Integration, the VLSI Journal 73 (2020) 30–42

Contents lists available at ScienceDirect

Integration, the VLSI Journal

journal homepage: www.elsevier.com/locate/vlsi

Improving power analysis attack resistance using intrinsic noise in 3D ICs

Zhiming Zhang [a], Jaya Dofe [b], Qiaoyan Yu [a,*]

[a] Department of Electrical and Computer Engineering, University of New Hampshire, Durham, NH, 03824, USA
[b] Department of Computer Engineering, California State University, Fullerton, CA, 08231, USA

ARTICLE INFO

Index Terms:
AES
Correlation power analysis (CPA)
Intrinsic noise
Three-dimensional (3D) integration
Power distribution network (PDN)
Side-channel analysis (SCA)
Attack resilience

ABSTRACT

Three-dimensional (3D) integration is envisioned as a natural defense to thwart side-channel analysis (SCA) attacks on the hardware implementation of cryptographic algorithms. However, neither physical experiments nor quantitative analysis is available in existing works to study the impact of power distribution network (PDN) on the SCA attacks. Through quantitative analyses and experiments with realistic 3D models, this work demonstrates the impact of noise in PDN on the 3D chip's resilience against correlation power analysis (CPA) attack, which is one of SCA attacks. The characteristic of PDN noise is extracted from our experiments. To expand the natural defense originated from the 3D integration, this work proposes to exploit the PDN noise inherently existing in 3D chips to thwart CPA attacks. Instead of introducing external noise or flattening the power profile, the proposed method utilizes the spatially and temporally varied supply voltages from other 3D planes to blur the power correlation of the crypto unit. Both theoretical analysis and experimental validation prove that the proposed method can effectively enhance the resilience of a crypto unit embedded in the 3D chip against CPA attacks. Simulation results show the proposed method improves the average guessing entropy by 9× over the baseline. Emulation on an FPGA platform demonstrates that the proposed method successfully slows down the key retrieval speed of CPA attack, with significantly less power overhead than representable power equalization techniques. Test vector leakage assessment (TVLA) shows that the proposed method improves the confidence to accept null hypothesis 201× over the baseline.

1. Introduction

Side-channel analysis (SCA) attack retrieves the secret key applied in a cryptographic device by analyzing the side-channel signals (e.g., power, delay, and electromagnetic leakage) gained from the physical implementation of that device. Among various power-based SCAs, correlation power analysis (CPA) outperforms simple power analysis (SPA) and differential power analysis (DPA) [1], receiving more attentions [2,3]. Existing efforts on CPA attacks and their counteracting techniques are primarily limited in the context of hardware implemented with two-dimensional (2D) integrated circuits (ICs). As the technology node is approaching to the physical limit of silicon, three-dimensional (3D) integration becomes a promising path to facilitate further growth in transistor density and performance. Unfortunately, studies of CPA in the context of the 3D ICs have not been widely explored yet. Our work fills a gap in this field.

The surveys [4,5] envision that SCA in 3D ICs may be more challenging than in 2D ICs, but neither physical experiment nor quantitative analysis is available in those surveys. The work [6] predicts that due to the integration of multiple components on the 3D chip, the increased noise on the side-channel signal (power) will challenge the power analysis attack. Hence, the 3D integration can act as a natural defense to resist the power analysis attacks. Our work based on the realistic power distribution network (PDN) [7] demonstrates that the 3D PDN introduces noise to the power profile of the crypto unit embedded in the 3D chip. As a result, the 3D PDN noise could ease or challenge CPA attacks in 3D ICs, depending on the load switching activities, PDN topology, and crypto module deployment in the 3D chip. The preliminary version of this paper is available in Ref. [8]. We extend our early work by providing the second practical implementation method to alter the power supply of complete AES crypto module in FPGA and validating the CPA attack resilience of our method.

The rest of the paper is organized as follows. The related work and major contributions are summarized in Section 2. The preliminaries and our prior observations are provided in Section 3. Theoretical analysis on the characteristics of 3D PDN noise is presented in Section 4. Exper-

* Corresponding author.
E-mail addresses: jdofe@fullerton.edu (J. Dofe), qiaoyan.yu@unh.edu (Q. Yu).

https://doi.org/10.1016/j.vlsi.2020.02.007
Received 23 October 2019; Received in revised form 11 February 2020; Accepted 16 February 2020
Available online 21 March 2020
0167-9260/

imental analysis of the effect of PDN noise on CPA attacks is discussed in Section 5. Our countermeasure to enhance the resilience of 3D chips against CPA attacks is proposed in Section 6. The experimental results are presented in Section 7. This work is concluded in Section 8.

2. Related work and our contributions

2.1. Existing Countermeasures against power-based SCA

Countermeasures against power-based SCA aim for eliminating the power-data dependency of the cryptographic device. Algorithm-level dummy instruction insertion yields power trace misalignment at the cost of increased execution time [9]. Masking techniques randomize the intermediate values of the crypto module to change the correlation between the hypothesized and measured power [9]. However, it is typically challenging to implement a cost-effective de-masking process due to the non-linear function in the cryptographic algorithm. Power balancing techniques [10,11] are used to distort the power measurement for the crypto module. Power balancing methods attempt to maintain the power consumption at the same level regardless of the input, thus making the power consumption non-correlated with the secret key. Unfortunately, power balancing techniques lead to large power overhead. Circuit-level techniques for power line isolation, such as switching capacitor based current equalization [12], generally result in power increase and performance loss. The analog component for power line isolation is difficult to reuse and requires extra efforts on a layout and routing [9]. To increase the power variance, on-chip noise generation approaches introduce noise by inserting buffers to draw current [13], or scale voltage and frequency [14,15]. However, the noise manipulation on voltage and frequency makes the system vulnerable to the attack that scales the power model accordingly [9]. In addition, the isolated noise generator could be muted by experienced attackers.

A current flattening circuit based countermeasure is proposed in Ref. [16] 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 Ref. [14] to randomize the power traces and prevent the attacker from performing time correlation between different power traces. Double width single core (DWSC) method in Ref. [17] 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 [18]. Other random masking based countermeasures are discussed in Refs. [19,20]. On-chip noise generation, clock randomization, and memory scrambling techniques are utilized in Ref. [21] to obscure the power profile.

2.2. Contributions of this work

The main contributions of this work are as follows:

1) We perform theoretical analysis to identify the relationship between power correlation coefficient and the statistical parameters of additive and multiplicative noise and validate it using MATLAB simulation.
2) We analyze the characteristics of noise induced by PDNs from other planes and examine the impact of 3D PDN noise on the efficiency of CPA attacks in 3D ICs via realistic 3D model based experiments.
3) To enhance the resilience of 3D chips against CPA attacks, we propose to exploit the inherent PDN noise from other 3D planes to introduce additive noise to the power profile of the crypto module embedded in the 3D chip.

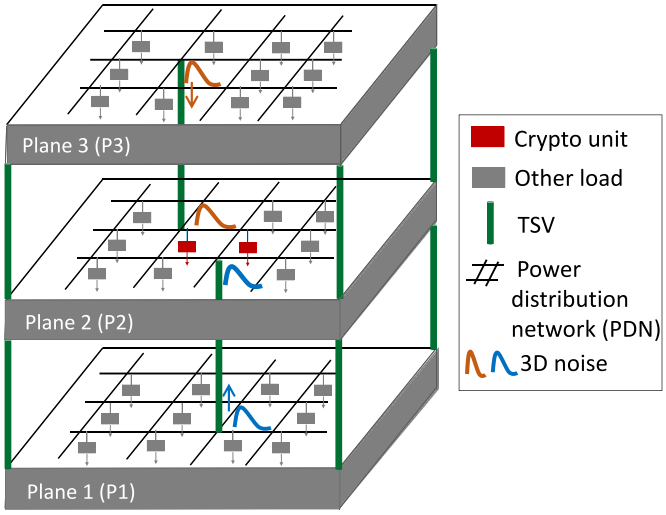


Fig. 1. An example of stack-based 3D chip architecture. TSV is used for inter-plane communication. 3D PDN noise is transferred to the crypto unit embedded in the middle plane of a 3D chip.

4) Besides the theoretical analysis on the feasibility of proposed method, we propose two practical implementations: application of spatially varied supply voltage (SVSV) and temporally varied supply voltage (TVSV), to obscure the power profile of the crypto module in 3D chips. As our implementations provide immutable noise on the supply voltage, they are low cost and also can thwart the countermeasure removal attack from adversary.
5) We perform FPGA validation of proposed method to analyze the key retrieval speed in CPA attack.

3. Preliminaries

A 3D IC integrates multiple planes into a single chip, in which through-silicon vias (TSVs) are commonly used for inter-plane communication. Fig. 1 depicts an example of a 3D chip. Being a critical component, a PDN delivers power supply to all the devices in 3D chip. We further zoom in the 3D PDN in Fig. 2 and show that the PDN in each plane consists of a global power network, virtual power network, and decoupling capacitors [22]. There are three types of PDNs available for PDN noise management: traditional, always-on, and reconfigurable PDNs. The traditional PDN utilizes decoupling capacitors in the virtual (local) power network. The always-on PDN employs decoupling capacitors in the global power grid. Note that it is usually not practical to directly connect decoupling capacitors to the global grid due to the long connection path, which increases the power supply noise in neighboring planes. Fortunately, the low impedance vertical TSV connection of 3D ICs facilitates the utilization of always-on decoupling capacitors on a plane to suppress the power supply noise in neighboring planes. The reconfigurable PDN switches between the traditional and always-on decoupling capacitors via reconfigurable switching transistors.

In our prior work [7], we set up experiments to investigate the impact of 3D PDN noise on the power profile of a crypto unit AES Sbox embedded in a 3D chip. The realistic PDN, TSV and circuit load models in Ref. [23] were used to generate the 3D noise. In plane 2, we placed an AES Sbox implemented at transistor level in the 45 nm technology node. As shown in Fig. 3, the noise from other 3D planes could alter the peak value of the dynamic power in a positive or negative way. We computed the *Pearson correlation coefficient* (PCC) [24] between the sampled and estimated power consumption. The estimated power consumption is calculated based on Hamming distance power model between two consecutive intermediate state register values.

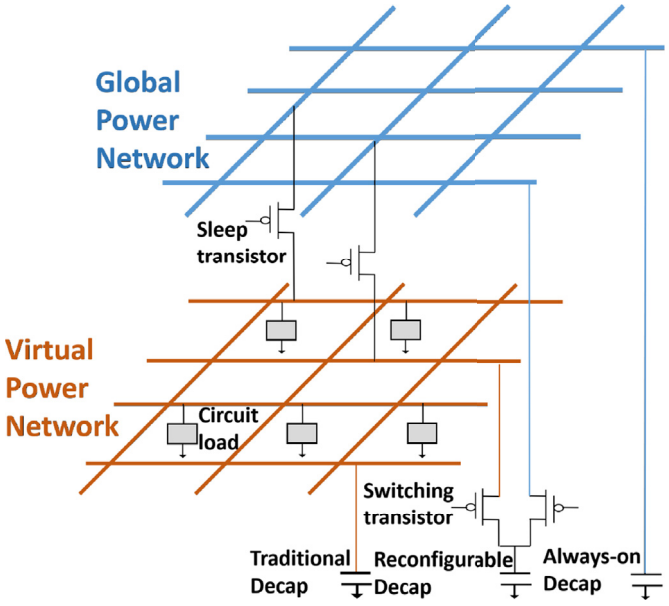


Fig. 2. Three kinds of decoupling capacitors in a panel-level PDN for traditional, always-on, and reconfigurable topologies, respectively.

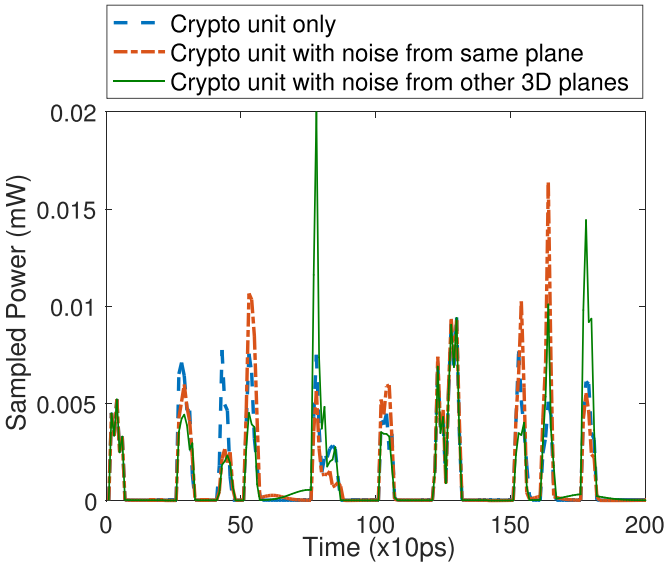


Fig. 3. Impact of 3D PDN noise on the power profile of a crypto unit in a 3D chip.

We use correlation coefficient and guessing entropy metrics for security assessment which are popularly used.

The first 3 bars in Fig. 4 show that the noise from PDN cannot be ignored because the PDN noise has noticeable impact on the PCC reduction. This reduction on PCC can be equivalent to an enhanced resilience against CPA attacks. The PCC comparison between different PDN topologies (represented by the fourth to sixth bars in Fig. 4) indicates that the type of PDN typologies could influence the power correlation, as well. This is because the 3D PDN noise is topology-dependent.

This work follows up our prior study and characterizes the PDN noise in the context of CPA attacks. Moreover, we exploit the characteristics of 3D PDN noise to improve the chip's CPA resilience over the natural defense from the 3D integration.

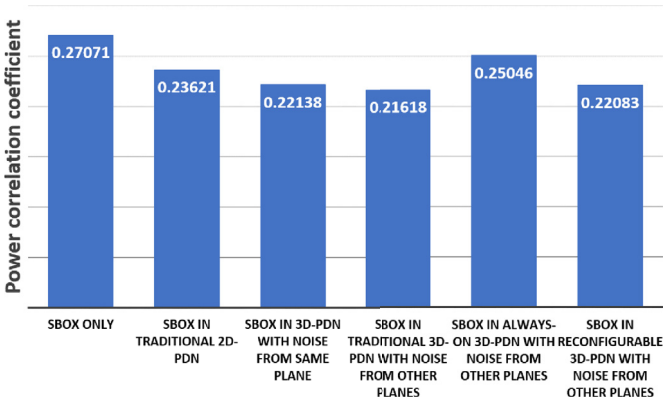


Fig. 4. Impact of PDN noise on Pearson correlation coefficient between measured and estimate crypto power.

4. Theoretical analysis on the impact of different noise characteristics on Pearson correlation coefficient

4.1. Definition of Pearson correlation coefficient

In statistics, PCC $r(X, Y)$ defined in Eq. (1) is used to indicate whether the two variables X and Y are correlated or not. The PCC has been adopted as an effective metric to examine whether a hypothesized crypto key is the real key applied in the crypto unit. In CPA attacks, a PCC value of 0 means no correlation between the measured side-channel signal X and the estimated side-channel signal Y. A larger absolute PCC value indicates a positive correlation between X and Y.

$$r(X,Y) = \frac{E[XY] - E[X]E[Y]}{\sqrt{E[X^2] - (E[X])^2} \cdot \sqrt{E[Y^2] - (E[Y])^2}} \tag{1}$$

4.2. Two types of noise

One type of common CPA countermeasures relies on various noise injection techniques that could hinder the extraction of the real power consumption of the crypto unit. The injected noise can be modeled with an additive or a multiplicative characteristic, expressed in Eq. (2) and Eq. (3), respectively.

$$X' = X + \delta \tag{2}$$

$$X' = X \cdot \delta \tag{3}$$

Here, X is the original power, X' is the power contaminated by noise, and δ is the noise with a mean of μ and a standard deviation of σ. To simplify the analysis, we assume that δ and X are independent. This assumption is applied to Sections 4.3 and 4.4, as well. In real life, examples of additive noise could be the thermal noise or voice noise [25], which are simply added onto the signal we desired. For multiplicative noise, an example could be the speckle noise, which is caused by the fluctuation of the original signal itself [26]. In ICs, additive noise could be provided by adding dummy circuits to consume extra power, including power grids in power delivery network, or using on-chip decoupling capacitors to store charge and discharge energy. For multiplicative noise, random dynamic voltage and frequency scaling may be utilized to insert multiplicative power noise into the cryptographic circuit [27].

4.3. Impact of additive noise on PCC

We substitute X in Eq. (1) with $X'(= X + \delta)$ and have the new PCC $r_A(X', Y)$ defined in Eq. (4).

$$r_A(X',Y) = \frac{E[(X+\delta)\cdot Y] - E[X+\delta]E[Y]}{\sqrt{E[(X+\delta)^2] - (E[X+\delta])^2} \cdot \sqrt{E[Y^2] - (E[Y])^2}} \tag{4}$$

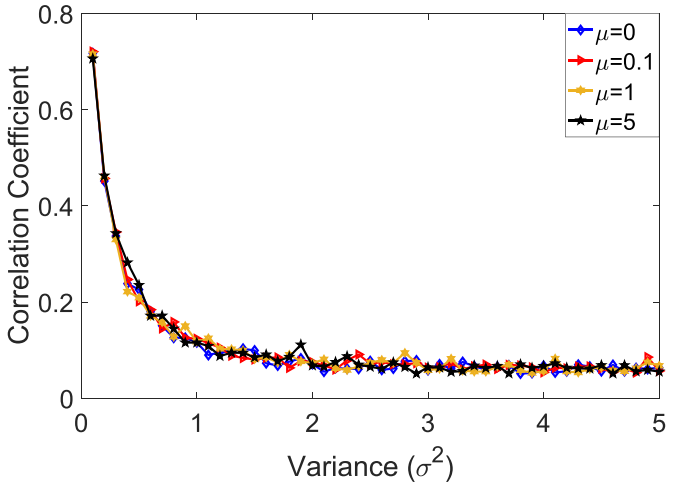


Fig. 5. Impact of parameters of additive noise on Pearson correlation coefficient.

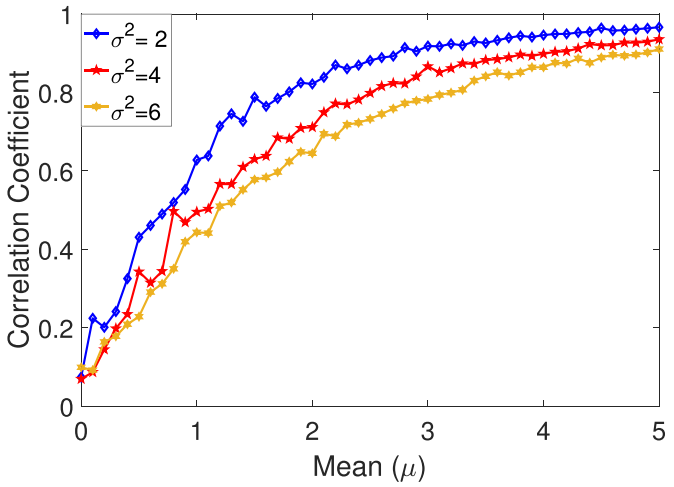


Fig. 6. Impact of the parameters of multiplicative noise on Pearson correlation coefficient.

After arranging Eq. (4), we further replace the term $(E[\delta^2] - (E[\delta])^2)$ with σ_δ^2 to obtain the simplified new PCC expressed in Eq. (5).

$$r_A(X', Y) = \frac{E[XY] - E[X]E[Y]}{\sqrt{E[X^2] - (E[X])^2 + \sigma_\delta^2} \cdot \sqrt{E[Y^2] - (E[Y])^2}} \tag{5}$$

From Eq. (5) we can see, after additive noise contaminates the original power profile of the crypto unit, the PCC will be affected by the noise variance. More specifically, the PCC decreases with the increasing σ_δ^2. The mean μ of the inserted noise does not have direct influence on the new PCC value.

To validate the analysis above, we added an additive white Gaussian noise to a set of power traces extracted from an Sbox implemented with a 45 nm technology. We varied the variance σ^2 and mean μ of the noise, and used MATLAB to compute the PCC between the original power (measured from Cadence Spectre simulation) and the power contaminated by the Gaussian noise. From the simulation results shown in Fig. 5 we can observe, the trend of correlation coefficient and variance σ^2 matches with the mathematical analysis in Eq. (5): as the noise variance increases, the correlation coefficient drops; while the change on the mean μ does not impact the correlation coefficient.

4.4. Impact of multiplicative noise on PCC

The $r_M(X', Y)$ defined in Eq. (6) is for the Pearson correlation coefficient between the original power and the power contaminated by multiplicative noise.

$$r_M(X', Y) = \frac{E[(X \cdot \delta) \cdot Y] - E[X \cdot \delta]E[Y]}{\sqrt{E[(X \cdot \delta)^2] - (E[X \cdot \delta])^2} \cdot \sqrt{E[Y^2] - (E[Y])^2}} \tag{6}$$

We simplify the $r_M(X', Y)$ above and obtain Eq. (7). This equation indicates that the PCC depends on the ratio of $\frac{\mu^2}{\sigma_\delta^2}$. $r_M(X', Y)$ increases with the increasing $\frac{\mu^2}{\sigma_\delta^2}$ ratio.

$$r_M(X', Y) = \frac{E[XY] - E[X]E[Y]}{\sqrt{E[X^2]\left(\frac{\sigma_\delta^2}{\mu^2} + 1\right) - (E[X])^2} \cdot \sqrt{E[Y^2] - (E[Y])^2}} \tag{7}$$

We followed the same procedure as we used in Section 4.3, except replacing the additive noise with a multiplicative one. The simulation results shown in Fig. 6 are consistent with the conclusion we draw from the theoretical analysis expressed in Eq. (7).

5. Experimental analysis on the impact of 3D PDN noise on CPA attacks

Correlation Power Analysis (CPA) is an attack that exploits the correlation between the power consumed by the hardware implementation of a cryptographic algorithm and the power estimated by using the Hamming weight or Hamming distance power model to retrieve the crypto key. In this section, we use realistic wire and TSV models [23] to simulate the 3D noise and examine the impact of 3D noise on the Sbox resilience against CPA attacks. Moreover, we characterize the 3D noise from our experiments.

5.1. Characteristics of 3D PDN noise

A PDN with different load circuits leads to different noise characteristics. Literature [28,29] extensively discuss the current and voltage modeling for PDN noise. In this work, we are interested in learning whether the 3D PDN results in additive or multiplicative noise to the power consumption of the crypto unit embedded in the 3D structure.

Our experiments illustrate that the switching or idle status of the load in other 3D planes has a noticeable impact on the power measurement of the crypto unit (Sbox) that is placed in middle plane. We simulated four scenarios for comparison:

- *P1OFF*: the crypto plane (plane 2) and the top plane (plane 3) are switching while the bottom plane (plane 1) is in an idle state,
- *P3OFF*: the crypto plane and bottom plane are switching but the top plane is inactive,
- *P1P3OFF*: only the crypto plane is switching,
- *ALLON*: all three planes are active.

Fig. 7 shows the power consumption for Sbox in the four scenarios discussed above. As can be seen, the Sbox power for the ALLON case is in general higher than other three scenarios; the P1OFF and P3OFF cases yield the same Sbox power profile. The mean and standard variation for each power profile are summarized in Table 1.

To examine the characteristic of 3D PDN noise in the context of CPA, we subtract (divide) the power consumption of the Sbox operated in a 2D chip from that of the Sbox in a 3D chip shown in Fig. 1. The intensive peaks shown in Fig. 8(a) indicate the significant difference on power that is caused by the 3D PDN noise. In contrast, the power ratio between the 3D and 2D scenarios does not vary frequently. As depicted in Fig. 8(b), there are few difference spikes in the range of 1000 sampling nodes. These observations apply to both P1P3OFF and ALLON cases.

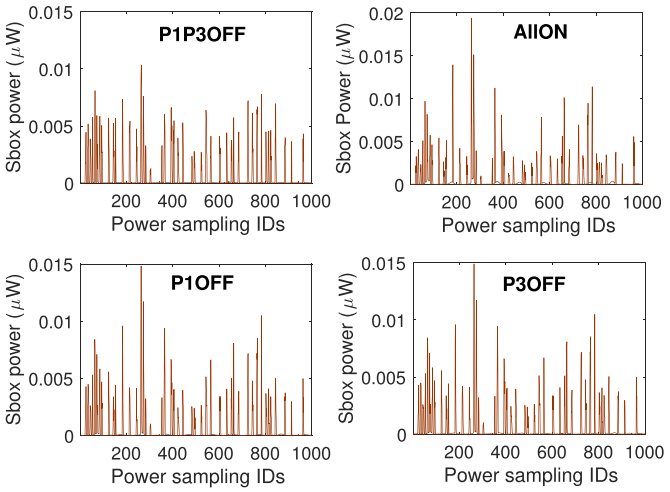


Fig. 7. The power profile of an Sbox affected by different noise from the 3D chip.

Next, we follow the PCC definition in Eq. (1) to calculate the PCC between the measured Sbox power in four 3D scenarios and in a 2D PDN. As shown in Fig. 9(a), the P1P3OFF case leads to the highest PCC among the four cases under comparison. This is reasonable because idle planes 1 and 3 only pass leakage noise to plane 2. In contrast, the PCC for ALLON case is the lowest among all cases since both the top and bottom planes transfer PDN noise to the Sbox plane. We also compare the PCC in Eq. (8).

$$r_{P1P3OFF} > r_{P1OFF}(= r_{P3OFF}) > r_{ALLON} \tag{8}$$

The variance on the Sbox power for the four scenarios is depicted in Fig. 9(b). As can be seen, the relative relationship between four variances is as expressed in Eq. (9).

$$\sigma^2_{P1P3OFF} < \sigma^2_{P3OFF}(= \sigma^2_{P1OFF}) < \sigma^2_{ALLON} \tag{9}$$

This trend satisfies the relationship between variance and PCC expressed in Eq. (5), i.e., the increasing variance leads to a decreasing PCC.

The ratio of $\frac{\mu^2}{\sigma^2_\delta}$ for the power profiles obtained from the four scenarios is compared in Fig. 9(c) and Eq. (10).

$$\mu^2/\sigma^2_{P1P3OFF} > \mu^2/\sigma^2_{ALLON} > \mu^2/\sigma^2_{P3OFF}(= \mu^2/\sigma^2_{P1OFF}) \tag{10}$$

As shown, the ratio for the P3OFF case is the lowest one but its PCC value is not the highest. In other words, Eq. (8) and Eq. (10) are not indicating the same noise characteristic. Hence, we conclude that the 3D PDN noise is additive, and not multiplicative, in the context of 3D CPA attacks.

5.2. Comparison of CPA efficiency in 2D and 3D ICs

The 3D PDNs induce more noise to the crypto unit embedded in a 3D IC than in a 2D chip because of the co-existed intra- and inter-plane

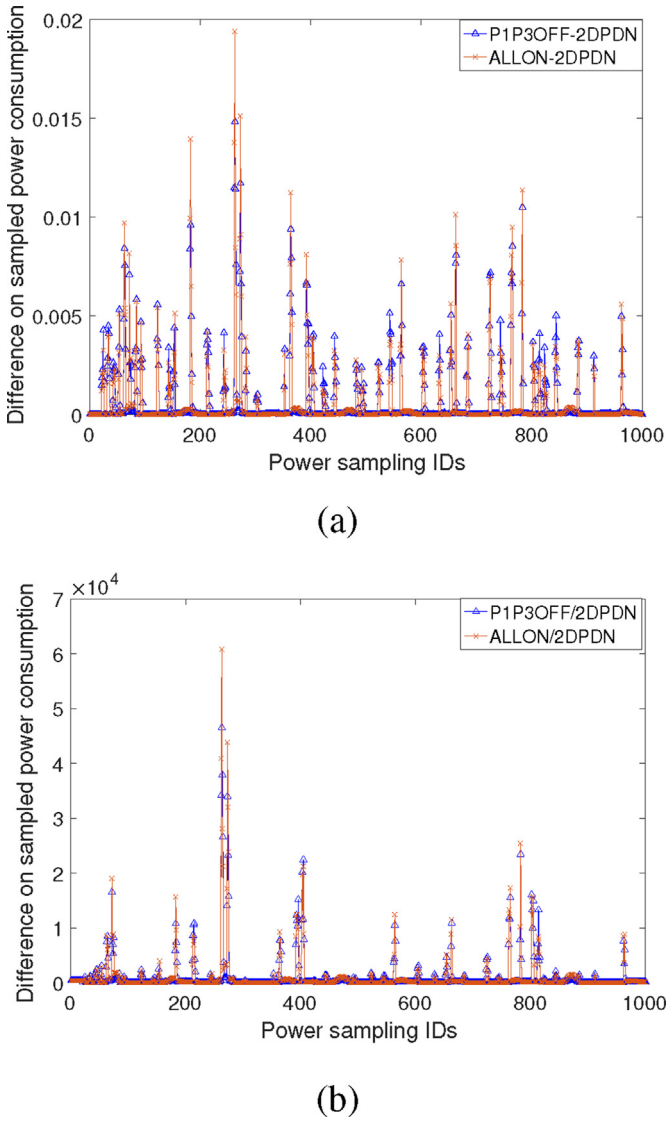


Fig. 8. Comparison of Sbox power in a 3D PDN versus in a 2D PDN. (a) Power difference and (b) power ratio.

PDN noise. In this section, we examine the impact of PDN noise on the crypto key retrieval speed. A CPA attack was applied to the gate-level Sbox implemented in a 2D PDN. We adopt *guessing entropy* [3,30] as a metric to evaluate the key retrieval speed. The metric guessing entropy quantifies the average number of guesses that are required to identify the correct value of a key byte. As shown in Fig. 10, for the Sbox in a 2D chip, 900 power traces are sufficient to retrieve the key (i.e., the guessing entropy goes to zero). In contrast, the guessing entropy for the 3D case does not reach zero until 1500 power traces are used in the CPA attack. From this comparison we conclude, more power traces will be

Table 1
Mean and standard deviation of the power profile for the Sbox in different 3D switching scenarios.

Noise Assessment		P1OFF	P3OFF	P1P3OFF	ALLON
Additive	Mean	7.01e-04	7.02e-04	6.96e-04	7.36e-04
	Std	1.70e-03	1.70e-03	1.59e-03	1.85e-03
Multiplicative	Mean	9.81e+02	9.82e+02	9.11e+02	1.11e+03
	Std	3.59e+03	3.59e+03	3.21e+03	4.00e+03

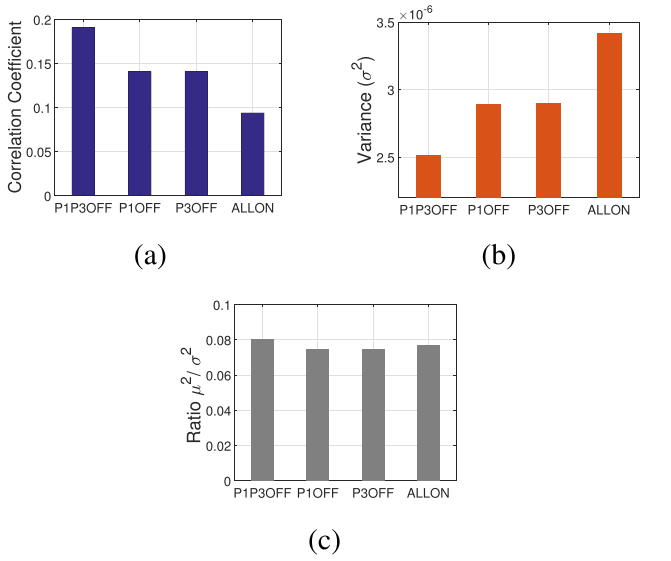


Fig. 9. Impact of 3D PDN noises on Sbox power profile. (a) Correlation coefficient, (b) variance, and (c) ratio of $\frac{\mu^2}{\sigma_\delta^2}$ for the Sbox in four 3D scenarios.

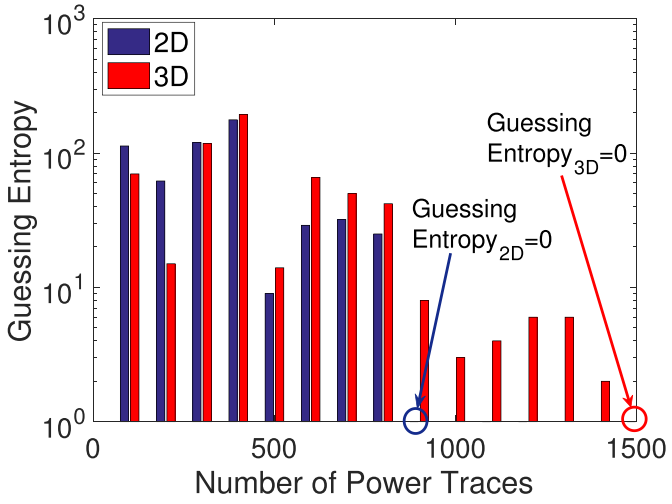


Fig. 10. Guessing entropy for CPA attacks in 2D and 3D (P1P3OFF) ICs.

needed for a CPA attack to recover the secret key from a 3D chip than from a 2D one. Note that the 3D scenario for Fig. 10 is P1P3OFF and other planes (P1 and P3) only pass leakage power to the Sbox plane.

Further, we increase the PDN noise by turning on planes 1 and 3 to examine the key retrieval speed of CPA attacks in 3D ICs. As shown in Fig. 11, the guessing entropy of the ALLON case generally remains as the highest one, compared to the P1P3OFF and P3OFF cases.

6. Proposed 3D PDN noise-based countermeasure against CPA attacks

Inspired by the observation in Sections 4 and 5, we propose a new countermeasure that exploits the intrinsic PDN noise from other 3D planes to introduce additive noise to the power of a crypto module in the 3D chip. In the following subsections, we introduce the theoretical foundation and hardware implementation of our proposed PDN noise-based countermeasure. The concept of our method is shown in Fig. 12. The noise from other planes is transferred through power TSVs to drive the crypto unit such that the supply voltage for the crypto unit is not a constant and predictable value. The unpredictability on voltage is

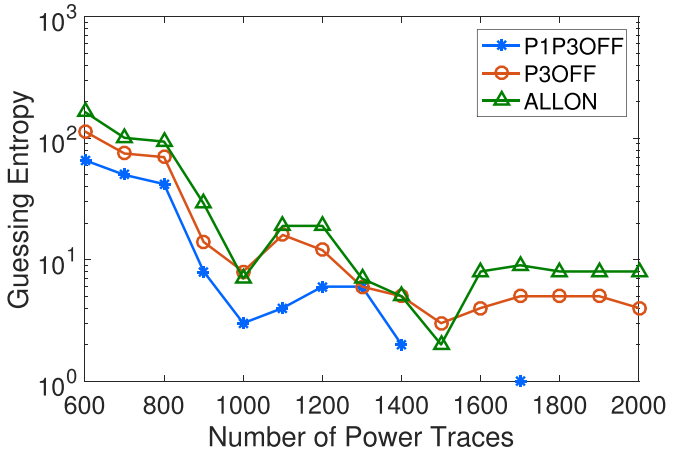


Fig. 11. Impact of different switching activities of 3D planes on guessing entropy.

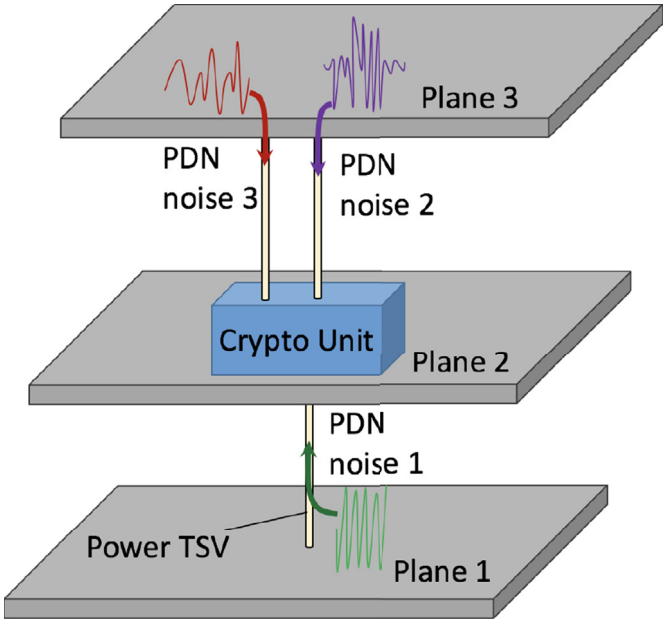


Fig. 12. Concept of proposed PDN noise based countermeasure against CPA attacks.

induced by the unplanned activities in other planes.

6.1. Theoretical foundation of proposed method

As we know, the traditional power consumption is modeled with Eq. (11).

$$P_{orig} = \alpha f C_L V_{DD}^2 \tag{11}$$

Where α, f, C_L, and V_{DD} are switching activity factor, system clock frequency, load capacitance, and supply voltage, respectively. To alter the original power P_{orig}, we can change the circuit switching activities, alter the clock frequency dynamically, replace a fixed load with a changeable one, or use an adaptive supply voltage. As the supply voltage is the dominant factor in the power consumption, we propose to obscure the power of a crypto unit by manipulating the supply voltage. As increasing σ_δ in the additive noise model will help to reduce PCC, we exploit the additive noise available on chip to develop countermeasures against

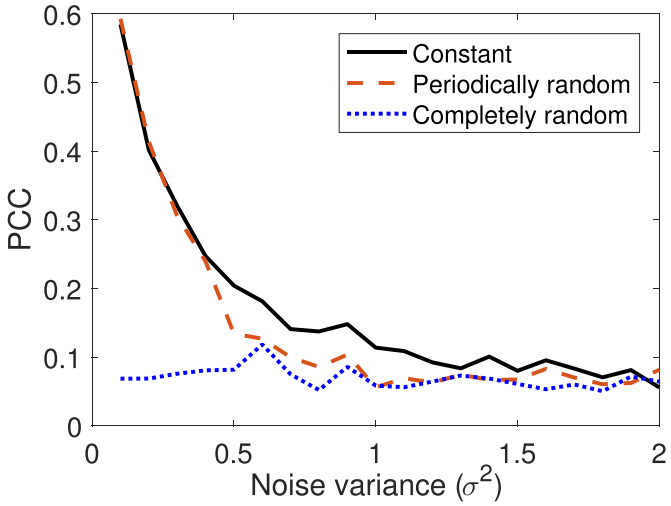


Fig. 13. Impact of the combination of multiple additive noises on correlation coefficient.

CPA attacks in 3D ICs.

1) *Exploiting Spatial Variation on Supply Voltage as Power Noise Source:* We propose to utilize m voltages from m power TSVs to drive the crypto unit. Each voltage drives a portion of the crypto unit. Now, the new power consumption P_{new} is revised in Eq. (12). α_i, C_{Li}, and V_{DDi} stand for the switching activity factor, load capacitance, and supply voltage of each portion of the crypto unit. We assume the range of voltage variation is relatively small (<20% of the nominal V_{DD}). Thus, the second-order term of ΔV_i^2 can be ignored in Eq. (12).

$$\begin{aligned} P_{new} &= \sum_{i=1}^{m} \left(\alpha_i f C_{Li} V_{DDi}^2 \right) \\ &= \sum_{i=1}^{m} \alpha_i f C_{Li} \left(V_{DD} + \Delta V_i \right)^2 \\ &\approx P_{orig} + \sum_{i=1}^{m} \left(2\alpha_i f C_{Li} V_{DD} \cdot \Delta V_i \right) \end{aligned} \tag{12}$$

In addition to the original power, the second term in Eq. (12) is the additive power portion contributed by the use of multiple V_{DD}s. Thus, the proposed spatially dynamic voltage approach indeed can bring an additive noise to the original power. More number of different voltages and the additional independence between those V_{DD}s will facilitate power correlation reduction between the physically measured power and the estimated power. This is because the theoretically estimated power does not consider the impact of driving voltage.

2) *Exploiting Temporal Variation on Supply Voltage as Power Noise Source:* Alternatively, the supply voltage can be varied temporally. This means, we change the supply voltage along with the time. Hence, the revised power consumption is expressed in Eq. (13).

$$\begin{aligned} P_{new} &= \frac{\sum_{i=1}^{N} \left(\alpha f C_L V_{DDi}^2 \right)}{N} \\ &= \frac{\sum_{i=1}^{N} \alpha f C_L \left(V_{DD} + \Delta V_i \right)^2}{N} \\ &\approx P_{orig} + 2\alpha f C_L \cdot \frac{\sum_{i=1}^{N} \left(V_{DD} \cdot \Delta V_i \right)}{N} \end{aligned} \tag{13}$$

In Eq. (13), N is the number of different supply voltages changed during the time period of interest. We can alter the supply voltage V_{DDi} in a completely or periodically random fashion. The latter one requires less number of diverse V_{DDi}s, but it is less effective than the former method in regard to the resilience against CPA attacks. Fig. 13 shows the application of periodically random noise that helps to reduce the correlation coefficient over the constant nominal supply voltage. The application of completely random noise leads to an approximately flat PCC even though the variance of multiple noises is in a wide range.

6.2. Implementation of proposed method

1) *Application of Spatially Varied Supply Voltages (SVSV):* As mentioned before, due to the large scale of integration, 3D chips inherently have more noise sources than 2D ICs. In this work, we first propose to utilize the supply voltages from multiple TSVs to drive the crypto unit. Fig. 14(a) depicts the proposed implementation method, which applies spatially varied supply voltages to resist CPA attacks. We divide the crypto unit into multiple sub-units (for instance, four). Each sub-unit is driven by a local supply voltage $V_{DDi}(i = 1, 2, 3, 4)$. A crossbar is used to connect the local V_{DD} pins with the PDN nodes close to four power TSVs. Due to the non-uniform switching activities in individual 3D planes, each TSV passes a unique voltage from other planes to the plane carrying a crypto unit. The effect of parasitic resistance and capacitance (RC) of the metal wire between the power grid and the local V_{DD} pin further increases the variance of four V_{DD}s driving the crypto unit (i.e. Sbox in AES).

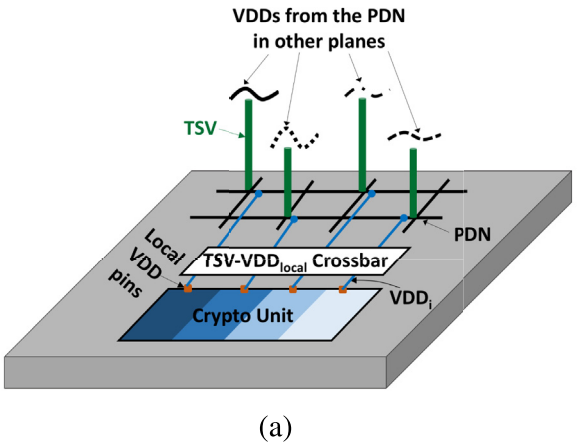
Fig. 14(b) shows the voltage of four power TSVs. As can be seen, both the magnitude and occurrence timing for the peak voltage of the four V_{DD}s are not exactly same. The variance of these four V_{DD}s over the baseline (a single supply voltage) are noticeable as shown in Fig. 14(c). We can exploit the variance on local V_{DD}s to blur the correlation between the measured and hypothetical power profile of the crypto module. The crossbar can be a direct in-out mapping or dynamically rotated. The crypto unit was driven by the four voltages transferred from four power TSVs shown in Fig. 14(b). We compared the power profiles of the baseline and proposed method in Fig. 15. As shown, the instant sampled power for two cases are dramatically different. In Section 7.2, we illustrate the impact of our method on the CPA attack resilience.

2) *Application of Temporally Varied Supply Voltages (TVSV):* Alternatively, we can multiplex multiple voltage sources to power up the *entire* crypto unit, rather than multiple sub-units. As shown in Fig. 16, the four V_{DD}s from nearby planes are fed to a multiplexer *MUX*. At each period of time, only one of these V_{DD}s will be selected to drive the crypto unit. A dynamic rotator is used to control the multiplexer. To achieve dynamic rotation in hardware, we can use a pseudorandom number generator (PRNG) to dynamically select induced VDDs to drive the crypto unit. The role of multiplexer is to assign varied supply voltages to the crypto unit at different time slots in a complete process of running the cryptographic algorithm. Fig. 17 demonstrates the AES power consumption at three time periods. The values of sampling power are distinguished from each other. This indicates the power traces captured through CPA attacks are altered by the voltage noise. Modification on the power consumption will impact the CPA efficiency.

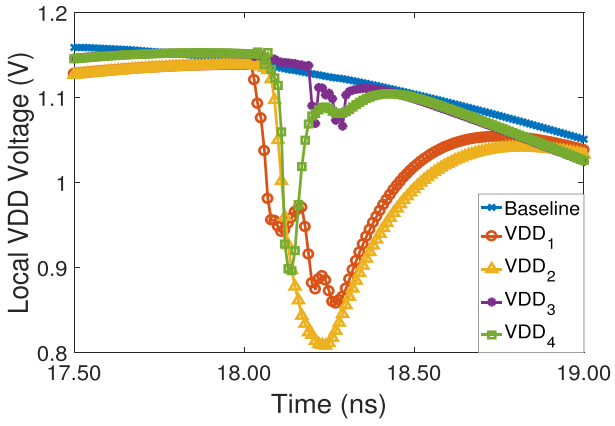
7. Experimental results

7.1. Experimental setup

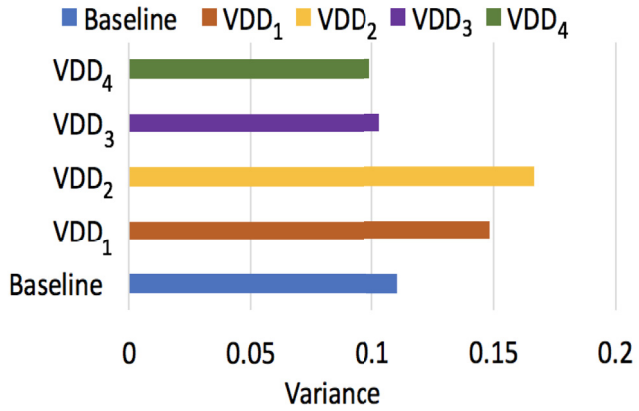
We evaluated the proposed method by using transistor-level simulation and FPGA emulation. For the transistor-level simulation, we implemented a stacked 3D IC with three planes in a 45 nm NCSU FreePDK technology [23]. In each plane, a PDN is composed of a global power grid and multiple virtual grids. The latter one provides a power supply for local load circuits in each plane. To save power consumption, sleep transistors are used to connect virtual grids and global grids. Global power grids are connected through TSVs to the other planes. The detailed parameters for TSVs and local metal wires are listed in Table 2. The crypto module in our experiment is an AES Sbox implemented at transistor level. The Sbox power consumption was measured in Cadence Virtuoso. Hamming distance power model [2] was adopted



(a)



(b)



(c)

Fig. 14. Proposed countermeasure applying multiple voltage sources to the multiple sub-units of the crypto unit. (a) Architecture, (b) waveform of different supply voltages, and (c) variance on V_{DD} [8].

to calculate the hypothesized power for the Sbox.

For FPGA emulation, we used a SAKURA-G FPGA board. That board contains two Spartan-6 FPGAs: one (LX75 FPGA) for a cryptographic implementation and the other (LX9 FPGA) for power traces capturing. The bitstream associated with the Verilog-HDL code for AES-128 was downloaded to the SAKURA-G board. A Python-based ChipWhisperer [2] software was used to perform power trace capturing and analysis. The other setup for the CPA attacks can be found in our prior work [3].

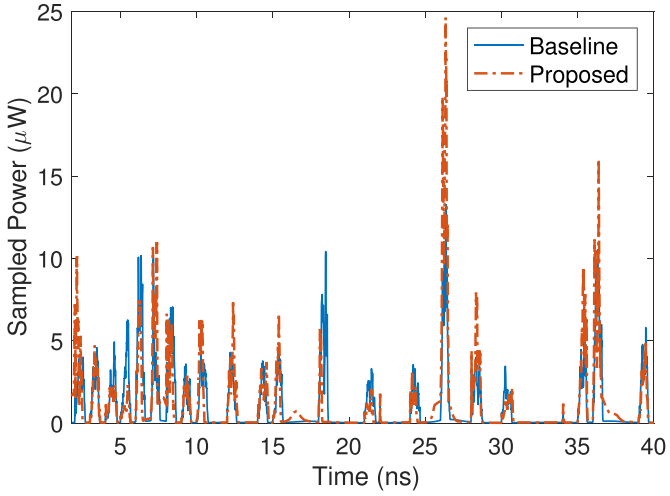


Fig. 15. Sbox power profiles for a single and four V_{DD}s driving cases.

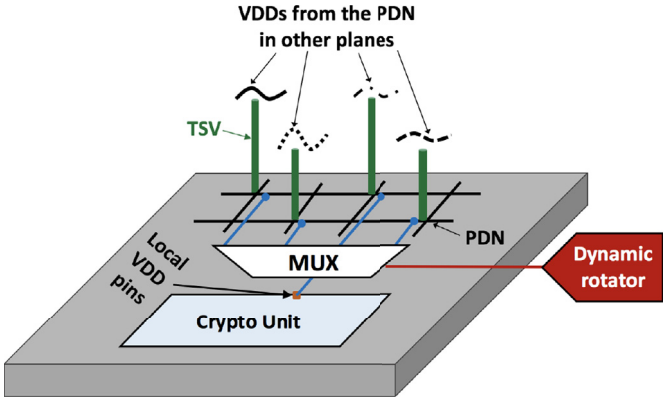


Fig. 16. Proposed countermeasure multiplexing multiple voltage sources for the entire crypto unit.

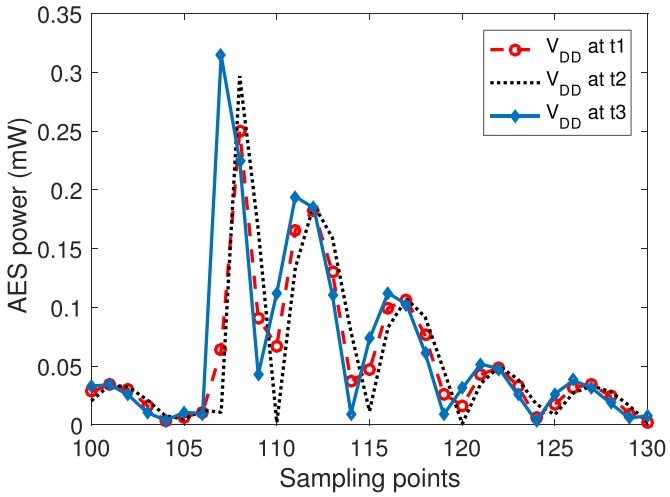
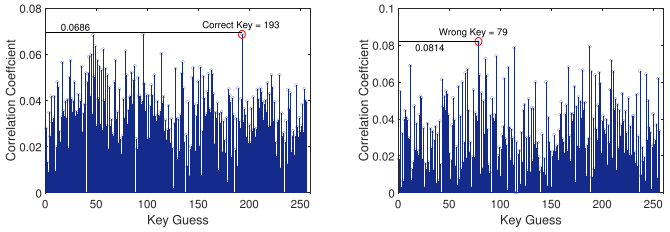


Fig. 17. AES power profiles measured at three different operation periods.

1. **2D**: The crypto unit is embedded in a 2D PDN. No other loads are connected in the PDN.
2. **3D baseline** [7]: The crypto module is placed in the middle plane of a 3D chip, in which the always-on PDN topology is employed to

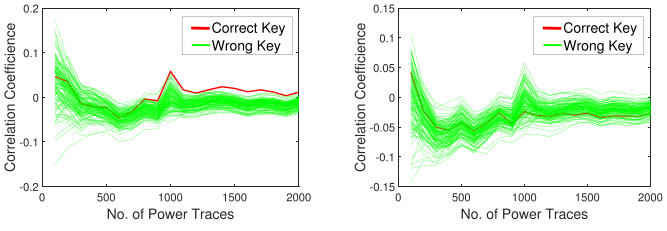
Table 2
Parameters for TSV and wire model.

TSV Model (per TSV) [23]					
Diameter	Height	Pitch	Resistance	Inductance	Capacitance
10 μm	60 μm	20 μm	20 mΩ	34.94 pH	283 fF
RC Model for Local Wire Interconnect (per mm) [31]					
Resistance			Capacitance		
3.31 kΩ			170.59 fF		



(a) (b)

Fig. 18. Correlation coefficient for all possible keys in the case of (a) 3D baseline and (b) proposed application of spatially varied supply voltages (SVSV). The highest correlation coefficient in (a) is achieved at the correct key. In contrast, the highest correlation coefficient in (b) is obtained at a wrong key; thus the proposed method thwarts a CPA attack.



(a) (b)

Fig. 19. Correlation coefficient for 3D (a) baseline and (b) proposed method.

provide supply voltages for each 3D plane.

3. **Proposed SVSV**: Similar with the 3D baseline, the crypto unit is located in the middle plane of a 3D chip; however, the crypto unit is divided into four submodules, each of which is driven by the supply voltage from a unique power TSV. The PDN topology is always-on type. In our simulation (in Cadence), four current sources [28] are added in the top plane to mimic four load circuits, which affect the voltage levels of four spatially distributed TSVs.The four current pulses are in the range of 100 %400 mA.
4. **Proposed TVSV**: The crypto module remains as a whole to be driven alternatively by one of the four supply voltages originated from four power TSVs.

7.2. Improved Resilience against CPA attacks

1) *Transistor-level Simulation:* The transistor-level implementations of the baseline and proposed SVSV Sboxes were simulated in Cadence Virtuoso. We generated 2000 power traces for each simulation and then performed a CPA attack on each case. As shown in Fig. 18(a), the CPA attack is able to retrieve the correct key (193) in the 3D baseline case. In contrast, our proposed SVSV method successfully thwarts the CPA attack given 2000 power traces because the retrieved key (79) is a wrong one.

The key retrieval speed of CPA attacks is depicted in Fig. 19. Once the correlation coefficient for the correct key stands out from the wrong keys, we consider the CPA attack succeeds and the corresponding number of power traces is what we need to collect from simulation. As shown in Fig. 19(a), in the 3D baseline case, the correlation coefficient for the correct key is steadily higher than the wrong keys after 1000 power traces. However, our proposed SVSV prevents the success of the CPA attack for the given 2000 power traces. As shown in Fig. 19(b), the correlation coefficient for the correct key is lower than many wrong keys.

Based on the 2000 power traces, we averaged the correlation coefficients for all the wrong keys and compared it with the correlation coefficient for the correct key in Fig. 20. As shown, our method enlarges the difference between the correlation coefficients over 2D and 3D baseline, respectively. A larger difference indicates more difficult for CPA attacks to retrieve the correct key for the same number of the power traces. We repeated the power trace collections and CPA attacks three times. Proposed method improves the CPA attack resilience by 29.1% and 18.7% over 2D and 3D baseline.

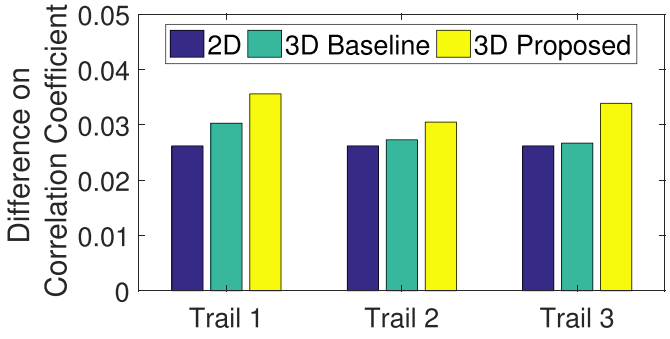


Fig. 20. Average difference on correlation coefficients for correct and wrong keys.

Guessing entropy is another evaluation metric that describes how many guesses the CPA attack will take to find the correct key. As shown in Fig. 21, when the guessing entropy of the baseline approaches to zero, our method's remains high even after 2000 power traces. The guessing entropy for both methods (baseline and proposed) at the point of 1000 power traces are reported in Table 3 for three trials. The average guessing entropy of our method is 9× that of the 3D baseline and is 99 higher than 2D.

2) *FPGA Emulation:* Transistor-level simulation is relatively slow and does not include the noise from the power measurement equipment and external environment. Hence, we only examined the 8-bit key retrieval for a single Sbox in transistor-level simulation. In this subsection, we evaluate our method on the SAKURA-G FPGA platform. The Verilog-HDL implementation for AES-128 was configured on the FPGA. For AES-128, there are 16 key bytes in total. The main FPGA Spartan-6 XC6SLX75 is powered by a supply voltage from the *VCCINT* pin. As

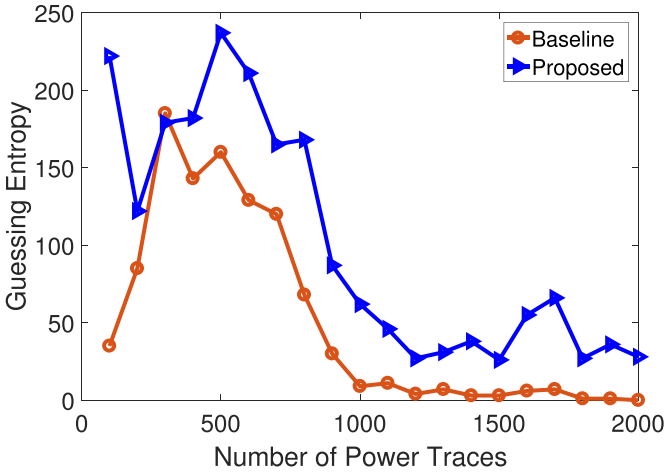


Fig. 21. Improved guessing entropy by proposed method.

Table 3
Guessing entropy for different trials.

Design	Trail 1	Trail 2	Trail 3	Average
2D	0	0	0	0
3D Baseline	16	11	6	11
3D Proposed	77	46	175	99

the FPGA does not support multiple supply voltages, we adjusted the value of VCCINT through a trimmer *VR*1 to generate different supply voltages for the proposed TVSV implementation. The supply voltage for AES was monitored by a multimeter through the on-board pin *J*1. We first collected a set of AES power traces for each supply voltage at separate intervals and then combined the multiple sets of the collected power traces in the ChipWhisperer Capture and Analyzer tool during the process of CPA attack. In our emulation, we selected four voltage levels: 1.1 V, 1.15 V, 1.2 V and 1.25 V (the standard value of VCCINT is 1.2 V).

Key retrieval speed: The ChipWhisperer Analyzer retrieves the correct key for the AES-128 by validating the crypto key byte by byte. Given a fixed number of power traces, the less number of retrieved key bytes means a better resilience achieved by the countermeasure against CPA attacks. At each voltage level, we generated eight ChipWhisperer projects, each including 250 power traces. Then, we combined all power traces for different supply voltages and different ChipWhisperer projects to form a complete power profile set for the CPA attack on AES-128. As shown in Fig. 22, the proposed countermeasure effectively thwarts the CPA attack. For the given 8000 power traces, the CPA attack is not able to retrieve all 16 key bytes for the AES-128 protected with proposed method. In contrast, the baseline leaks the crypto key with a more rapid speed than our method. On average, our method leaks 4.25 less key bytes than the baseline. Note, the AES-128 only has 16 key bytes and hence 4.25 is a large portion of the total crypto key vector. The CPA attack on the baseline was based on the 8000 power traces collected from the AES-128 operating at the supply voltage of 1.2 V.

The power traces for the experiment in Fig. 22 are *evenly* contributed by four different supply voltages. We further examined whether other combinations of the power traces collected from different supply voltage scenarios will lead to a different key retrieval speed. In addition to the baseline (all traces with 1.2 V), we assembled the power traces with the percentage shown in Fig. 23(a). For instance, in the configuration 1 (i.e., Config. 1 for TVSV), the dominant power traces are contributed by the case running the supply voltage of 1.25 V. As shown in Fig. 23(b), no matter which configuration is used, our countermeasure reveals less

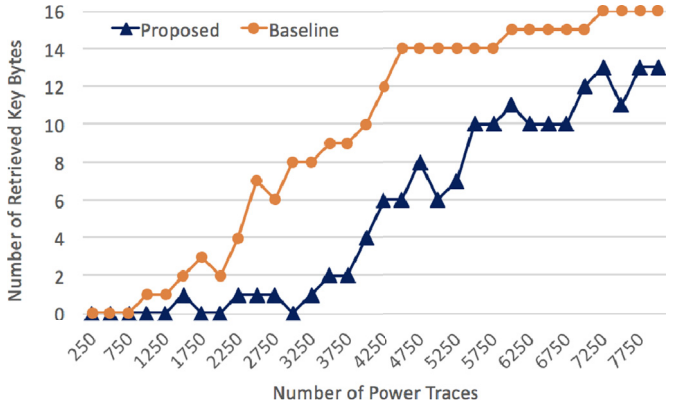


Fig. 22. Reduction on the number of retrieved key bytes achieved by the proposed method.

number of key bytes than the baseline. In addition, none of our configurations allows the CPA attacks to retrieve all 16 key bytes within 8000 power traces. This further confirms the proposed countermeasure indeed impacts the key retrieval efficiency of CPA attacks.

Partial guessing entropy: To find out the reason behind the observation in Fig. 23(b), we studied the partial guessing entropy (PGE) for each key byte. A smaller PGE means less number of guessing is needed to identify the correct key byte. The accumulated PGE (APGE) represents the total number of guesses that may take to retrieve the entire crypto key. We examined the impact of different supply voltages on APGE. Fig. 24(a) and (b) show the APGEs for 16 AES key bytes based on the analysis of 4000 and 5000 power traces, respectively. After comparing these two cases, we conclude that the general trend of APGE for each supply voltage decreases when more power traces are analyzed. However, there is no obvious clue that indicates which voltage offers a better resilience against CPA attacks. That explains why it is not clear which configurations used in the experiment for Fig. 23(b) is the best in terms of resilience against CPA attacks.

Test vector leakage assessment: Leakage detection is important to validate the physical security of cryptographic devices. Test vector leakage assessment (TVLA) [32] approach is one of the popular techniques to detect the leakage. In this method, a set of preselected test vectors is selected and then statistical tests are performed on collected power measurement. The test results into a confidence score using which a fail/pass decision can be made for the crypto under test.

We conducted the TVLA on the basic and proposed TVSV secured AES. Our goal is to evaluate to what extent the data-dependency of the AES power traces can be mitigated by our method. Each power trace collected by ChipWhisperer Capture consists of 396 time instants, representing 396 sampling points. Based on all the 8000 power traces, collected for the results shown in Fig. 22, we calculated the TVLA value for each time instant and plotted in Fig. 25. R1 to R10 represents the AES first to 10th round. As shown in Fig. 25, the TVLA absolute values for TVSV secured AES are generally lower than those for the baseline AES for 10 AES rounds (roughly from 80 to 320). A smaller TVLA absolute value means higher confidence to accept the null hypothesis [33]. We evaluate this confidence level with a probability Pr_{con} as expressed in Eq. (14).

$$Pr_{con} = 2\int_{TVLA_{lr}}^{\infty} pdf(t,v)dt \tag{14}$$

In which, $pdf(t,v)$ is the probability density function of the Student's t distribution with the degrees of freedom of v. t is the t-test statistic and we simply use 16,000 (8000 traces + 8000 traces) for v.

Because the previous results shown in Fig. 22 are obtained from the AES last round attack performed in ChipWhisperer Analyzer, we zoom in the TVLA values for the time instants observed in the AES last round.

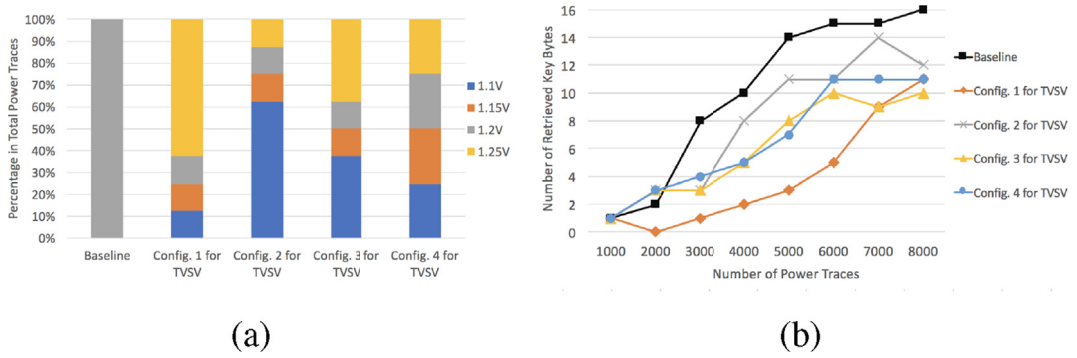


Fig. 23. Comparison of CPA key retrieval speed. (a) Power trace configuration and (b) Number of retrieved key bytes for different number of power traces.

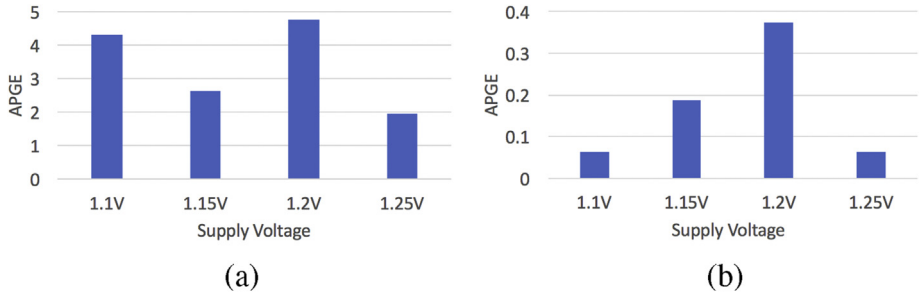


Fig. 24. APGE obtained in CPA attacks based on (a) 4000 and (b) 5000 power traces.

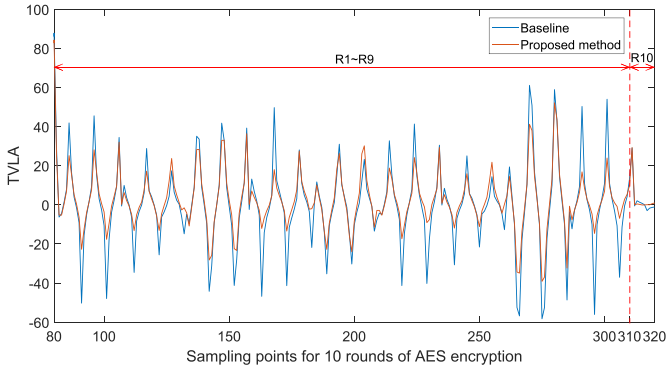


Fig. 25. TVLA comparison between basic and our secured AES.

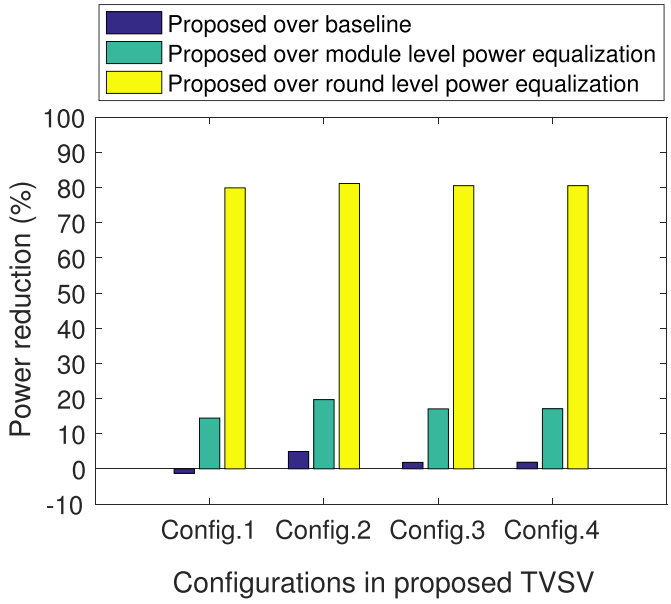


Fig. 26. Power reduction comparison.

Table 4
$TVLA_{lr}$ and Pr_{Con} for basic and our secured AES.

AES versions	Result categories	
	$TVLA_{lr}$	Pr_{Con}
Baseline	4.9477	7.58×10^{-7} (100%)
Proposed method	3.7894	1.52×10^{-4} (201%)

Those TVLA absolute values (roughly from 310 to 320) were averaged and saved in $TVLA_{lr}$. The corresponding Pr_{con} was also adopted to quantify the mitigation ability against CPA attack. The values of $TVLA_{lr}$ and Pr_{con} are listed in Table 4. The $TVLA_{lr}$ for basic AES is 4.9477, which is greater than 4.5. Note, 4.5 is defined as a threshold to determine whether the traces carry sensitive information [34]. The $TVLA_{lr}$ of our proposed method is below the threshold of 4.5. This result indicates that our approach is less data dependent and leaks less sensitive information (i.e., key) than the baseline. Our method also improves Pr_{con} over 201× over the baseline.

7.3. Overhead on power

The entire AES was implemented in the SAKURA-G FPGA board and the ChipWhisperer tool captured 8000 power traces for each supply voltage (i.e., 1.1 V, 1.15 V, 1.2 V, and 1.25 V), respectively. The average power consumption for each power trace was calculated in MATLAB. The baseline power is the one using 1.2 V. The proposed method evaluated here is the implementation of TVSV. Four configurations shown in Fig. 23(a) were adopted. We analyzed the power traces and balanced the power trace at the module level and round level. Module level power balancing is achievable by using differential CMOS logic

Table 5
Comparison of power overhead.

Methods	QuadSeal [36]	SABL [35]	Current Equalizer [12]	Proposed
Power overhead	+4.0×	+1.9×	+33%	−81.1% %+1.25%

Table 6
Delay comparison.

Delay	3D IC: P3OFF or P1OFF		
	Baseline	Proposed w/o RC	Proposed w/RC
Average (ns)	0.2505	0.2780	0.3390
Normalized	100%	110.98%	135.33%
Delay	3D IC: ALLON		
	Baseline	Proposed w/o RC	Proposed w/RC
Average (ns)	0.2510	0.2808	0.3488
Normalized	100%	111.87%	139.00%

(such as the method in Ref. [35]), which makes each module consume the same power regardless of which input pattern is applied. We used the AES round consuming the highest power to replace the power profile for the remaining AES rounds, and calculated the average power for the module level power balancing. Round level power balancing can be realized by the current equalizer (such as the method in Ref. [12]). We assume the current equalizer technique compensates the fluctuation on the AES current throughout the entire AES round operation such that the AES power remains as high as the highest dynamic power observed in different AES rounds. We compared the proposed method with the baseline, module level and round level power balancing approaches and show the power reduction achieved by our method in Fig. 26. As our method does not introduce additional noise to flatten the power, our method can significantly reduce the power over the power balancing techniques. Depending on the TVSV configuration pattern, the power reduction achieved by our method is in the range of 14.4%–19.7% at the module level, and in the range of 79.9% and 81.1% at the round level. Since the TSV noise could lead the supply voltage exceed the nominal voltage, our method consumes more power by 1.3% than the baseline in the scenario of configuration 1 (that is why power reduction is negative). For other three configurations, our method reduces the power by 1.8% %4.9%.

As different detailed settings are used in different approaches [12,35,36], we could not repeat the exact same experiment in our FPGA platform. We cited their reported power overhead and compared those numbers with ours in Table 5. As shown, the algorithmic approach [36] leads to 4.0× overhead on power, SABL consumes 1.9× power on AES, and the switched capacitor current equalizer brings in 33% more power consumption. Instead of relying on artificially induced noise, our method exploits the inherently existing noise to reduce the power correlation. Thus, we can effectively reduce the power consumption of the crypto module. Our case study shows that the proposed method leads to a power overhead no more than 1.25% over the baseline.

7.4. Overhead on delay

The use of multiple V_{DD}s in the proposed SVSV method may lead to increased delay on the crypto module, depending on which V_{DD}s are selected. We randomly chose four in-out pairs to compare the delay measured in Cadence Virtuoso As shown in Table 6, the increased delay depends on the lumped RC model for wires and the on/off status of other 3D planes. Without considering the RC delay from the local power grid to the crypto module's V_{DD} pin, our method incurs 10.98% more delay than the 3D baseline with P3OFF(P1OFF). If RC delay is included, our delay overhead increases to 35.33%. When all the 3D planes are switching simultaneously, more noise passes to the Sbox plane that results in more delay overhead compared to P3OFF (P1OFF) case.

8. Conclusion

3D integration has emerged as a new technology to further increase the chip density. Although stacking multiple planes in 3D ICs seems promising to prevent precise extraction of side-channel signals, the impact of 3D intrinsic noise on CPA attacks has not been widely investigated yet. In this work, we adopt realistic models for 3D PDNs and TSVs and perform quantitative studies on the efficiency of CPA attacks in 3D ICs. Our theoretical analysis and experimental results confirm that the 3D PDN noise transferred from other planes is additive in the context of power correlation coefficient in CPA attacks. We exploit the unique 3D intrinsic noise to develop a novel PDN noise based countermeasure to thwart CPA attacks in 3D ICs. Simulation results show that our method improves the correlation difference by 29.1% and 18.7% over 2D and 3D baseline, respectively. The average guessing entropy of our method is 9× that of the 3D baseline for 1000 power traces. Emulation on an FPGA platform proves that the proposed implementation method consumes significantly less power than the existing power balancing techniques. Our method reduces the power overhead by up to 81.1% over the round-level power balancing technique. The TVLA indicates proposed method reduces the risk of leaking sensitive information through power traces and that shows the improvement on CPA resilience. The limitation of our method is the increase on delay. However, the delay overhead can be adjusted by managing the circuit loads in other 3D planes. In future work, we will develop load management methods for the noise source planes while maintaining the resilience against CPA attack.

CRediT authorship contribution statement

Zhiming Zhang: Formal analysis, Validation, Writing - original draft. **Jaya Dofe:** Formal analysis, Validation, Writing - original draft. **Qiaoyan Yu:** Investigation, Methodology, Project administration, Supervision, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This research is partially supported by the National Science Foundation under CAREER grant (No. CNS-1652474) and NSF/SRC STARSS grant (No. CNS-1717130). Any opinions, findings and conclusions expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF/SRC.

References

[1] P. Kocher, J. Jaffe, B. Jun, P. Rohatgi, Introduction to differential power analysis, J. Cryptograph. Eng. 1 (Apr 2011) 5–27.
[2] E. Brier, C. Clavier, F. Olivier, Correlation power analysis with a leakage model, in: Proc. CHES04, 2004, pp. 16–29.
[3] J. Dofe, H. Pahlevanzadeh, Q. Yu, A comprehensive FPGA-based assessment on fault-resistant AES against correlation power analysis attack, J. Electron. Test. 32 (Oct. 2016) 611–624.

[4] P. Gu, et al., Leveraging 3D technologies for hardware security: opportunities and challenges, in: Proc. GLSVLSI, vol. 16, 2016, pp. 347–352.
[5] Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, M. Tehranipoor, Security and vulnerability implications of 3D ICs, IEEE Trans. Multi-Scale Comput. Syst. 2 (April 2016) 108–122.
[6] J. Valamehr, et al., A Qualitative Security Analysis of a New Class of 3-D Integrated Crypto Co-processors, Springer Berlin Heidelberg, 2012, pp. 364–382.
[7] J. Dofe, Z. Zhang, Q. Yu, C. Yan, E. Salman, Impact of power distribution network on power analysis attacks in three-dimensional integrated circuits, in: Proc. GLSVLSI17, 2017, pp. 327–332.
[8] J. Dofe, Q. Yu, Exploiting pdn noise to thwart correlation power analysis attacks in 3d ics, in: Proceedings of the 20th System Level Interconnect Prediction Workshop, SLIP 18, ACM, New York, NY, USA), 2018, pp. 6:16:6.
[9] L. Zhang, L.V. Gutierrez, M.B. Taylor, Power Side Channels in Security ICs: Hardware Countermeasures, 2016. CoRR, vol. abs/1605.00681.
[10] X. Wang, et al., Role of power grid in side channel attack and power-grid-aware secure design, in: Proc. DAC13, May 2013, pp. 1–9.
[11] D. Das, et al., High efficiency power side-channel attack immunity using noise injection in attenuated signature domain, in: Proc. HOST17, May 2017, pp. 62–67.
[12] C. Tokunaga, D. Blaauw, Securing encryption systems with a switched capacitor current equalizer, IEEE J. Solid State Circ. 45 (Jan 2010) 23–31.
[13] A.L. Masle, G.C.T. Chow, W. Luk, Constant power reconfigurable computing, in: Proc. ICFPT11, Dec 2011, pp. 1–8.
[14] S. Yang, W. Wolf, N. Vijaykrishnan, D.N. Serpanos, Y. Xie, Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach, in: Proc. DATE05, vol. 3, March 2005, pp. 64–69.
[15] W. Yu, S. Kose, Exploiting voltage regulators to enhance various power attack countermeasures, IEEE Trans. Emerg. Top. in Comput. 6 (2) (2018) 244–257.
[16] R. Muresan, S. Gregori, Protection circuit against differential power analysis attacks for smart cards, IEEE Trans. Comput. 57 (11) (2008) 1540–1549.
[17] A. Arora, J.A. Ambrose, J. Peddersen, S. Parameswaran, A double-width algorithmic balancing to prevent power analysis side channel attacks in aes, in: Proc. ISVLSI, Aug 2013, pp. 76–83.
[18] P.C. Liu, H.C. Chang, C.Y. Lee, A low overhead dpa countermeasure circuit based on ring oscillators, IEEE Trans. Circ. Syst. II: Express Brief. 57 (July 2010) 546–550.
[19] E. Prouff, M. Rivain, Masking against side-channel attacks: a formal security proof, in: Proc. Of EUROCRYPT13, 2013, pp. 142–159.
[20] C. Claude, et al., Higher-order masking schemes for S-boxes, in: Proc. FSE12, 2012, pp. 366–384.
[21] G. Tim, M. Amir, Generic side-channel countermeasures for reconfigurable devices, in: Proc. CHES11, 2011, pp. 33–48.
[22] H. Wang, Enhancing Power and Signal Integrity in Three-Dimensional Integrated Circuits, PhD thesis, The Graduate School, Stony Brook University, Stony Brook, NY., 2016.
[23] S.M. Satheesh, E. Salman, Power distribution in TSV-based 3-D processor-memory stacks, IEEE J. Emerg. Select. Top. Circuit. Syst. 2 (Dec 2012) 692–703.
[24] O.X. Standaert, E. Peeters, G. Rouvroy, J.J. Quisquater, An overview of power analysis attacks against field programmable gate arrays, Proc. IEEE 94 (Feb 2006) 383–394.
[25] J. Park, A.A. Korosov, M. Babiker, S. Sandven, J. Won, Efficient thermal noise removal for sentinel-1 topsar cross-polarization channel, IEEE Trans. Geosci. Rem. Sens. 56 (March 2018) 1555–1565.
[26] J.M. Bioucas-Dias, M.A.T. Figueiredo, Multiplicative noise removal using variable splitting and constrained optimization, IEEE Trans. Image Process. 19 (July 2010) 1720–1730.
[27] W. Yu, S. Kse, Implications of noise insertion mechanisms of different countermeasures against side-channel attacks,, in: 2017 IEEE International Symposium on Circuits and Systems (ISCAS), May 2017, pp. 1–4.
[28] A. Todri, M. Marek-Sadowska, J. Kozhaya, Power supply noise aware workload assignment for multi-core systems, in: Proc. ICCAS08, Nov 2008, pp. 330–337.
[29] R. Zhang, et al., Transient voltage noise in charge-recycled power delivery networks for many-layer 3D-IC, in: Proc. ISLPED15, July 2015, pp. 152–158.
[30] C. O'Flynn, Z.D. Chen, Side channel power analysis of an AES-256 bootloader, in: 2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE), May 2015, pp. 750–755.
[31] V.H. Nguyen, P. Christie, A. Heringa, A. Kumar, R. Ng, An analysis of the effect of wire resistance on circuit level performance at the 45-nm technology node, in: Proc. IITC05, June, 2005, pp. 191–193.
[32] J. Cooper, E. Demulder, Test Vector Leakage Assessment (Tvla) Methodology in Practice (Extended Abstract), 2013.
[33] D.B. Roy, S. Bhasin, S. Guilley, A. Heuser, S. Patranabis, D. Mukhopadhyay, Leak Me if You Can: Does Tvla Reveal Success Rate, 2016. tech. rep., Cryptology ePrint Archive, Report 2016/1152.
[34] T. Schneider, A. Moradi, Leakage assessment methodology,, in: T. Gneysu, H. Handschuh (Eds.), Cryptographic Hardware and Embedded Systems CHES 2015, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015, pp. 495–513.
[35] K. Tiri, M. Akmal, I. Verbauwhede, A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards, in: Proceedings of the 28th European Solid-State Circuits Conference, Sept 2002, pp. 403–406.
[36] D. Jayasinghe, A. Ignjatovic, J.A. Ambrose, R. Ragel, S. Parameswaran, Quadseal: quadruple algorithmic symmetrizing countermeasure against power based side-channel attacks, in: 2015 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), Oct 2015, pp. 21–30.