Impact of Power Distribution Network on Power Analysis Attacks in Three-Dimensional Integrated Circuits

Jaya Dofe, Zhiming Zhang, Qiaoyan Yu
Department of Electrical and Computer Engineering
University of New Hampshire, USA
qiaoyan.yu@unh.edu

Chen Yan and Emre Salman
Department of Electrical and Computer Engineering
Stony Brook University, USA
emre.salman@stonybrook.edu

ABSTRACT

Correlation power analysis (CPA) attacks on the hardware implementation of cryptographic algorithms can retrieve the cipher key by analyzing the correlation between hypothesized keys and the power measurement of that crypto hardware. The existing CPA attacks and the countermeasures are mainly for two-dimensional (2D) integrated circuits (ICs). There is a lack of study on CPA in the context of three-dimensional (3D) ICs. To fill in this gap, this work investigates the impact of a 3D power distribution network (PDN) on the efficiency of CPA mounted on a cryptographic module, which is in one of the 3D planes. The Pearson correlation coefficient is used as a metric to assess the impact of different PDN types, circuit loads, and switching activities of the neighboring planes on the CPA efficiency.

1. INTRODUCTION

Three-dimensional (3D) integrated circuits (ICs) have become increasingly attractive due to higher density and better global interconnect performance. Researchers have also leveraged the 3D technology to address the security threats on 2D chips. Techniques, such as split manufacturing and placing a cryptographic module in the middle layer of 3D chips, are developed to achieve higher resistance against reverse engineering and side-channel analysis attacks. The expected improvement on attack resistance mainly relies on the shielding capacity from the multiple planes in 3D chips. Unfortunately, the noise and thermal issues in 3D ICs may also hinder the applied security mechanisms from fully achieving the expected attack resistance. Security opportunities and challenges on 3D ICs have been identified in recent literature [1–5].

The secret key adopted in a cryptographic algorithm can be retrieved by correlation power analysis (CPA) attacks [6] mounted on hardware implementation, through the analysis on the correlation between hypothesized keys and the power measurement of that crypto hardware. To thwart side-channel attacks, existing works propose randomized countermeasures [7], intermediate data duplication [8], Boolean masking [9], dynamic and differential logic [10], and noise addition [11]. Alternatively, [12] and [13] have proposed to revise the traditional voltage regulators to alter the power measurement of the crypto hardware, thus improving the resistance against power analysis attacks. Since an accurate power measurement is vital for the success of CPA, we investigate the impact of power distribution networks on the efficiency of CPA, with special emphasis on the encryption engine within a 3D design environment.

The remainder of this work is organized as follows. Preliminaries of this work are introduced in Section 2. The related work and our main contributions are summarized in Section 3. The experimental setup for our study is presented in Section 4. Various dependent factors for CPA in 3D ICs are examined in Section 5. We conclude this work and discuss some future work in Section 6.

2. PRELIMINARIES

2.1 Power Distribution for 2D and 3D ICs

A modern power distribution network (PDN) consists of a global grid and multiple virtual grids that are connected to the global grid through sleep transistors and/or voltage regulators. Nominal power supply voltage is provided to the global grid through controlled collapse chip connection (C4) bumps, which connect the global grid with the flip-chip substrate. The virtual grids form voltage islands/domains that can be independently power gated. The grids are typically modeled with equivalent parasitic resistance and inductance per unit length, determined from the physical characteristics of the meta layers such as thickness, width, and spacing. On-chip decoupling capacitors are also used within these grids to provide instantaneous charge to switching load circuits, thereby reducing the transient power supply noise.

Power gating is a common method to significantly reduce subthreshold leakage current in nanoscale technologies [14]. For 3D systems, power gating is critical due to higher and heterogeneous integration where the amount of nonswitching circuits can be significantly high [15]. Thus, 3D ICs are expected to be heavily power gated to sufficiently reduce leakage power, as shown in Fig. 1. In this figure, the global grids of multiple planes are connected by via-last TSVs, which pass through the metal layers and connect the topmost metal layer in each plane.

Similar to 2D planar technologies, sleep transistors with high threshold voltage are utilized to achieve power gating in 3D ICs. These sleep transistors are distributed throughout

GLSVLSI '17, May 10 - 12, 2017, Banff, AB, Canada

ISBN 978-1-4503-4972-7/17/05...$15.00
DOI: http://dx.doi.org/10.1145/3060403.3060501

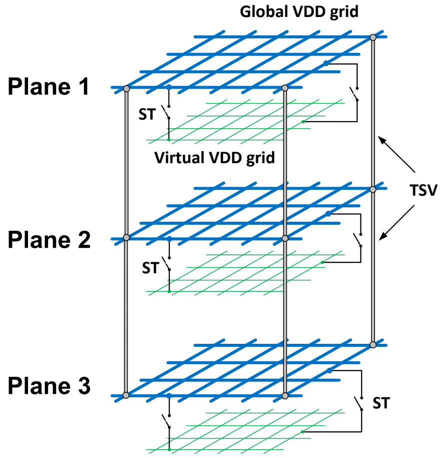


Figure 1: Power distribution network for a three-plane 3D IC with power gating, illustrating the global and virtual power grids, sleep transistors, and TSVs.

the entire 3D stack. In practice, a large number of sleep transistors is placed around the intended area to be power gated, forming a ring structure.

2.2 Power Supply Noise

A critical design challenge for TSV based 3D ICs is the reliable distribution of the power supply voltage to devices that are distributed throughout multiple planes [16]. The parasitic impedance of these additional planes, TSVs, and larger overall load current drawn from the power supply exacerbate the issue of power distribution by increasing both the peak and average power supply noise.

Furthermore, when a circuit block or an entire plane within a 3D IC transitions from sleep state to active state, a relatively large in-rush current is drawn to charge the capacitors in that block or plane, producing power noise at the semi-global or global power network. This noise affects the reliability of other active blocks and planes, and is referred to as *power gating noise* or *in-rush current noise*. Both power supply noise and power gating noise should be controlled to ensure that the functionality, timing performance, and reliability of the 3D system are satisfied. This paper studies whether power supply noise poses a challenge or offer an opportunity for power analysis attacks in 3D ICs.

2.3 Power Analysis Attacks

In cryptography, side-channel attacks (SCA) exploit the side-channel signals (e.g. timing, electromagnetic leak, thermal image, and power consumption) obtained from the hardware implementation of cryptographic algorithms to retrieve the confidential key applied in the cryptographic module. SCA techniques are more practical and time efficient than the brute force search. Among SCA techniques, power-based SCA (i.e. power analysis attack [6]) has been widely studied. Power analysis attacks are categorized in simple power analysis (SPA) [17], differential power analysis (DPA) [17], and correlation power analysis (CPA) [18].

In CPA, the attacker conducts theoretical predictions of the power consumption for the hardware implementation of the cryptographic algorithm. During the prediction, for a hypothesized key, the attacker can use the Hamming weight model or Hamming distance model to predict the number of bit transitions happened in the crypto state registers and thus estimate the associated power change between two consecutive clock cycles. Next, the theoretical estimation is compared with the real measurements. The Pearson correlation coefficient has been identified as an effective metric to assess how close a hypothesized key is to the true cipher key. The detailed CPA procedure is described in [6].

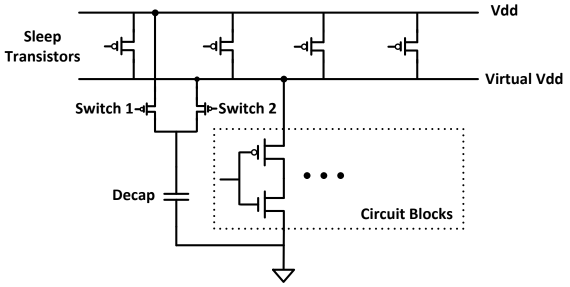


Figure 2: Conceptual representation of the reconfigurable decoupling capacitor topology with power gating.

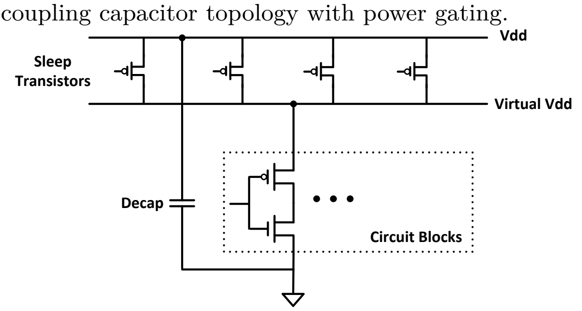


Figure 3: Conceptual representation of the always-on decoupling capacitor topology with power gating.

3. RELATED WORK

3.1 3D Power Noise Management

In traditional power networks, decoupling capacitors are typically connected to the virtual grids since a shorter physical distance between the capacitor and load circuit enhances the efficacy of the capacitor. In power gated 3D ICs, however, significant decoupling capacitance is lost when a block or plane is power gated. Thus, power gating in 3D ICs degrades the efficiency of decoupling capacitors in traditional power networks, thereby increasing the power supply noise. As demonstrated in previous research, decoupling capacitors placed in a plane can be highly effective for other planes in 3D ICs due to relatively low impedance TSVs [19]. Thus, unlike 2D ICs, decoupling capacitors in 3D ICs have a larger effective range. To leverage this characteristic, reconfigurable decoupling capacitors have been proposed for power gated 3D ICs [20]. In this method, as illustrated in Fig. 2, a decoupling capacitor is connected to the virtual grid through switch 2 when the load circuit (or the plane) is on. This configuration ensures that the impedance between the capacitor and the circuit is sufficiently low. Alternatively, when the plane is power gated, the decoupling capacitor is connected to the global grid through switch 1. Thus, even though the plane is gated, the decoupling capacitors within that plane can still be effective in reducing power supply noise of the other planes through low impedance TSVs. As a reference and comparison, an always-on topology has also been proposed where the decoupling capacitors are always connected to the global grid, as depicted in Fig. 3. Reconfigurable decoupling capacitor topology can achieve up to 50% and 87% reduction in, respectively, rms power supply and power gating noise at the expense of a moderate increase in physical area and power consumption [19]. The effect of these different 3D decoupling capacitor topologies on power analysis attacks is investigated in this paper.

3.2 Countermeasures for Power Analysis Attacks

A current flattening circuit based countermeasure is proposed in [21] to thwart DPA attacks in smart cards. This approach uses an analog control loop to maintain overall current consumption of the system to a predefined value. A dynamic voltage and frequency switching approach is presented in [22] to randomize the power traces and prevent the attacker from performing time correlation between different power traces. Double width single core (DWSC) method in [23] is another power balancing technique. The main idea of that work is to introduce complementary signal transitions along with the original ones to balance the power variations due to different input patterns, hence obscuring the correlation between internal computations and device power consumption. An internally generated random mask based digitally controlled ring oscillators is used to dynamically change the power consumption and thus thwart first order DPA attacks [24]. Other random masking based countermeasures are discussed in [25,26]. On-chip noise generation, clock randomization, and memory scrambling techniques are exploited in [11] to obscure the power profile.

3.3 Countermeasures for Other Side-channel Attacks in 3D ICs

Countermeasures for other side-channel attacks in 3D ICs have also attracted significant attention. In [27], a crypto co-processor is located in one of the 3D planes. To mitigate the side-channel attack on the access-driven cache in the co-processor, a dedicated memory is proposed to store cryptographic state and secret keys during the operations [27]. A 3D architecture is proposed to shield the thermal side-channel information in [2], where a micro-controller is applied to produce the dynamic random complementary activity patterns to hinder the side channel leakage. To defeat the cache-timing side-channel attacks in 3D ICs, a random eviction cache was introduced, which was designed to decorrelate timing information and key-dependent data [5].

3.4 Contributions of This Work

The main contributions of this work are as follows:

- To the best of our knowledge, this is the first work that studies the impact of the power supply noise induced by PDNs on the power analysis attacks in the context of 3D ICs.
- This work compares the power traces of a Sbox for the Advanced Encryption Standard (AES) measured with an ideal PDN, a nonideal 2D PDN, and a nonideal 3D PDN. We used a case study to quantitatively show the impact of different power supply noise on the correlation coefficient between the predicted and measured power consumption of the Sbox.
- We also examine the impact of different PDN topologies and the circuit switching activities in neighboring planes on the CPA efficiency.

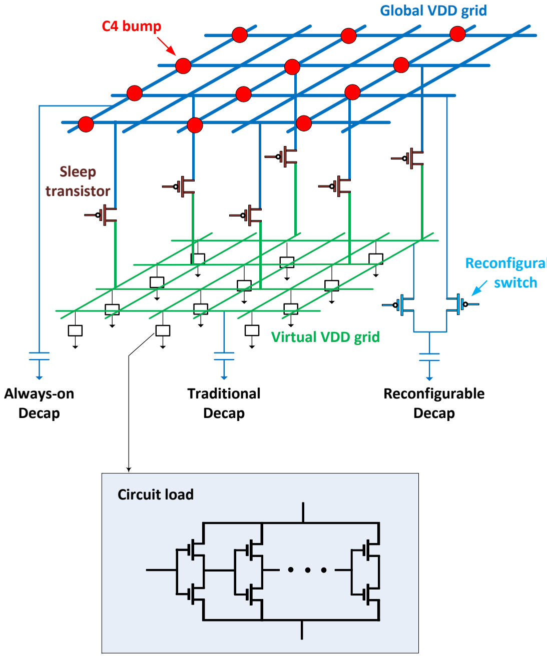


Figure 4: Plane-level power network illustrating distributed sleep transistors, decoupling capacitors (traditional and proposed topologies), switching load, and the C4 bumps.

4. EXPERIMENTAL SETUP

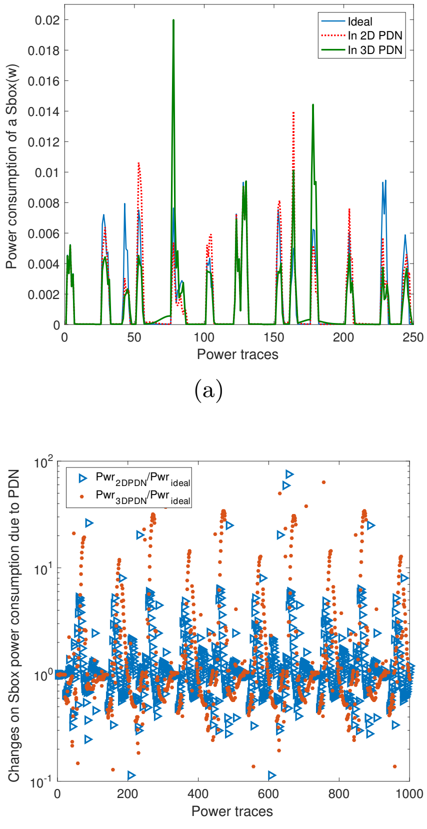
A power distribution network for a three-plane 3D IC with via-last TSVs is generated in 45 nm technology with 10 available metal layers in each plane. A portion of the power network with an area of 1 mm by 1 mm is analyzed. Each plane consists of a global power network, virtual power network, distributed sleep transistors [28], distributed decoupling capacitance, and distributed switching load circuit consisting of inverter gates and Sbox, as depicted in Fig. 4. Details of the power network characteristics can be found in [19].

We conducted power analysis attacks on a Sbox module for the iterative gate-level implementation of AES-128. We synthesized the Sbox Verilog HDL description in the Synopsys Design Compiler with a NCSU FreePDK at the 45nm technology node. The synthesized Sbox netlist was imported into the Cadence Virtuoso to perform transistor-level simulation. Pseudo-random inputs were provided as the stimulus for the Sbox. We used 10GHz frequency to sample the instantaneous power of the Sbox and formed 1000 power traces from our simulation. The Sbox module is placed in the middle plane of the 3D chip. The load circuits for the PDN are inverters with different sizes to mimic different load circuits in practical 3D ICs [19]. The analyses in Section 5 are based on the experimental setup mentioned here.

5. IMPACT OF POWER SUPPLY NOISE ON POWER ANALYSIS ATTACKS IN 3D ICS

5.1 Impact of Power Noise on Sbox Power Consumption

As the first step, we quantitatively compare the Sbox power trace extracted from an ideal Sbox power measure-



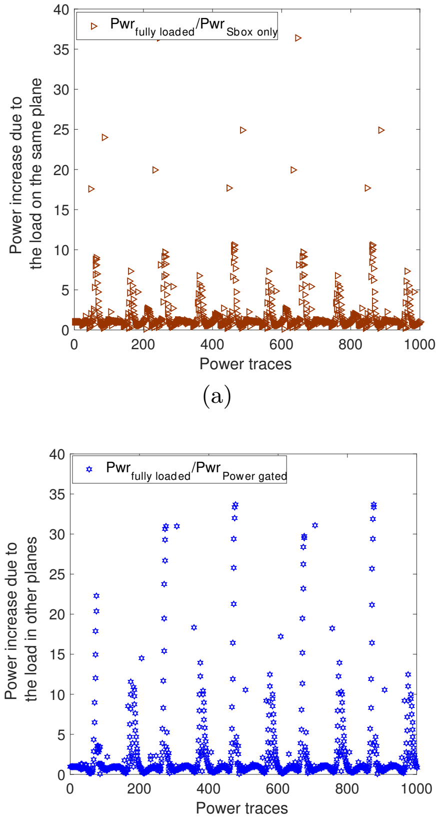
(b)

Figure 5: Impact of power distribution network on the Sbox power consumption. (a) Cropped 250 power traces, and (b) Changes on Sbox power consumption over ideal Sbox power.

ment (i.e. DC voltage supply for Vdd), with a 2D and 3D PDN. As shown in Fig. 5(a), the presence of 2D and 3D PDNs causes the peak power of the Sbox to shift, earlier or later, due to the power supply noise. Compared to the 2D PDN, the 3D PDN introduces larger noise and a more noticeable skew on power profile. Figure 5(b) indicates that the instantaneous power change caused by PDN is in the range of 0.1× and 100× over the ideal Sbox case. The average instantaneous power increase due to the 2D PDN is 172.22%, and the corresponding standard deviation is 4.6442. If the Sbox is connected to the 3D PDN, the average instantaneous power increase is 368.72% with a standard deviation of 7.5938. As a result, the 3D PDN can almost double the average change on the Sbox instantaneous power as compared to the 2D PDN.

5.2 Impact of Co-existing Load Circuits on Sbox Power Consumption

There are two load circuits (other than the Sbox module) within the 3D chip, those from the Sbox plane (denoted as same plane hereafter) and those from the neighboring planes (denoted as planes 1&3 hereafter). To study the impact of the co-existing load from the same plane on the Sbox power, we examined two cases: (1) Only one Sbox module is added to the middle plane (considered as Sbox only), and (2) one Sbox and many inverters (considered as fully loaded).



(b)

Figure 6: Impact of other circuit switching activities from (a) the same plane and (b) the other 3D planes on the Sbox power consumption.

As shown in Fig. 6(a), the other load circuits within the same PDN indeed affect the power trace of the Sbox, due to the power supply noise. If the planes 1 and 3 are fully loaded with inverters, the cross-plane current and voltage noise passed through the 3D PDN produces a more significant effect on the Sbox power as compared to 2D PDN. This is shown in Fig. 6(b). The circuit load in the neighboring planes causes 72.21% more power change than the load on the same plane with the Sbox. In addition, the standard deviation of power change due to the load on other planes is 1.72× larger as compared to the same plane load.

5.3 Variation of Power Noise Effects due to Different PDN Topologies

In this subsection, the impact of different PDN topologies on the Sbox power is examined. As shown in Fig. 7(a), if the middle plane has only Sbox as the load circuit and the other two planes (1 and 3) are power gated, the type of PDN adopted in the 3D design has negligible impact on the Sbox power. The measured instantaneous power in different PDNs is almost identical. In Fig. 7(b), the middle plane has other load circuit in addition to Sbox. In this case, when the planes 1 and 3 are power gated, all PDNs start to introduce random noise and thus change the Sbox power profile. Traditional PDN cannot reduce power noise as much, thus contributing more to the Sbox power change than the always-on and reconfigurable PDNs. As shown in Figs. 7(c)

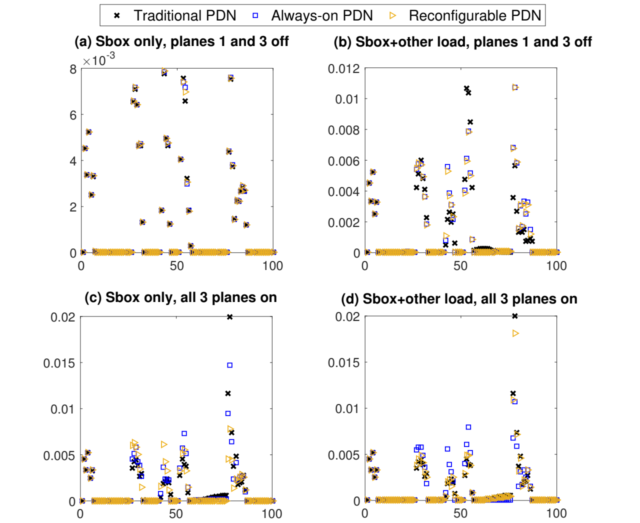


Figure 7: Impact of PDN types on the Sbox power consumption. (a) Only Sbox in plane 2, planes 1&3 off (b), Sbox and other load in plane 2, planes 1&3 off, (c) only Sbox in plane 2, all planes on, and (d) Sbox and other load in plane 2, all planes on. Note, in all subfigures above, X-axis and Y-axis are power traces and Sbox power consumption, respectively.

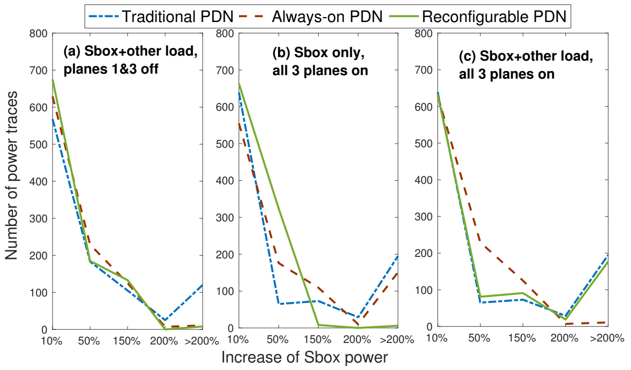
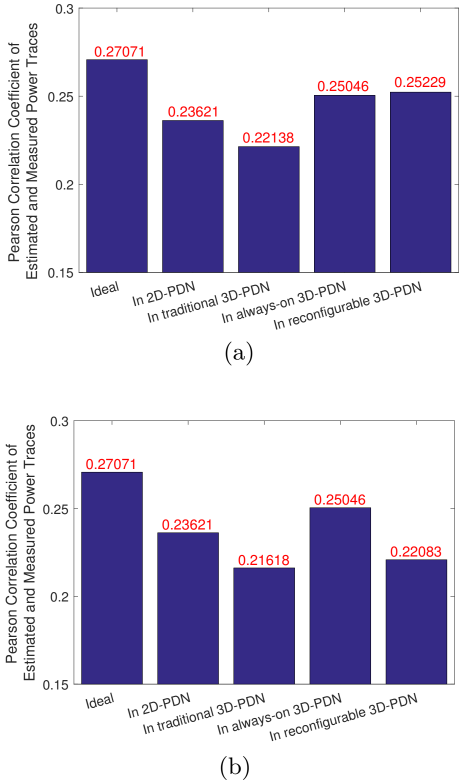


Figure 8: The percentage of Sbox power increase due to different PDNs and the load circuits in the 3D planes.

and (d), once all three planes are turned on, the effect of different PDNs on the Sbox power is noticeable. As compared to Fig. 8(a), the number of power traces that results in power increase by less than 50% is reduced, as indicated in Figs. 8(b) and (c). The reconfigurable PDN is capable to address the power grid noise even though the PDN in other planes is power gated, thus affecting the Sbox power the least (if the Sbox module occupies the entire plane). However, when the plane having the Sbox module includes other load circuits, the always-on PDN adds less noise than the traditional and reconfigurable PDNs. As a result, the Sbox power is less affected by the always-on PDN than the other two types of PDNs.

5.4 Power Correlation Modification due to PDN

As discussed in the previous subsections, the power distribution network changes the power profile of the cryptographic module of interest. The effect of the noise induced by the power grid on the correlation between the predicted and measured power of the Sbox is investigated in this section. We used Pearson correlation coefficient [6] as the evaluation metric. Each PDN is fully loaded with inverters, other than the Sbox module.



(a)

(b)

Figure 9: Pearson correlation coefficient between the measured and estimated Sbox power. (a) Sbox plane on and other planes off, (b) all planes on.

First, the planes 1 and 3 are power gated and only the Sbox plane is active. As shown in Fig. 9(a), the correlation coefficient for the other scenarios is less than that for the ideal Sbox power measurement case. This indicates that the power grid noise indeed can obscure the Sbox power profile. However, the degree of power profile alteration due to PDN varies with the PDN topology and the noise management mechanism applied in the PDN. The traditional 3D-PDN leads to the worst power grid noise, resulting in the lowest power correlation coefficient than other cases. Always-on and reconfigurable 3D-PDNs have different kind of noise management mechanisms, and hence the corresponding correlation coefficient goes up by 0.03 over the traditional 3D-PDN. When we turn on all three planes, the power correlation coefficient of the reconfigurable PDN case decreases. This is because the reconfigurable 3D-PDN offers similar performance on power grid noise to the traditional 3D-PDN when all planes are on.

6. CONCLUSION AND FUTURE WORK

Power analysis attacks have been demonstrated as a powerful mean to retrieve the secret key from the hardware implementation of a cryptographic algorithm. Generally, it is expected that the use of power analysis attacks on a cryptographic module embedded in a 3D chip is more difficult than a 2D IC due to the shielding effect among the 3D layers. There is a lack of detailed investigation on how the 3D structure affects the efficiency of power analysis attacks. In this work, we study the impact of power distribution networks on correlation power analysis (CPA) mounted on the non-linear unit, Sbox. Our simulation results show that the 3D power distribution network induces noise to the Sbox power measurement, which makes the CPA more challenging. The switching activities of the load circuits located in the same plane as the Sbox module change the power profile of the Sbox, as well. The impact of different types of decoupling capacitors (traditional, always-on, and reconfigurable) on the power traces for Sbox is examined. Our experiments indicate that the PDN with noise management modules makes the CPA easier.

7. REFERENCES

[1] J. Dofe, Q. Yu, H. Wang, and E. Salman, "Hardware security threats and potential countermeasures in emerging 3d ics," in *Proc. of GLSVLSI '16*, pp. 69–74, 2016.

[2] P. Gu *et al.*, "Leveraging 3d technologies for hardware security: Opportunities and challenges," in *Proc. of GLSVLSI '16*, pp. 347–352, 2016.

[3] Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, and M. Tehranipoor, "Security and vulnerability implications of 3d ics," *IEEE Trans.on Multi-Scale Computing Systems*, vol. 2, pp. 108–122, April 2016.

[4] J. Dofe, C. Yan, S. Kontak, E. Salman, and Q. Yu, "Transistor-level camouflaged logic locking method for monolithic 3d ic security," in *Proc. of AsianHOST'16*, pp. 1–6, Dec 2016.

[5] C. Bao and A. Srivastava, "3d integration: New opportunities in defense against cache-timing side-channel attacks," in *Proc. of ICCD*, pp. 273–280, Oct 2015.

[6] O. X. Standaert, E. Peeters, G. Rouvroy, and J. J. Quisquater, "An overview of power analysis attacks against field programmable gate arrays," *Proceedings of the IEEE*, vol. 94, pp. 383–394, Feb 2006.

[7] E. Oswald and M. Aigner, "Randomized addition-subtraction chains as a countermeasure against power attacks," in *Proc. of CHES'01*, pp. 39–50, 2001.

[8] L. Goubin and J. Patarin, "Des and differential power analysis (the "duplication" method)," in *Proc.of CHES'99*, pp. 158–172, 1999.

[9] M.-L. Akkar and C. Giraud, "An implementation of des and aes, secure against some attacks," in *Proc. of CHES'01*, pp. 309–318, 2001.

[10] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. of ESSCIRC'02*, pp. 403–406, Sept 2002.

[11] G. Tim and M. Amir, "Generic side-channel countermeasures for reconfigurable devices," in *Proc. of CHES'11*, pp. 33–48, 2011.

[12] M. Kar *et al.*, "Exploiting fully integrated inductive voltage regulators to improve side channel resistance of encryption engines," in *Proc. of ISLPED '16*, pp. 130–135, 2016.

[13] W. Yu and S. Kose, "A voltage regulator-assisted lightweight aes implementation against dpa attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, pp. 1152–1163, Aug 2016.

[14] H. Jiang, M. Marek-Sadowska, and S. Nassif, "Benefits and Costs of Power-gating Technique," in *Proceedings of IEEE International Conference on Computer Design*, pp. 559 – 566, October 2005.

[15] H. Wang and E. Salman, "Resource Allocation Methodology for Through Silicon Vias and Sleep Transistors In 3D ICs," in *Proc. IEEE ISQED*, pp. 528–532, March 2015.

[16] S. M. Satheesh and E. Salman, "Power Distribution in TSV-Based 3-D Processor-Memory Stacks," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 2, pp. 692–703, December 2012.

[17] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 5–27, 2011.

[18] B. Eric, C. Christophe, and O. Francis, "Correlation power analysis with a leakage model," in *Proc. of CHES'04*, pp. 16–29, 2004.

[19] H. Wang and E. Salman, "Decoupling Capacitor Topologies for TSV-Based 3-D ICs With Power Gating," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, vol. 23, pp. 2983–2991, December 2015.

[20] H. Wang and E. Salman, "Enhancing System-wide Power Integrity In 3D ICs With Power Gating," in *Proc. IEEE ISQED*, pp. 322–326, March 2015.

[21] R. Muresan and S. Gregori, "Protection circuit against differential power analysis attacks for smart cards," *IEEE Trans. on Computers*, vol. 57, no. 11, pp. 1540–1549, 2008.

[22] S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach," in *Proc. of DATE'05*, pp. 64–69 Vol. 3, March 2005.

[23] A. Arora, J. A. Ambrose, J. Peddersen, and S. Parameswaran, "A double-width algorithmic balancing to prevent power analysis side channel attacks in aes," in *Proc. of ISVLSI*, pp. 76–83, Aug 2013.

[24] P. C. Liu, H. C. Chang, and C. Y. Lee, "A low overhead dpa countermeasure circuit based on ring oscillators," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, pp. 546–550, July 2010.

[25] E. Prouff and M. Rivain, "Masking against side-channel attacks: A formal security proof," in *Proc. of EUROCRYPT'13*, pp. 142–159, 2013.

[26] C. Claude *et al.*, "Higher-Order Masking Schemes for S-Boxes," in *Proc. of FSE'12*, pp. 366–384, 2012.

[27] J. Valamehr *et al.*, "Cryptography and security," ch. A Qualitative Security Analysis of a New Class of 3-d Integrated Crypto Co-processors, pp. 364–382, 2012.

[28] H. Wang and E. Salman, "Power Gating Methodologies in TSV Based 3D Integrated Circuits," in *Proc. of the ACM/IEEE GLSVLSI*, pp. 327–328, May 2013.