2017 IEEE 35th International Conference on Computer Design

Power Profile Equalizer: a Lightweight Countermeasure against Side-channel Attack

Chenguang Wang*, Ming Yan*, Yici Cai*, Qiang Zhou* and Jianlei Yang†
*Tsinghua National Laboratory for Information Science & Technology
Department of Computer Science & Technology, Tsinghua University, Beijing, China
Email: {wang-cg13, yanm15}@mails.tsinghua.edu.cn, {caiyc, zhouqiang}@mail.tsinghua.edu.cn
†Fert Beijing Research Institute, BDBC, School of Computer Science and Engineering, Beihang University, Beijing, China
Email: jianlei@buaa.edu.cn

***Abstract*—Power attack is an important side-channel attack (SCA) method based on the correlation between measured power profile and internal switching activities. Various techniques have been proposed to prevent power attack. It has been noted that the on-chip power grid (PG) has a vital effect on the effectiveness of power attack by inducing a noise in the power profile. However, there is a lack of study on this intrinsic effect of PG. In this paper, we explore the methods of exploiting the PG-induced noise to counter with power attack. We note that the PG-induced noise strongly depends on the PG impedance and it can be regulated by adjusting the PG capacitor to control the power profile to fixed values, which contributes to reducing the power leakage. Further, we propose a novel adjustment technique for PG capacitor, i.e. power profile equalizer (PPE), as a lightweight (low-overhead) countermeasure against power attack. PPE exploits the regulated noise to equalize the power profile without violating the layout and supply noise constraints. To reduce the overheads, random walk is adopted to utilize the utmost on-chip resources. Moreover, PPE is implemented by optimizing PG which is an essential IC component rather than producing new circuits. As a result, PPE incurs low overheads. Experimental results show that PPE is able to improve the measurements to disclose (MTD) by 1800x while the area and power increase respectively by 0.12% and 0.91%.**

I. Introduction

In recent years, to protect cryptographic devices from side-channel attack (SCA) has been one of the major concerns of IC designers. SCA analyzes the side-channel leakage, e.g. power consumption and electromagnetic radiation, to extract the information [1]. Power attack is an important SCA method that is based on the correlation between the measured power profile and internal switching activities, e.g. Differential Power Analysis (DPA) [1] and Correlation Power Analysis (CPA) [2].

To prevent power attack, researchers have proposed various techniques that can be split into *masking* and *hiding* categories [3]. Masking combines sensitive variables with random values to reduce the power leakage. The first *d*th-order masking scheme is proposed in [4] for protecting Advanced Encryption Standard (AES). Nassar *et al.* present a lightweight Boolean masking method "RSM" [5]. Further, Patranabis *et al.* propose a two-round shuffling method for block ciphers [6].

On the contrary, hiding aims to control the power leakage to predefined values [7]. Various schemes have been proposed to flatten the fluctuations of current, voltage or power waveforms. Tiri *et al.* present new compound standard cells that have close-to-constant power consumption [8]. In [9], Tokunaga *et al.* present a current equalizer circuit by integrated switched capacitors. Wang *et al.* introduce a frequency-dependent noise-injection based compensation technique [10]. Further, Gornik *et al.* propose to decouple the main power supply from the internal by protecting each logic gate with a decoupling cell, which can be combined with standard cells to form a new library for security-related applications [11]. A multi-level switched capacitor voltage regulator is proposed by Yu *et al.* to scramble the power profile [12]. Further, Kar *et al.* perform a detailed analysis to exploit the fully integrated inductive voltage regulator to inhibit power attack [13].

Recently, there has been a growing interest in exploring the effect of on-chip power grid (PG) on power attack resistance. It is noted that PG plays an important role in the effectiveness of power attack [10]. Generally, the power profile is measured by the voltage drop across a resistor in series with the supply pin. For the impedance properties, PG induces a noise in the supply current when it flows via PG from inside the chip to supply pin for measurement, creating difficulty for power attack. In [14], Yang *et al.* propose a PG-induced noise aware framework to evaluate the power attack resistance at pre-silicon stage. Dofe *et al.* investigate the impact of three-dimensional PG on the efficiency of CPA [15]. To summarize, the PG-induced noise can create difficulty for performing power attack.

However, there is a lack of study on leveraging the intrinsic effect of PG to prevent power attack. Since an accurate power measurement is vital for the effectiveness of power attack, we investigate the PG-induced noise in the power profile and note that it is strongly dependent on the PG impedance of capacitor. Further, mathematical proofs are provided to demonstrate that the noise can be regulated to equalize the power profile by adjusting the PG impedance of capacitor. Moreover, detailed mathematical analysis is performed to determine exactly how the PG-induced noise can be regulated through the capacitor adjustment, i.e. adding equalization capacitor, to flatten the switching current waveform over time.

An important issue of the capacitor adjustment is that it may affect the performance of power supply because the voltage drop can be affected by adjusting the PG parameters (e.g.

This project is supported by National Natural Science Foundation of China (NSFC) under Grant No. 61774091 and in part by Grant No. 61602022.

1063-6404/17 $31.00 © 2017 IEEE
DOI 10.1109/ICCD.2017.54

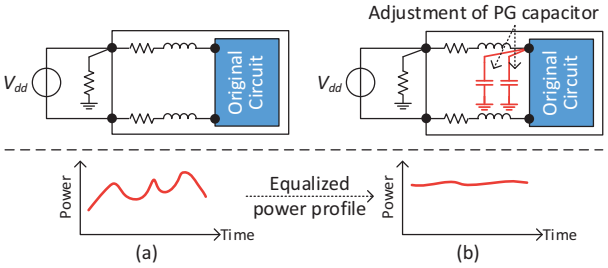

Fig. 1: Basic concept of the proposed countermeasure. (a) Unprotected. (b) Protected with Power Profile Equalizer.

decoupling capacitor optimization) or topology (e.g. topology optimization) [16]. To eliminate the negative effects, voltage scheduling is executed prior to the protection to maintain the supply noise within certain threshold. Moreover, the added capacitor only accounts for a fraction of the overall one.

Based on the above investigation, we propose a novel adjustment technique for PG capacitor, i.e. Power Profile Equalizer (**PPE**), as a lightweight countermeasure against power attack. PPE makes use of the regulated noise due to the additional equalization capacitor to control the power profile to fixed values, as shown in Fig.1. A refinement inspired by the random walk [17] is proposed to distribute the required equalization capacitor in a subcircuit of PG to utilize the utmost of on-chip resources. More importantly, PPE is based on optimizing the underlying PG which is anyway essential in modern IC rather than producing new circuit types. As a result, PPE incurs low overheads of on-chip area and power. Besides, to reduce the computational complexity of security metric, which is used to model and estimate the side-channel leakage [18], we propose a new simplified metric with an adequate accuracy.

To summarize, the contributions of this paper include:

1) We note that the PG-induced noise in the power profile strongly depends on the PG impedance. Mathematical proofs are provided to demonstrate that this noise can be regulated to control the power consumption leakage to fixed values, by adding equalization capacitor.
2) Based on the investigation, a novel adjustment technique for PG capacitor, i.e. power profile equalizer, is proposed as a lightweight countermeasure against power attack. PPE exploits the regulated noise due to the additional equalization capacitor to equalize the power profile, with the constraints of layout and supply noise satisfied.
3) We implement protected 128-bit AES designs using the proposed method. The experimental results of DPA attack on the implementation show that our method is able to provide competitive protection against power attack with fairly low overheads of on-chip area and power.

The rest of this paper is organized as follows. Section II provides the preliminaries. The theoretical foundations of PPE are presented in Section III. Section IV introduces the methodology of PPE. Section V presents the experimental results. The conclusion and discussion are in Section VII.

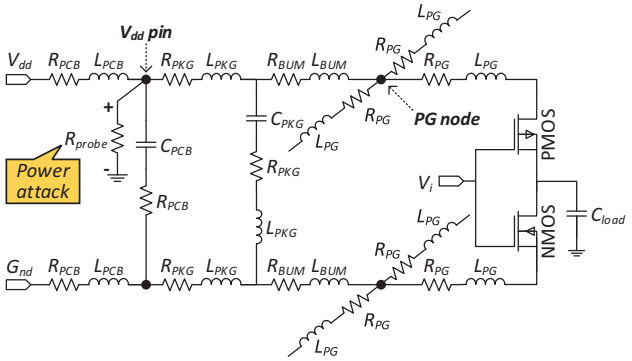

Fig. 2: Threat model of power attack.

II. Preliminaries

A. Threat Model of Power Attack

The threat model in this paper follows the commonly used one in the power attack community [19]. The power profile is usually measured through the voltage drop or current across a probe resistor (R_{probe}) in series with the V_{dd}/G_{nd} pin, as shown in Fig.2. Power attack can also use power measurement by precise instruments. At the attack point, e.g. a V_{dd} pin, the measurement will be introduced noise due to the impedance properties of the package, bump pads, and PG. It is known that the PG component dominates the entire impedance.

B. Power Grid and Cell Modeling

The power grids in each metal layer can be accurately modeled using lumped impedance parameters. Each power wire in the grid is represented as a set of connected segments under the typical π-model [16], with each segment modeled using lumped *RLC* (resistor, inductor, and capacitor). The inductor mainly stems from the PG-package interconnection, which is often ignored, leading to a purely *RC* network [20]. The package is distributed to the nodes with partially-lumped solder bump impedance. In this paper, the PG is modeled as an *RC* network which has resistive connections between the nodes and a capacitor from every node to G_{nd}, as illustrated in Fig.3. The *RC* parameters are extracted from the post-placement-and-routing layout with commercial tools.

The modeling of cell switching current has been an active branch of research. In a typical *RC* model of cell, the switching activities are modeled as an equivalent circuit consisting of a time-varying resistor, loading capacitor, and decoupling capacitor [16]. Although this model is accurate, the simulation of the entire circuits requires analyzing a varying topology as circuit elements switch in and out of the network, complicating the simulation. Generally, a convenient choice is to model the switching cell as a piecewise linear (*PWL*) current source whose waveform approximates the actual one of the functional block. In this paper, the *PWL* current source is depicted in the HSPICE vector format which is transformed from the *Value Change Dump* (*VCD*) file with random input patterns provided as the stimulus of the AES encryption engine.

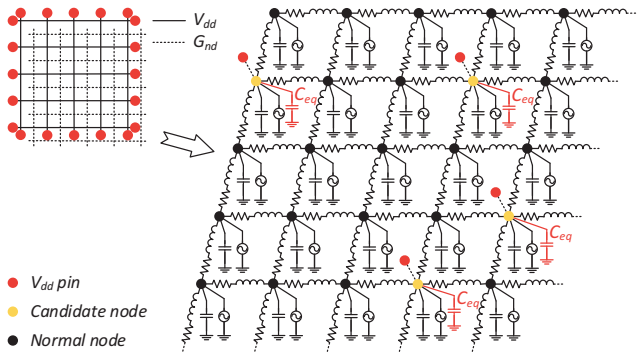

Fig. 3: Lumped RC model of power grid.

III. Power Profile Equalization by Regulating the PG-induced Noise

In this section, the theoretical foundations are provided. By reviewing the power consumption of IC, we investigate the PG-induced noise in power profile and note the strong dependence of the noise on the PG impedance of capacitor. Further, it is demonstrated that the noise can be regulated to equalize the power profile by adjusting the PG capacitor, i.e. adding equalization capacitor. Mathematical analysis is performed to size the required equalization capacitor.

A. PG-induced Noise in Power Profile

It is known that there are three major terms of the total power consumption (P_{tot}) in digital CMOS circuits:

$$P_{tot} = \alpha f \cdot C_{load} \cdot V_{dd}^2 + V_{dd} \cdot I_{sc} + V_{dd} \cdot I_{leak} \quad (1)$$

In (1), the first term represents the switching component which is a function of switching activity factor α, clock frequency f, loading capacitor C_{load}, and the square of supply voltage V_{dd}. The second and third terms are respectively due to the direct-path short circuit current I_{sc} and leakage current I_{leak}. It is known that the switching component dominates the total power consumption [21]. Further, the average power and energy consumption during an operation can be expressed as:

$$\begin{aligned} P_{tot} &= P_{dyn} + P_{stat} = k \cdot \alpha f \cdot C_{avg} \cdot V_{dd}^2 + V_{dd} \cdot I_{leak} \\ E_{tot} &= P_{tot} \cdot T = k \cdot C_{tot} \cdot V_{dd}^2 + V_{dd} \cdot I_{leak} \cdot T \end{aligned} \quad (2)$$

where P_{tot} is the total power (the dynamic P_{dyn} pluses the static P_{stat}), E_{tot} is the total energy consumption, C_{avg} is the total average capacitor switched by the operation per clock cycle, k is a constant, C_{tot} is the total capacitor switched by the operation, and T is the operation period.

It can be seen that the power consumption of IC is mainly dependent on the capacitor, current, and supply voltage. Besides, in CMOS gates, the current through MOS transistors depends on the supply voltage, which is usually defined in the specification. As a result, the total power and total energy consumption can be changed by varying the capacitor.

Due to the intrinsic impedance properties, PG has an effect on the total capacitor. By affecting the capacitor, PG scrambles the power consumption and ultimately induces a noise in the power profile measurement. To summarize, the PG-induced noise in power profile measurement is strongly dependent on the PG impedance of capacitor.

B. Noise Regulation by Adding Capacitor

The significant problem here is how to regulate the noise to equalize the power profile. Based on the above investigation, we introduce the approach of adding equalization capacitor.

1) PG Capacitor and Candidate Nodes: The total PG capacitor consists of 1) Intrinsic parasitic capacitor of functional block (C_p). 2) Decoupling capacitor allocated to suppress the power supply noise (C_{de}). 3) **Equalization capacitor** allocated to flatten the switching current waveform (C_{eq}). Like the decoupling capacitor is imperative for suppressing the power supply noise, the additional equalization capacitor is expected to flatten the switching current waveform by regulating the PG-induced noise.

We define the **candidate nodes** for C_{eq} location as the connection nodes between PG network and supply pins, i.e. the nodes which are connected to the supply I/O pads (with wire-bond packaging) or bumps (with flip-chip packaging), as shown in Fig.3. The reasons here are as follows.

It can be noted that the current waveform which flows via the node connected to the attack point, i.e. the candidate node, is the most approximate to the measured power profile. From the perspective of an adversary, the most "useful" information is the switching current waveform at the candidate node, which provides an ideal side-channel leakage without noise. Consequently, the equalization capacitor should be placed at the candidate nodes to have a flattening effect on the current waveform and ultimately the measured power profile.

2) Equalization Capacitor Sizing for Noise Regulation: In order to guarantee the performance of circuits, the total energy consumption should be consistent before and after adding the equalization capacitor. By (2) and $C = Q/U$, the consistent energy means the total charge cannot be changed when V_{dd} is stable, which is expressed as:

$$Q_{tot} = I_{ref} \cdot \Delta t = \int_{t}^{t+\Delta t} I_{sw}(t)dt \quad (3)$$

In (3), Q_{tot} is the total charge that each functional block draws from the power supply, I_{ref} is the fixed current value, $I_{sw}(t)$ is the switching current waveform, and Δt is the duration the switching process lasts. It can be noted that the $I_{sw}(t)$ time integral above and below I_{ref} (respectively Q_a and Q_b) are identical, i.e. $Q_a = Q_b$, as shown in Fig.4. As a result, the total energy consumption is guaranteed through the charge compensation over time.

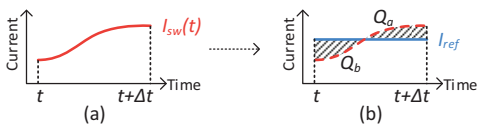

Fig. 4: Flattening the switching current waveform.

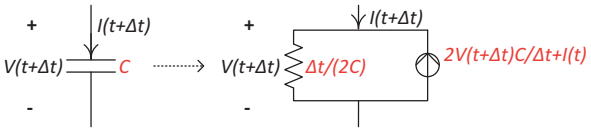

Fig. 5: Discrete model of capacitor.

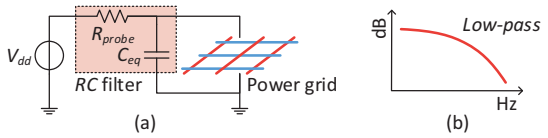

Fig. 6: Low-pass property of the RC filter.

Let us examine the typical static discrete model of capacitor in Fig.5, which consists of a resistor and a parallel equivalent current source induced by the capacitor, i.e. $I_{eq}(t)$:

$$I_{eq}(t) = V(t+\Delta t) \cdot 2C_{eq}/\Delta t + I_{sw}(t) \tag{4}$$

where $V(t)$ is the voltage waveform and Δt is the time step of the discrete transformation, which is defined considering the tradeoff between the accuracy and computational complexity.

In order to size the equalization capacitor required to control the switching current waveform to the fixed current value of I_{ref}, the C_{eq}-induced current source ($I_{eq}(t)$) is expected to fill in the gap between the actual switching current and the computed fixed value, which is expressed as (5):

$$I_{eq}(t) = I_{sw}(t+\Delta t) - I_{ref} \tag{5}$$

Besides, it is known that the probe resistor R_{probe} and the additional equalization capacitor C_{eq} can be considered as an *RC* filter with the low-pass property, as shown in Fig.6. The *RC* filter helps to equalize the measured power profile by flattening the voltage ripples on high frequencies. On the other hand, it has been noted that the PG impedance has a frequency-dependent factor, as illustrated in Fig.7 [22], which means that the intrinsic resistance against power attack provided by PG can vary with the operation frequencies of cryptographic devices. The above frequency-dependent properties collaboratively contribute to scrambling the power profile and thus preventing power attack.

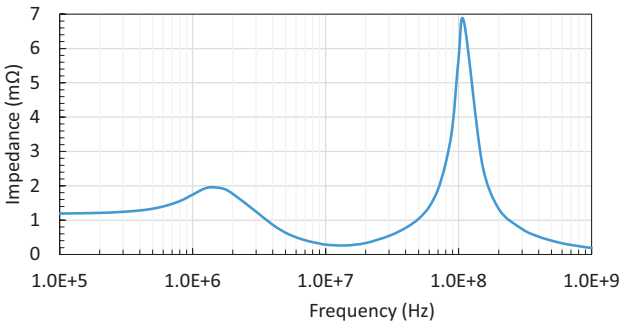

Fig. 7: Frequency-dependent impulse response of power grid.

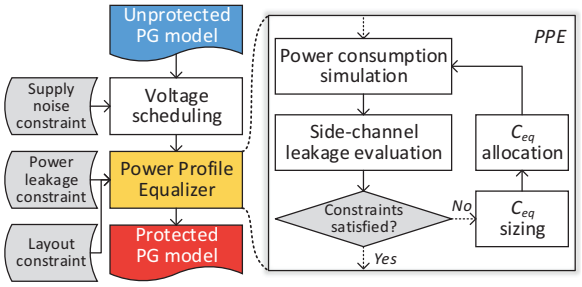

Fig. 8: Flow chart of Power Profile Equalizer.

IV. Methodology of Power Profile Equalizer

Based on the above investigation, we propose the methodology of PPE, as presented in Fig.8. In order to suppress the supply noise, voltage scheduling is executed prior to PPE to satisfy the supply noise constraint. The power consumption is simulated with random input patterns. Based on the simulated power profiles, the side-channel leakage metric is computed to determine whether the predefined power leakage constraint is satisfied. If not, the equalization capacitor sizing and allocation are iterated until the constraints are satisfied.

We propose a new security metric to reduce the computational complexity. Besides, to reduce the overheads, we also propose a refinement for the allocation by random walk algorithms. The details of PPE will be introduced as follows.

A. Side-channel Leakage Evaluation

Generally, security metric is used to model and evaluate the side-channel leakage, e.g. signal-to-noise ratio (*SNR*), which has been commonly used in previous literatures [18]. However, it has been noted that *SNR* is inaccurate because the noise can be averaged out by advanced signal processing [19]. Moreover, the existing metrics which are accurate are usually too complicated to compute in a lightweight framework. To overcome this limitation, we propose a new security metric, i.e. *correlation-concerned SNR* (*cSNR*), by eliminating the disadvantages of *SNR* to reduce the computational complexity. Besides, *cSNR* has an adequate accuracy for the evaluation.

In power attack, the measured power (P) mainly stems from the switching activities of transistors, while the hypothetical power (P^*) is computed with hypothetical subkey [2]. It is known that the minimal number of measurements to disclose (MTD) strongly depends on the highest value of correlation coefficients between P^* and P, i.e. $\rho(P^*,P)_{max}$:

$$MTD = 3 + 8\Big(Z_\alpha / \ln\frac{1+\rho(P^*,P)_{max}}{1-\rho(P^*,P)_{max}}\Big)^2 \tag{6}$$

In (6), the quantile Z_α is the distance between 0 and $\rho(P^*,P)_{max}$. In general, *SNR* is defined by the variances of Q and N as $var(Q)/var(N)$, where Q is the power of the target gates where intermediate values are processed, and N is the noise derived from the uncorrelated gates. The impact of *SNR* on $\rho(P^*,P)$ can be expressed as:

$$\rho(P^*,P) = \rho(P^*,Q)/\sqrt{1+1/SNR} \tag{7}$$

By (6) and (7), it can be seen that *SNR* has a negative effect on MTD. However, the correlation between power and noise, i.e. $\rho(Q, N)$, is usually assumed to be zero and thus ignored in previous works, which implies counterexamples in special scenarios and potential threats to cryptographic devices [10]. To solve this problem, *cSNR* is defined with $\rho(Q, N)$ considered, which also has a negative effect on MTD:

$$cSNR = \frac{var(Q)}{var(N)} \cdot \frac{1}{1 - \rho(Q, N)} \tag{8}$$

In terms of $\rho(Q, N)$, the power leakage can be categorized into two cases, i.e. $\rho(Q, N) = 0$ and $\rho(Q, N) \neq 0$. The difference between the two cases can be expressed in the value of *cSNR*, however, *SNR* is consistent for both cases, which demonstrates the advantage of *cSNR* over *SNR*. In practice, it is difficult and unnecessary to exactly measure Q and N. On this observation that the nonideal PG induces a noise in the power profile, the power consumption with ideal/nonideal PG are measured as the substitutes of Q/N, which is verified to have an adequate accuracy for the power leakage evaluation.

B. Sizing of Equalization Capacitor

Based on the mathematical proofs provided in Section III, the required equalization capacitor at the candidate node of x (C^x_{eq}) can be sized by (9):

$$\begin{aligned} C^x_{eq} &= \frac{I_{sw}(t + \Delta t) - I_{ref} - I_{sw}(t)}{2V(t + \Delta t)} \cdot \Delta t \\ I_{ref} &= \int_t^{t+\Delta t} I_{sw}(t)dt/\Delta t \end{aligned} \tag{9}$$

In (9), $I_{sw}(t)$ is represented by a *PWL* current source as mentioned before, and $V(t)$ is obtained by standard power grid analysis as the previous literatures.

However, due to the limited on-chip area in the post-placement-and-routing layout, the required equalization capacitor can be beyond the space available. Besides, the additional equalization capacitor incurs more power consumption. To overcome this limitation, we propose a distributed allocation technique based on the random walk algorithms.

C. Allocation Refined with Random Walk

Random walk [17] is one category of the Monte Carlo methods of numerical computation. It has been noted the PG analysis problem can be speeded up without sacrificing the degree of accuracy by random walk. To reduce the overheads of chip area and power consumption, we propose a refinement for the allocation based on the random walk algorithms to utilize the utmost on-chip resources.

The principles of random walk are applied to generating subcircuits and then distributing the equalization capacitor all over the subcircuits rather than at single candidate nodes. The required equalization capacitor is allocated at each node of the subcircuit in a distributed manner. As a result, even if the space available at x is limited, C^x_{eq} can be allocated in the subcircuit, which reduces the required C^x_{eq} under certain layout and power leakage constraints in return. The refinement for the allocation contains two phases as follows.

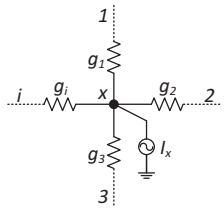

Fig. 9: A representative power grid node x.

1) Subcircuit Generation: The subcircuit generation here is similar to the classical problem of circuit partitioning which is generally modeled as a hypergraph/graph partitioning problem [16], however, the difference is that only a fraction of the entire nodes will be assigned into the generated subcircuits.

Let us examine the single PG node x in Fig.9. We have (10) by Kirchhoff's Current and Voltage Law, where i is the adjacent node of x, $degree(x)$ is the total number of nodes adjacent to x, g_i is the conductance between x and i, and I_x is the current source of the functional block.

$$\sum_{i=1}^{degree(x)} g_i \cdot (V_i - V_x) = I_x \tag{10}$$

$$V_x = \sum_{i=1}^{degree(x)} \frac{g_i}{\sum_{i=1}^{degree(x)} g_i} \cdot V_i - \frac{I_x}{\sum_{i=1}^{degree(x)} g_i} \tag{11}$$

Equation (10) can be rewritten as (11). Setting the multiplication fraction of V_i as $P_{x\to i}$ (probability of visiting i from x) as expressed in (12), we can see that $\sum_{i=1}^{degree(x)} P_{x\to i} = 1$:

$$P_{x\to i} = \frac{g_i}{\sum_{i=1}^{degree(x)} g_i} \tag{12}$$

As a result, the subcircuit generation problem is modeled as a mathematically equivalent random walk problem. Each step of the random walk is selected by the highest value of $P_{x\to i}$, then a subcircuit (G_x) is generated based on the ever visited nodes. However, it is time-consuming and unnecessary to perform exhaustive random walk in practice [17], so the superior limits of iterations (*MAX_ITER*) and steps (*MAX_STEP*) are set empirically.

2) Distributed Allocation in Subcircuit: The problem here is how to distribute C^x_{eq} all over the generated subcircuit. Let us examine (11), it can be noted that the voltage of each node is a linear function of the voltages of its adjacent nodes. $P_{x\to i}$ represents the linear coefficient associated with V_i and thus quantifies the influence of node i on x. Likewise, $P_{x\to i}$ can be used to determine the distributed factor of C^x_{eq} for the allocation all over the nodes in G_x, which is expressed as:

$$C^j_{eq} = \frac{P_{x\to j}}{\sum_{j=1}^{degree(G_x)} P_{x\to j}} \cdot C^x_{eq} \tag{13}$$

where j represents each node in G_x, C^j_{eq} is the distributed fraction of C^x_{eq} at j, $degree(G_x)$ is the total number of nodes in G_x, and $P_{x\to j}$ is the probability of visiting j from x.

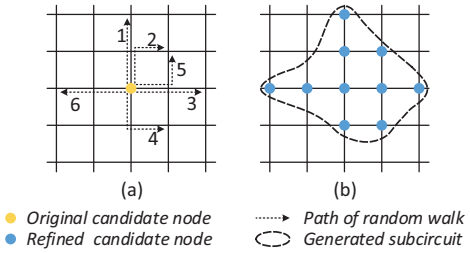

Fig. 10: Example of the random walk application.

TABLE I: On-chip overheads reduction by the refinement

Refinement?	Tot. Area (μm^2)	Avg. Power (μW)
No	335169	67.14967395
Yes	307302 **(-8.31%)**	62.39059746 **(-7.09%)**

Fig.10 provides an example of the refinement. First, each step is selected by the highest $P_{x\to i}$ from the current node x until the selection is repeated for certain times, e.g. each path in Fig.10(a) has two steps (*MAX_STEP*=2). Then, the above process is iterated for certain times, e.g. six paths are generated (*MAX_ITER*=6). As a result, each node in the subcircuit is the refined candidate node for C_{eq}, as shown in Fig.10(b). The technique is validated by comparing the overheads of designs without and with the refinement under the same power leakage constraint, as presented in Table I. It can be seen that fewer resources are consumed with the proposed refinement.

D. Algorithm Description

Algorithm 1 provides our proposed countermeasure against power attack. Given the unprotected PG model, the sizing and allocation of equalization capacitor are iterated until the iteratively updated *cSNR* meets the predefined power leakage constraint. The algorithm outputs a protected PG model.

Algorithm 1 Power Profile Equalizer

Require: Unprotected power grid model;
Output: Protected power grid model;
  Load the PG model and perform PG analysis;
  Simulate the power consumption and compute *cSNR* by (8);
  while *cSNR* $>$ power leakage constraint **do**
    while $\exists x \in$ PG nodes $\models x$ is unvisited **do**
      if x is directly connected to V_{dd} pin **then**
        Candidate nodes$\leftarrow x$;
        Compute C_{eq}^{x} by (9);
      end if
    end while
    while $\exists x \in$ Candidate nodes $\models x$ is unvisited **do**
      while *ITER* $\leq$ *MAX_ITER* **do**
        while *STEP* $\leq$ *MAX_STEP* **do**
          $P_{x\to i} := g_i / \sum_{i=1}^{degree(x)} g_i$;
          $G_x \leftarrow i \models P_{x\to i} \geq P_{x\to s}, s = 1, 2, ..., degree(x)$;
          STEP ++;
        end while
        ITER ++;
      end while
      $C_{eq}^{j} := C_{eq}^{x} \cdot P_{x\to j} \sum_{j=1}^{degree(G_x)} P_{x\to j}$;
      Allocate C_{eq}^{j} at node j, $\forall j \in G_x$;
    end while
    Update the PG model and compute *cSNR*;
  end while

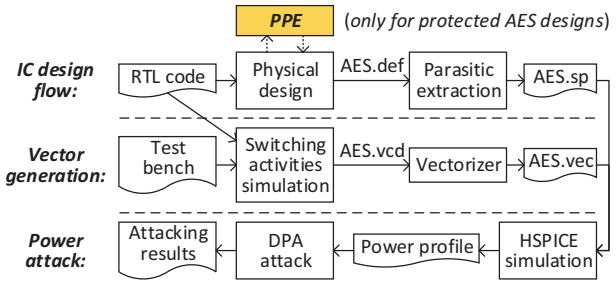

Fig. 11: Flow chart of experimental framework.

V. Experimental Results

To validate the effectiveness and efficiency of PPE, DPA is performed to extract the encryption key of unprotected and protected AES-128 designs implemented with industrial $0.13\mu m$ technology kits, which is executed on a Linux server with Intel Xeon E5506 CPU @ 2.4 GHz and 24 GB RAM. The switching activities, i.e. the *PWL* current sources, are depicted in the HSPICE vector format, which is transformed from the corresponding *VCD* files using a tool named Vectorizer. The PPE and Vectorizer are implemented in C++ language. The overall experimental framework is presented in Fig.11.

A. Security Improvement

Fig.12 presents the power profile of unprotected AES design while executing the encryption. Each of the ten spikes indicates the beginning of one round operation of AES. As a comparison, Fig.13 presents the same experiment on the protected one, where the ten spikes are identified as well. It can be seen that the protected power profile is flattened compared with the unprotected one. However, the encryption key cannot be extracted even if each of the round operations is identified.

Fig.14 shows the differential power profile of the unprotected design, where the existence of a clear peak indicates a correct guess of the encryption key [1] because the correct subkey will partition the power profile according to the value of the bits actually operated in the device. As a comparison, there exists no clear peak in the differential power profile of the protected design, which means the guessed subkey is not correct, as shown in Fig.15. The final results show that the MTD of the protected design has been improved by 1800x.

Table II provides the on-chip overheads of the proposed method. It can be seen that compared with the unprotected AES encryption engine, the chip area and power consumption of the protected one increase by respectively 0.12% and 0.91%, which is within reasonable bounds.

As mentioned above, the proposed protection method may affect the power supply noise due to the additional capacitor. To overcome this limitation, voltage scheduling is executed prior to PPE to maintain the supply noise within 5% V_{dd}[1]. Besides, the additional capacitor only accounts for a fraction of the total PG capacitor. As a result, the supply noise constraints can be still maintained within the certain threshold (V_{th}).

[1]Typically, the power supply noise is maintained within 5%–10% V_{dd} [16].

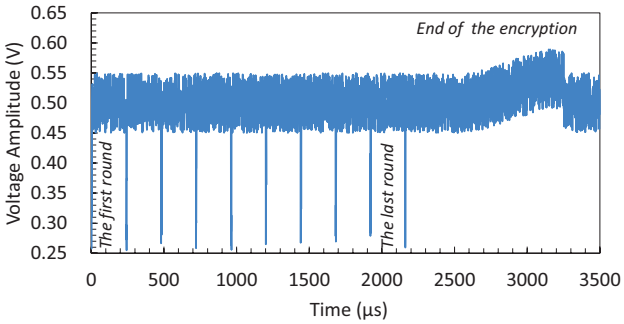

Fig. 12: Power profile of unprotected AES design.

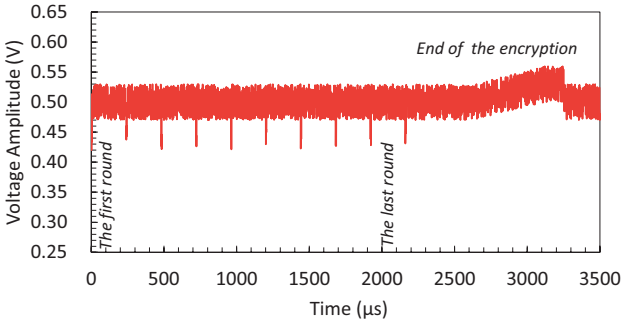

Fig. 13: Power profile of protected AES design.

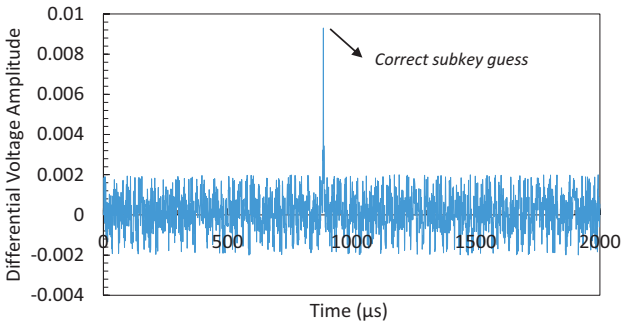

Fig. 14: Differential power profile of unprotected AES design.

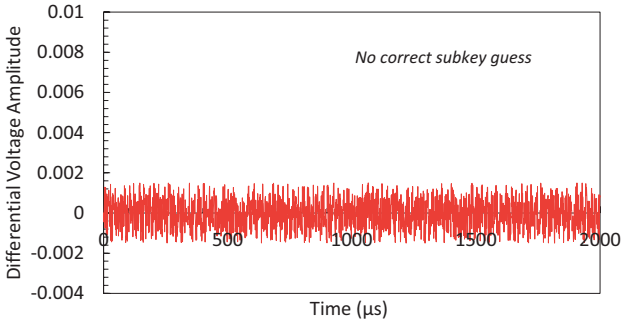

Fig. 15: Differential power profile of protected AES design.

TABLE II: On-chip overheads of PPE

AES Design	Tot. Area (μm^2)	Avg. Power (μW)
Unprotected	306925	61.826359
Protected	307302 (**+0.12%**)	62.390597 (**+0.91%**)

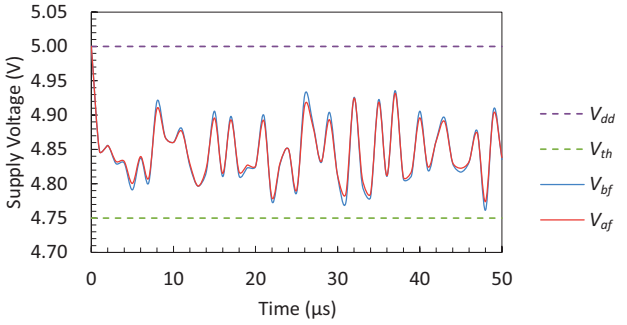

Fig. 16: Voltage waveforms before and after the placement of equalization capacitor.

Fig.16 shows the supply voltage before (V_{bf}) and after (V_{af}) the placement of equalization capacitor. The slight differences between V_{bf} and V_{af} can be attributed to the slightly higher total capacitor due to the additional equalization capacitor. One interesting finding is that the voltage drop is alleviated by the additional C_{eq}, and the reason is that C_{eq} has the similar effect with C_{de} on the power supply noise.

B. Comparison with Existing Works

To the best of our knowledge, PPE makes the first attempt to exploit the intrinsic PG-induced noise to prevent power attack, which is different from the existing literatures in the principles, thus a fair and elaborate comparison is not currently possible. Based on the reported attacking results on AES, a rough comparison is concluded in Table III.

Tokunaga *et al.* report a significant MTD improvement of 2500x, however, the power overhead is 33% [9], which can compromise the functionality of the circuits. The results in [10] are not presented in MTD, but it can be deduced that the MTD has been improved by at least 2x. Gornik *et al.* propose a countermeasure to improve MTD by 466x [11], which incurs higher overheads than the other works. Yu *et al.* perform a detailed theoretical proof of the proposed method, with the improvements presented only by analyzing the power trace entropy [12]. The method in [13] has a zero overhead of chip area with a reasonable performance in MTD improvement, however, the power overhead has not been reported yet.

The main challenges for the power attack countermeasures are the increased chip area, power consumption, and design complexity. Our technique has a low design complexity because it is based on optimizing the PG which is an essential component in IC and thus allows for easier integration into the IC design flow. Moreover, it can be seen that our technique improves the MTD by 1800x while incurs fairly low overheads, which can be attributed to:

1) No circuit types are newly produced. On the contrary, it makes use of the intrinsic noise in the power profile induced by PG rather than producing new circuits.
2) The allocation is refined by random walk algorithms to utilize the utmost on-chip resources under the layout constraints, which reduces the overheads in return.

TABLE III: Comparison with existing works

Works	Power Attack on AES	MTD	On-chip Overhead	
			Area	Power
Tokunaga *et al.* [9]	DPA	2500x	+7.2%	+33%
Wang *et al.* [10]	CPA	>2x	+37.5%	+35.2%
Gornik *et al.* [11]	CPA & DPA	466x	10x	3.5x
Yu *et al.* [12]	Entropy analysis	N/A	N/A	N/A
Kar *et al.* [13]	CPA	80x	Zero	N/A
This Paper	DPA	**1800x**	**+0.12%**	**+0.91%**

VI. Conclusion and Discussion

In this paper, we explore the techniques of leveraging the intrinsic PG-induced noise in the power profile measurement to protect the cryptographic devices against power attack. We investigate the PG-induced noise and note its strong dependence on the PG impedance of capacitor. Further, mathematical proofs are provided to demonstrate that the noise can be regulated by adding capacitor at the candidate nodes to equalize the power profile, which contributes to reducing the power consumption leakage and thus preventing power attack. Further, based on the above theoretical foundations, PPE is proposed as a lightweight countermeasure against power attack. Experimental results show that PPE is able to protect the AES designs with the MTD improved by 1800x while the chip area and power consumption increase by respectively 0.12% and 0.91%, which is quite low compared with the existing literatures.

The first point we should highlight is that PPE has quite low overheads while provides competitive protection against power attack. PPE is based on optimizing the underlying PG which is an essential IC component rather than producing new circuit types. Besides, a refinement based on the random walk is applied to distributing the capacitor all over a subcircuit rather than at a single node to utilize the utmost on-chip resources. As a result, the overheads are significantly reduced.

We also notice that the adjustment of PG capacitor may affect the performance of power supply. To eliminate the possible negative effects, voltage scheduling is executed prior to PPE. On the other hand, the additional capacitor only accounts for a fraction of the entire PG capacitor including the intrinsic parasitic and decoupling capacitor. As a result, the power supply noise can be maintained within the certain threshold, which is verified by the voltage waveforms.

To reduce the high computational complexity of security metric, we propose the *cSNR* which is easy to compute and has an adequate accuracy for the side-channel leakage evaluation. The new metric is based on the commonly used *SNR* with the correlation between the power and noise considered, which is assumed to be zero and thus ignored in the *SNR* definition, eliminating the potential counterexamples in special scenarios.

In the future, on the observation that the simulated current sources are dependent on the stimulus input patterns, we plan to train a current source model from the properties of the simulated switching activities by machine learning applications. Besides, the properties of simulated results which are identical to different input patterns will be removed to generalize the learned model.

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology - CRYPTO*, 1999, pp. 388–397.

[2] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems, CHES*, 2004, pp. 16–29.

[3] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks - revealing the secrets of smart cards*. Springer, 2007.

[4] M. Rivain and E. Prouff, "Provably secure higher-order masking of AES," in *Cryptographic Hardware and Embedded Systems, CHES*, 2010, pp. 413–427.

[5] M. Nassar, Y. Souissi, S. Guilley, and J. Danger, "RSM: A small and fast countermeasure for aes, secure against 1st and 2nd-order zero-offset scas," in *Design, Automation & Test in Europe Conference & Exhibition, DATE*, 2012, pp. 1173–1178.

[6] S. Patranabis, D. B. Roy, P. K. Vadnala, D. Mukhopadhyay, and S. Ghosh, "Shuffling across rounds: A lightweight strategy to counter side-channel attacks," in *IEEE International Conference on Computer Design, ICCD*, 2016, pp. 440–443.

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

[8] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Design, Automation & Test in Europe Conference & Exhibition, DATE*, 2004, pp. 246–251.

[9] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, 2010.

[10] X. Wang, W. Yueh, D. B. Roy, S. Narasimhan, Y. Zheng, S. Mukhopadhyay, D. Mukhopadhyay, and S. Bhunia, "Role of power grid in side channel attack and power-grid-aware secure design," in *The 50th Annual Design Automation Conference, DAC*, 2013, pp. 78:1–78:9.

[11] A. Gornik, A. Moradi, J. Oehm, and C. Paar, "A hardware-based countermeasure to reduce side-channel leakage: Design, implementation, and evaluation," *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 34, no. 8, pp. 1308–1319, 2015.

[12] W. Yu, O. A. Uzun, and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *The 52nd Annual Design Automation Conference, DAC*, 2015, pp. 115:1–115:6.

[13] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Exploiting fully integrated inductive voltage regulators to improve side channel resistance of encryption engines," in *International Symposium on Low Power Electronics and Design, ISLPED*, 2016, pp. 130–135.

[14] J. Yang, C. Wang, Y. Cai, and Q. Zhou, "Power supply noise aware evaluation framework for side channel attacks and countermeasures," in *International Conference on Field-Programmable Technology, FPT*, 2014, pp. 161–166.

[15] J. Dofe, Z. Zhang, Q. Yu, C. Yan, and E. Salman, "Impact of power distribution network on power analysis attacks in three-dimensional integrated circuits," in *Proceedings of the on Great Lakes Symposium on VLSI, GLVLSI*, 2017, pp. 327–332.

[16] C. J. Alpert, D. P. Mehta, and S. S. Sapatnekar, Eds., *Handbook of Algorithms for Physical Design Automation*. CRC Press, 2008.

[17] H. Qian, S. R. Nassif, and S. S. Sapatnekar, "Power grid analysis using random walks," *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 24, no. 8, pp. 1204–1224, 2005.

[18] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

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

[20] M. Fawaz and F. N. Najm, "Accurate verification of RC power grids," in *Design, Automation & Test in Europe Conference & Exhibition, DATE*, 2016, pp. 814–817.

[21] J. Rabaey, *Low power design essentials*. Springer Science & Business Media, 2009.

[22] M. S. Gupta, J. L. Oatley, R. Joseph, G. Wei, and D. M. Brooks, "Understanding voltage variations in chip multiprocessors using a distributed power-delivery network," in *Design, Automation & Test in Europe Conference & Exhibition, DATE*, 2007, pp. 624–629.