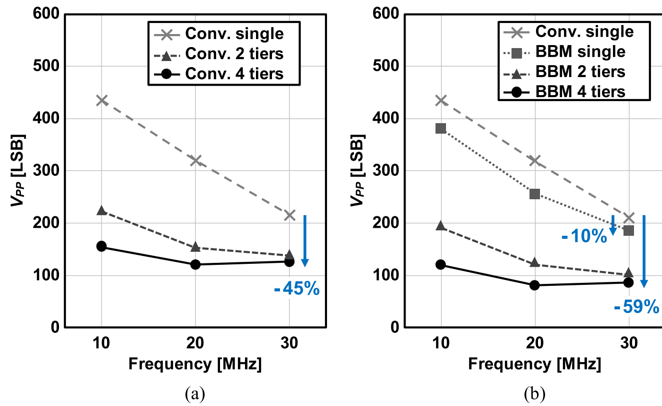


Fig. 10. Peak-to-peak values of VDD noise versus operation frequency in public key crypto #2. (a) Conventional stacks and (b) proposed BBM stack.

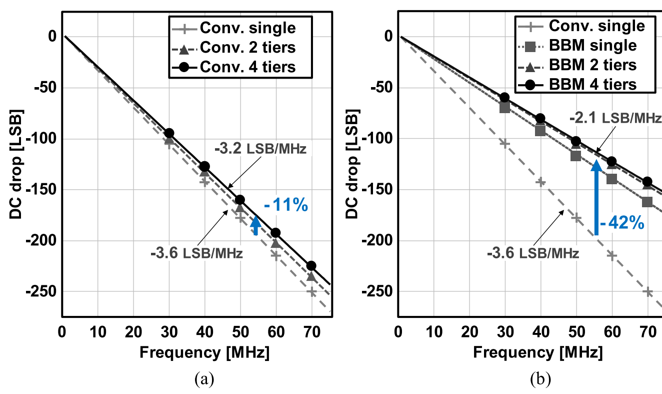


Fig. 11. Measured dc drop versus clock frequency when clock buffers are only operated. (a) Conventional stack and (b) proposed BBM stacks.

The effect of BBM stripes on the reduction of series impedance is estimated to be 42% as explained in Fig. 11. The resistance is derived from the slopes of on-chip power supply DC drops measured against the toggling frequency in clock buffer trees, where crypto cores are intentionally halted.

C. EM Radiation and SC Leakage Measurements

Dynamic IR drop suppression by the distributed BBM capacitance contributes to the mitigation of EM side channel (SC) leakage from cryptographic operation. This is straightforwardly expected since the local EM emissions that originate from nearby power supply current will be effectively suppressed by the distributed capacitances. The following experiments are provided to relate the SC leakage mitigation with the dynamic IR drop suppression. Fig. 12 shows the measurement setup where an EM probe senses local EM waves emitted from the demonstrator. The output from EM probe is amplified and then stored in an oscilloscope as EM waveform traces. The local EM radiation is governed by dynamic power current consumption of a crypto core and correlated with logic operation internally dealing with secret information. We have evaluated the hidden data dependence in EM radiation during crypto processing by applying the statistical t-test method on captured waveforms. The t-test value, t, suggests the presence of SC leakage when it exhibits the statistical significance with $|t| > 4.5$, according to the test vector leakage assessment

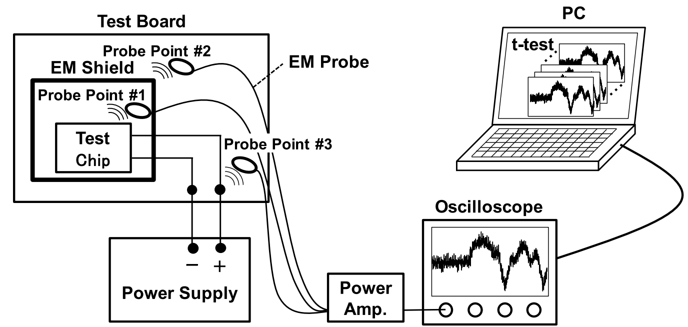


Fig. 12. Experimental setup for SC leakage evaluation.

(TVLA) methodology [18]. The t-test method has been widely adopted to quantify the effects of countermeasures against SC leakage in cryptographic engines at architecture and circuit levels [19], [20]. We apply this method to assess SC leakages among packaging structures.

The statistical significance is evaluated between two ensembles of EM traces measured in the crypto core operation of interest. The one uses a certain plain text of 256 bits uniquely over the entire set. The other chooses 256-bit plain text randomly generated in every input case. The EM measurement is alternatively performed on these two crypto operations, and EM traces are collected up to 20 K input cases. An oscilloscope stores EM traces, where each trace is averaged over five iterations of the crypto operation with an input case. The channel bandwidth of 125 MHz is chosen for waveform measurements. These measurement conditions are carefully designed to quantify and compare SC leakage suppression by the BBM capacitance among various 3-D stacked samples. The following measurement results firmly support and extend the experimental conclusions reported in [17].

First, we measure the local EM emission at the proximate position over the stack, as the measurement point #1 in Fig. 12. The highest SC leakage is observed for the single chip with BBM in Fig. 13 showing t-test values. This is naturally understood since the power consumption current of crypto operation flows through BBM as a part of V_{DD} wirings and strongly couples to the EM probe nearby its backside surface. The leakage is evidently attenuated as the number of chips in a 3-D stack increases, resulting from the power noise attenuation by BBM capacitance distributed over the stack. The number of EM traces to reach the significant leakage ($|t| > 4.5$) in the four-chip BBM stack becomes almost equivalent to the single chip without BBM. We have also experimentally confirmed that the suppression is almost negligible among multitier conventional 3-D stacks without BBM. It is important to claim that t-value no longer exceeds 4.5 even with 20 K test cases, if we cover the single chip with outer metal shields biased at V_{SHD}, as measured at the point #2 of Fig. 12.

Second, EM measurements were performed at the location of power supply terminals on the printed circuit board (PCB), as the point #3 in Fig. 12. This facilitates the leakage assessment by an adversary without knowing internal device structures. The t-test values are compared in Fig. 13 among the public-key crypto demonstrator in conventional assembly and in 3-D BBM stacking. The leakage level remains sufficiently suppressed over 20 K test cases in the four-tier stack with

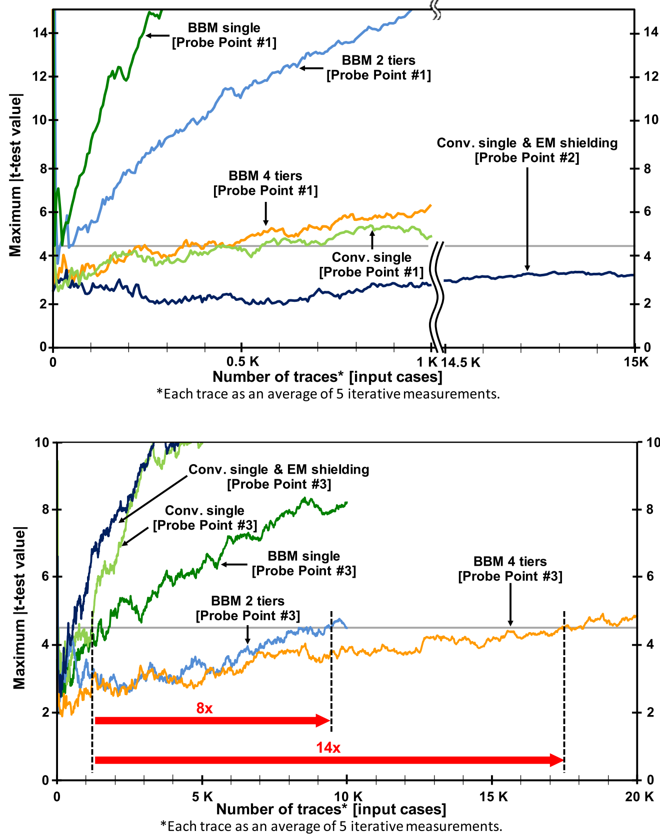


Fig. 13. *T*-test results of SC leakage measurements.

BBM, in contrast to the conventional single chip assembly even with EM shielding, achieving 14× increase in the number of EM traces for t-value >4.5. The increase is also measured as 8× for the two-tier BBM stacked demonstrator.

While the EM waves in the first measurements are vertically emitted from the backside plane of crypto chips, the second ones are caused on the board by power current horizontally flowing from on-die μVRMs having low-pass characteristics with limited bandwidth. EM radiation is more or less present in these measurements; however, the statistical significance among EM traces is effectively diminished with the distributed BBM capacitance.

V. Conclusion

The characteristics of BBM PDN in 3-D CMOS chip stacking are experimentally evaluated with Si demonstrators equipped with cryptographic engines and on-chip power noise monitors. Post-wafer BBM processing on 0.13-μm CMOS wafers attains 12.8 nF on the backside of a crypto chip. Up to four BBM chips are 3-D stacked and packaged in flip-chip assembly.

The advantage of BBM capacitance distributed over the 3-D stack efficiently attenuates dynamic IR drops on power nodes for 59% in voltage variation. The mitigation of SC leakage by 14× is achieved in comparison with conventional single chip assembly, which is metered with t-value representing the statistical significance from hardware security viewpoints.

The 3-D chip stacking with BBM PDN provides novel technology options toward high SC leakage resiliency among security ICs, in close collaboration with countermeasure design techniques of cryptographic circuits and algorithms.

References

[1] Y. Min *et al.*, "Embedded capacitors in the next generation processor," in *Proc. IEEE 63rd Electron. Compon. Technol. Conf. (ECTC)*, May 2013, pp. 1225–1229.

[2] M. Kim, H. Liu, D. Klokotov, A. Wong, T. To, and J. Chang, "Performance improvement for FPGA due to interposer metal insulator metal decoupling capacitors (MIMCAP)," in *Proc. IEEE 70th Electron. Compon. Technol. Conf. (ECTC)*, Jun. 2020, pp. 386–392.

[3] T. Akahoshi *et al.*, "Development of CPU package embedded with multilayer thin film capacitor for stabilization of power supply," in *Proc. IEEE 67th Electron. Compon. Technol. Conf. (ECTC)*, May 2017, pp. 179–184.

[4] B. Dang *et al.*, "Three-dimensional chip stack with integrated decoupling capacitors and thru-Si via interconnects," *IEEE Electron Device Lett.*, vol. 31, no. 12, pp. 1461–1463, Dec. 2010.

[5] S. Y. Hou *et al.*, "Integrated deep trench capacitor in Si interposer for CoWoS heterogeneous integration," in *IEDM Tech. Dig.*, Dec. 2019, pp. 19.5.1–19.5.4.

[6] E. Song *et al.*, "Power integrity performance gain of a novel integrated stack capacitor (ISC) solution for high-end computing applications," in *Proc. IEEE 70th Electron. Compon. Technol. Conf. (ECTC)*, Jun. 2020, pp. 1358–1362.

[7] P. Muthana *et al.*, "Design, modeling, and characterization of embedded capacitor networks for core decoupling in the package," *IEEE Trans. Adv. Packag.*, vol. 30, no. 4, pp. 809–822, Nov. 2007.

[8] I. Savidis, S. Kose, and E. G. Friedman, "Power noise in TSV-based 3-D integrated circuits," *IEEE J. Solid-State Circuits*, vol. 48, no. 2, pp. 587–597, Feb. 2013.

[9] M. Nagata, S. Takaya, and H. Ikeda, "In-place signal and power noise waveform capturing within 3-D chip stacking," *IEEE Des. Test*, vol. 32, no. 6, pp. 87–98, Dec. 2015.

[10] P. D. Franzon, E. J. Marinissen, and S. M. Bakir, Eds., *Handbook of 3D Integration: Design, Test, and Thermal Management*, vol. 4. Weinheim, Germany: Wiley, 2019.

[11] 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.

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

[13] 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.

[14] D. Prasad *et al.*, "Buried power rails and back-side power grids: Arm CPU power delivery network design beyond 5 nm," in *IEDM Tech. Dig.*, Dec. 2019, pp. 19.1.1–19.1.4.

[15] 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 μTSVs," *IEEE Trans. Electron Devices*, vol. 67, no. 1, pp. 11–17, Jan. 2020.

[16] X. Sun *et al.*, "3D heterogeneous package integration of air/magnetic core inductor: 89%-Efficiency buck converter with backside power delivery network," in *Symp. VLSI Technol. Circuits, Dig. Tech. Papers*, Jun. 2020, pp. 1–2.

[17] H. Sonoda *et al.*, "Secure 3D CMOS chip stacks with backside buried metal power delivery networks for distributed decoupling capacitance," in *IEDM Tech. Dig.*, Dec. 2020, pp. 1–4.

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

[19] T. Schneider and A. Moradi, "Leakage assessment methodology," *J. Cryptograph. Eng.*, vol. 6, no. 2, pp. 85–99, Jun. 2016.

[20] D. Šijačić, J. Balasch, B. Yang, S. Ghosh, and I. Verbauwhede, "Towards efficient and automated side-channel evaluations at design time," *J. Cryptograph. Eng.*, vol. 10, no. 4, pp. 305–319, Nov. 2020.