IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 14 March 2016; revised 10 August 2016; accepted 15 October 2016.
Date of publication 21 October 2016; date of current version 6 June 2018.

Digital Object Identifier 10.1109/TETC.2016.2620382

Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures

WEIZE YU AND SELÇUK KÖSE, (Member, IEEE)

The authors are with the Department of Electrical Engineering, University of South Florida, Tampa FL 33620
CORRESPONDING AUTHOR: W. YU (weizeyu@mail.usf.edu)

ABSTRACT The security implications of on-chip voltage regulation on the effectiveness of various voltage/frequency scaling-based countermeasures such as random dynamic voltage and frequency scaling (RDVFS), random dynamic voltage scaling (RDVS), and aggressive voltage and frequency scaling (AVFS) are investigated. The side-channel leakage mechanisms of different on-chip voltage regulator topologies are mathematically analyzed and verified with circuit level simulations. Correlation coefficient between the input data and monitored power consumption of a cryptographic circuit is used as the security metric to compare the impact of different on-chip voltage regulators when implemented with the aforementioned countermeasures. As compared to a cryptographic circuit without countermeasure, the RDVFS technique implemented with an on-chip switched-capacitor voltage converter reduces the correlation coefficient over 80 percent and over 92 percent against differential and leakage power analysis attacks, respectively, through masking the leakage of the clock frequency and supply voltage information in the monitored power profile.

INDEX TERMS On-chip voltage regulation, voltage/frequency scaling, security metric, power analysis attacks

I. INTRODUCTION

Power analysis attacks (PAA) are powerful non-invasive side-channel attacks to obtain the secret key that is stored within cryptographic circuits in feasible time without significant cost [1]–[3]. Differential power analysis (DPA) and leakage power analysis (LPA) attacks are two types of PAA that exploit different characteristics of the side-channel leakage profile [4]–[10]. DPA attacks exploit the correlation between the input data and dynamic power consumption of cryptographic circuits [11]. Alternatively, LPA attacks utilize the correlation between the input data and leakage power dissipation of cryptographic circuits [8].

Dynamic power consumption of a cryptographic circuit is $P_{dyn} = \alpha f_c V_{dd}^2$ where f_c, V_{dd}, and α are, respectively, the clock frequency, supply voltage, and activity factor. Activity factor α is determined by the number of $0 \rightarrow 1$ transitions that occur in the cryptographic circuit under different input data [12]. To hide the actual dynamic power consumption P_{dyn} of a cryptographic circuit, different logic families are proposed to make the dynamic power consumption constant under different input data values. The wave dynamic differential logic (WDDL), which is a type of balanced logic gate, is proposed in [13], [14] to make the activity factor α constant regardless of the input data values. A switched-capacitor current equalizer-based countermeasure is proposed in [15] to achieve a constant P_{dyn} through discharging the residual charge in every switching cycle. However, DPA attacks countermeasures that hide the dynamic power dissipation of a cryptographic circuit by maintaining constant dynamic power consumption typically cause significant power/area/performance overhead [15], [16]. Alternatively, masking technique [17], [18] is an effective DPA attacks countermeasure that uses random intermediate data values to be inserted among the actual side channel leakage data to reduce the correlation between the input data and α. However, masking technique may also induce significant area overhead due to the large look-up table (LUT) when a large amount of random data is inserted [17], [18]. Please note that the effectiveness of masking-based countermeasures is directly correlated with the number of inserted data values. There is therefore a tradeoff between the LUT size and the effectiveness of the masking operation.

To minimize the information leakage through the power consumption profile, existing power management techniques that scale voltage and/or frequency at runtime have been tailored as a countermeasure against DPA attacks [4], [5], [11].

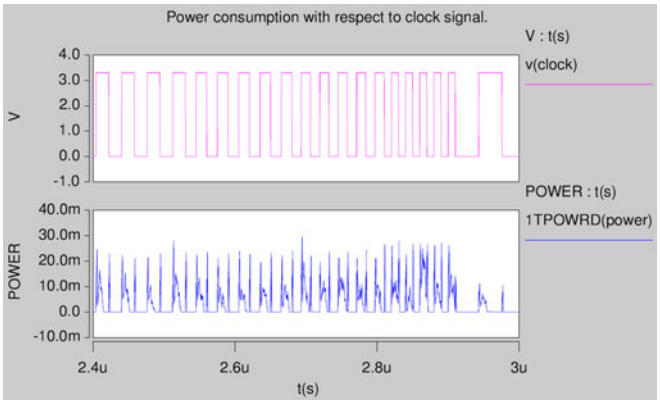


FIGURE 1. Relationship between the clock pulse and power consumption of a cryptographic circuit [5].

These voltage/frequency scaling (VFS) based countermeasures typically randomize the supply voltage and/or the frequency to break the one-to-one relationship between these parameters and the actual workload. Random dynamic voltage and frequency scaling (RDVFS) technique is one of the first VFS-based countermeasures against DPA attacks that reduces the power consumption while also increasing the security [4]. The working principle of the RDVFS technique is to randomly vary f_c and V_{dd} to mask the dynamic power variations from an attacker. RDVFS technique, however, has major security flaws since the clock frequency f_c can be leaked in the input power profile, as demonstrated in Figure 1 [5]. In other words, in a cryptographic circuit that utilizes conventional RDVFS, f_c becomes a linear function of V_{dd}, ($f_c = K_1.V_{dd} + B$ where K and B are the linear parameters) [5].

An attacker can therefore unriddle the fluctuations in the f_c and V_{dd} by solely monitoring the width of the spikes in the power consumption profile. After analyzing the pulse width of the monitored power consumption of the cryptographic circuit concurrently with the input data, a cryptographic circuit that houses the RDVFS technique can therefore be breached with negligible effort [5]. Another VFS-based countermeasure, random dynamic voltage scaling (RDVS) technique, is proposed in [5] to disrupt the linear relationship between f_c and V_{dd}. Unfortunately, this technique introduces significant power overhead to disrupt the relationship between f_c and V_{dd} where the security increases with higher power overhead. In order to minimize the power overhead while utilizing VFS as a countermeasure to secure a cryptographic circuit, Avirneni *et al.* [11] proposed the aggressive voltage and frequency scaling (AVFS) technique. In the AVFS technique, f_c and V_{dd} are independent so that an attacker can no longer estimate the changes in V_{dd} by solely monitoring the pulse width of the spikes in the monitored power dissipation profile. AVFS technique, however, increases the total chip area by about 3 percent due to redundant register duplication to minimize the circuit contamination delay [11].

Leakage power dissipation primarily has two components: subthreshold power leakage and gate-oxide power leakage [19]. These two power leakage components increase significantly with the continuous scaling of the silicon technology and the reduced supply voltage levels. Conventional LPA attacks are quite sensitive to measurement noise [20] and therefore have attracted relatively less attention as compared to DPA attacks. LPA attacks can still be quite effective if the clock frequency of the cryptographic circuit is lowered by the attacker and the analysis is reinforced with average sampling analysis [21]. Although there are no VFS-based countermeasures specifically tailored against LPA attacks, the leakage power dissipation is naturally affected by the voltage scaling techniques and the aforementioned VFS-based countermeasures are also partly effective against LPA attacks. Moreover, on-chip voltage regulation is becoming an essential part of cryptographic circuits, enabling faster and more power efficient voltage/frequency scaling (VFS) [22] with less than 1 percent area overhead [23]. In this paper, we investigate the security implications of three different on-chip voltage regulator topologies: low-dropout (LDO) regulator, buck converter, and switched-capacitor (SC) converter that can be implemented with countermeasures such as RDVFS, RDVS, and AVFS against both DPA and LPA attacks.

The rest of the paper is organized as follows. Security implications of the side-channel leakage mechanisms of three different on-chip voltage regulator topologies (LDO regulator, buck converter, and SC converter) are investigated in Section II. Security evaluations of on-chip voltage regulation with VFS technique against DPA and LPA attacks are provided, respectively, in Sections III and IV. The overhead of a cryptographic circuit that employs different techniques is discussed in Section V. Power attacks simulation is performed in Section VI, while conclusions are offered in Section VII.

II. ON-CHIP VOLTAGE REGULATION WITH VFS LOAD

Each voltage regulator topology has different input and output voltage/current characteristics. These differences change the way how different voltage regulators may leak critical information. In this section, the side-channel leakage mechanisms of three widely used on-chip voltage regulator topologies are investigated.

A. LOW-DROPOUT (LDO) REGULATOR WITH VFS LOAD

The relationship between the input current I_{in} and the load current I_{load} of an LDO regulator, as shown in Figure 2, is

$$I_{in} = I_R + I_{cap} + I_{load}, \tag{1}$$

where I_R and I_{cap} are, respectively, the resistor and capacitor current. To minimize the power conversion loss, the resistances of R_1 and R_2 are typically quite large, making the resistor current I_R negligible. Recently, output-capacitorless LDO voltage regulators have proliferated to reduce the area of LDO regulators [24], [25]. As a result, the capacitor current I_{cap} can also be ignored in our derivations without loss of generality. The relationship between I_{in} and I_{load} can therefore be approximated as

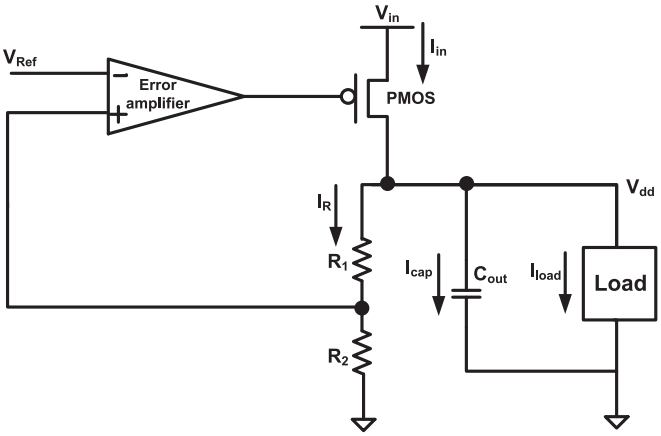


FIGURE 2. Schematic of a conventional LDO voltage regulator.

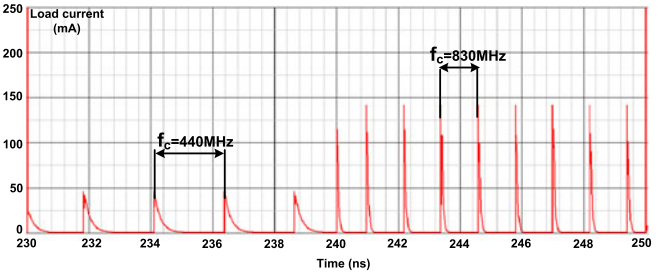
$$I_{in} \approx I_{load}. \tag{2}$$

Similarly, the relationship between the input power P_{in} and load current I_{load} can be denoted as

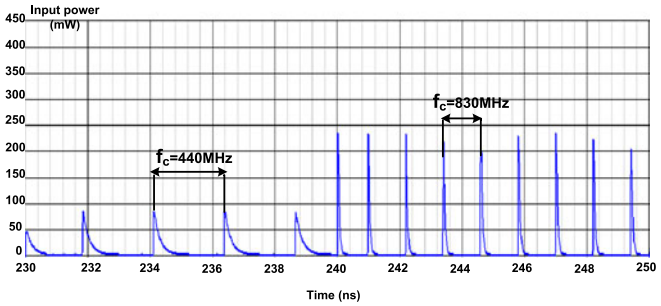
$$P_{in} \approx V_{in} I_{load}, \tag{3}$$

where V_{in} is the input voltage. Since there is an approximated linear relationship between P_{in} and I_{load}, certain characteristics of the clock frequency f_c can be estimated by an attacker by monitoring the input power profile.

The relationship between the load current and input power of an LDO voltage regulator is analyzed under a switching load where the clock frequency and supply voltage (f_c, V_{dd}) pair varies between (440 MHz, 0.8 V) and (830 MHz, 1.2 V) [11]. As shown in Figures 3(a) and 3(b), a linear relationship exists between the load current I_{load} and input power P_{in} of an LDO



(a)



(b)

FIGURE 3. (a) Transient load current profile of an LDO voltage regulator with VFS load. (b) Transient input power profile of an LDO voltage regulator with VFS load.

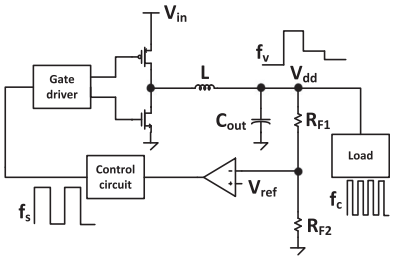


FIGURE 4. Schematic of a conventional buck converter.

regulator. An attacker can therefore determine the variations in f_c by monitoring the variations in P_{in} to nullify RDVFS technique under DPA attacks. The correlation between the input power and load current of an LDO regulator is so high that an attacker can visually extract the workload information without using any advanced analysis techniques.

B. BUCK CONVERTER WITH VFS LOAD

A buck converter, as shown in Figure 4, can have three different operating modes: continuous conduction mode (CCM), discontinuous conduction mode (DCM), and the boundary between CCM and DCM, (BCM). The relationships between the input voltage V_{in} and the output voltage V_{dd} of a buck converter (shown in Figure 4) operating in these three operating modes are

$$V_{dd} = \begin{cases} DV_{in}, & K_2 > 1-D, (CCM) \\ DV_{in}, & K_2 = 1-D, (BCM) \\ \frac{2V_{in}}{1+\sqrt{1+4K_2/D^2}}, & K_2 < 1-D, (DCM) \end{cases}, \tag{4}$$

where D is the duty cycle of the input switching signal. The critical value is $K_2 = 2Lf_s/R$ where L is the inductance of the filter inductor, f_s is the switching frequency, and R is the impedance of load. It is quite difficult for an attacker to analyze the variations of V_{dd} if the buck converter works in the DCM since the critical value K_2 would become uncertain due to the variations in the value of the load impedance R under different input data. An attacker can, however, still determine the changes in V_{dd} by monitoring the slope of the input power profile which is a strong function of the filter inductor current. When the inductor is in the charging state, the relationship between V_{dd} and the slope of input current S_1 is

$$S_1 = \frac{dI_{in}}{dt} = \frac{V_{in} - V_{dd}}{L}. \tag{5}$$

Similarly, the relationship between V_{dd} and the slope of input power S_2 is

$$S_2 = \frac{dP_{in}}{dt} = \frac{1}{L}(V_{in}^2 - V_{in}V_{dd}). \tag{6}$$

We investigate the possible leakage of critical workload information through the slope of the monitored input power signature via simulations. The relationship between S_2 and V_{dd} of a buck converter is analyzed under a switching load when the clock frequency and supply voltage (f_c, V_{dd}) pair for the switching load varies between (440 MHz, 0.8 V) and (830 MHz, 1.2 V). The switching frequency of buck

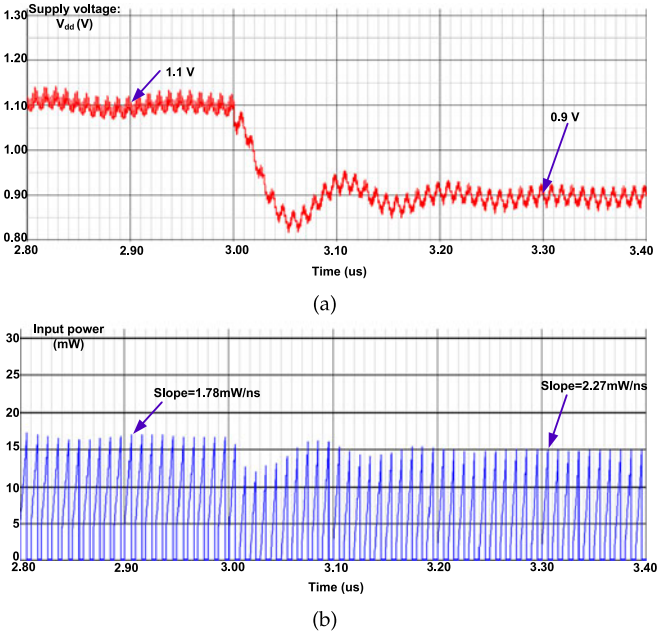


FIGURE 5. **(a) Transient supply voltage (output voltage) V_{dd} of a buck converter with VFS load. (b) Transient input power profile of a buck converter with VFS load.**

converter is typically around 100 MHz [26]. When V_{dd} drops from 1.1 to 0.9 V, S_2 increases from 1.78 to 2.27 mW/ns, as shown in Figure 5. An inversely linear relationship exists between S_2 and V_{dd}, as illustrated in Figure 6. This inversely linear relationship demonstrates the possible information leakage through the slope of input power profile that may nullify RDVFS technique under DPA attacks.

C. SWITCHED-CAPACITOR (SC) CONVERTER WITH VFS LOAD

An SC voltage converter utilizes one or multiple flying capacitors with a switch network where the flying capacitors

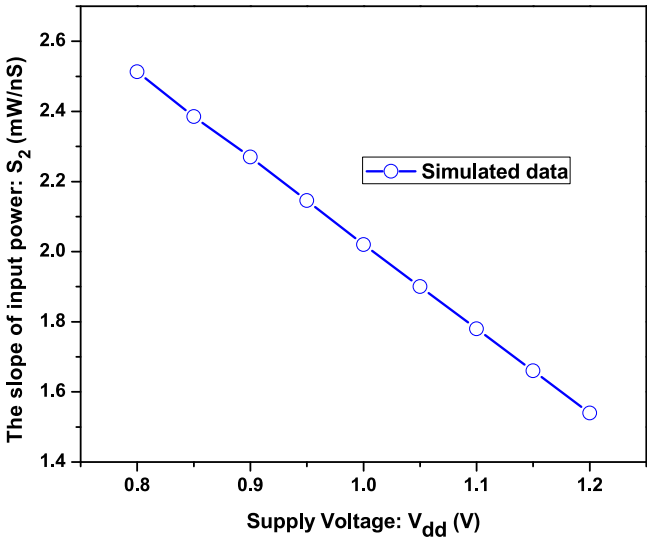


FIGURE 6. **Relationship between the supply voltage V_{dd} and the slope of the input power S_2 in the charging state.**

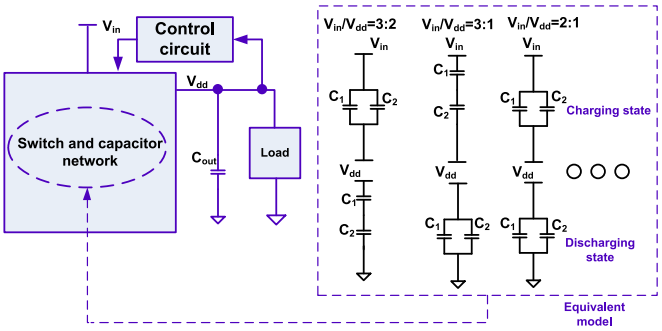


FIGURE 7. **Basic architecture of a switched-capacitor (SC) voltage converter.**

charge from the input voltage V_{in} and discharge to the output node periodically to generate a DC output voltage V_{dd}. The basic architecture of an SC voltage converter is illustrated in Figure 7. Different voltage conversion ratios can be obtained by modifying the connections of the switches and capacitors within an SC converter.

The relationship between the switching frequency f_s and the load current I_{load} of an SC converter is [27]

$$A(V_{dd})f_s = I_{load}, \tag{7}$$

where $A(V_{dd})$ is a function of the supply voltage V_{dd}. Typically, the switching frequency of an SC converter is around 100 MHz [22], which is much lower than the clock frequency f_c of a typical S-box which can be around 500 MHz [11]. Therefore, in a single switching period of an SC converter, several spikes occur due to the high clock frequency of the transistors. Assuming that the number of the transitions of load power within a switching period is M, the relationship between f_s and f_c can be written as

$$\begin{aligned} f_s &= \frac{1}{A(V_{dd})} I_{load} = \frac{1}{A(V_{dd})} \frac{P_{dyn}}{V_{dd}} \\ &= \frac{1}{A(V_{dd})} \frac{\sum_{i=1}^{M} \alpha_i f_c V_{dd}^2}{V_{dd}} = \frac{f_c V_{dd}}{A(V_{dd})} \sum_{i=1}^{M} \alpha_i, \end{aligned} \tag{8}$$

where P_{dyn} is the dynamic power consumption of a cryptographic circuit and $\alpha_i (i = 1, 2, \ldots)$ is the corresponding activity factor. While the value of $\sum_{i=1}^{M} \alpha_i$ is determined by the input data, the switching frequency f_s, which may be exploited to obtain critical information about f_c, is masked by scrambling the monitored activity factor $\sum_{i=1}^{M} \alpha_i$. An SC converter with a variable $\sum_{i=1}^{M} \alpha_i$ is analyzed under a switching load circuit with 670 MHz clock frequency and 1 V supply voltage [11] while $\sum_{i=1}^{M} \alpha_i$ varies between 50 and 400 pF. As shown in Figure 8, the switching frequency f_s is successfully changed by varying $\sum_{i=1}^{M} \alpha_i$ in input power profile with a constant f_c.

When the SC converter is in the charging state, the equality denoting the charging of the flying capacitor should be satisfied as

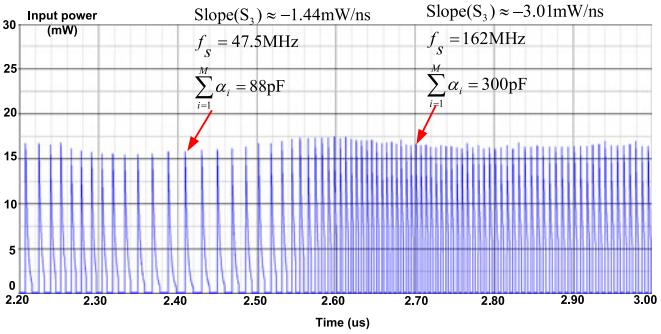


FIGURE 8. Transient input power of an SC converter with variable $\sum_{i=1}^{M} \alpha_i$.

$$\frac{V_{in} - V_1(t)}{R(V_{dd})} = C_{top}(V_{dd}) \frac{dV_1(t)}{dt}, \tag{9}$$

where $C_{top}(V_{dd})$ is the capacitance of the top plate in the equivalent flying capacitor, $R(V_{dd})$ is the equivalent series resistance, and $V_1(t)$ is the voltage of the top plate of the equivalent flying capacitor. The expression for $V_1(t)$, the input power in charging state $P_{in}(t)$, and the slope of input power in charging state S_3, respectively, are

$$V_1(t) = V_1(0) + (V_{in} - V_1(0))(1 - e^{-t/R(V_{dd})C_{top}(V_{dd})}), \tag{10}$$

$$P_{in}(t) = V_{in} \frac{dV_1(t)}{dt} = \frac{V_{in}^2 - V_{in}V_1(0)}{R(V_{dd})C_{top}(V_{dd})} e^{-t/R(V_{dd})C_{top}(V_{dd})}, \tag{11}$$

$$S_3 = \frac{dP_{in}(t)}{dt} = -\frac{V_{in}^2 - V_{in}V_1(0)}{R^2(V_{dd})C_{top}^2(V_{dd})} e^{-t/R(V_{dd})C_{top}(V_{dd})}, \tag{12}$$

where $V_1(0)$ is the voltage of the top plate in the equivalent flying capacitor before charging. To prevent the leakage of the supply voltage V_{dd} information through the input power profile from the slope of the input power S_3 in the charging state, the variations of the supply voltage (reflected by $R(V_{dd})C_{top}(V_{dd})$) and the the variations of load power induced by different input data (reflected by $V_1(0)$) are also scrambled together. As shown in Figure 8, S_3 also depends on the variation of $\sum_{i=1}^{M} \alpha_i$ in input power profile when V_{dd} is fixed.

III. SECURITY EVALUATION OF ON-CHIP VOLTAGE REGULATION WITH VFS TECHNIQUE AGAINST DPA ATTACKS

Countermeasures against side-channel attacks either insert noise to the side-channel leakage or reduce the critical signal in the side-channel leakage. VFS-based countermeasures typically insert noise to the power consumption profile to increase the number of measurements that an attacker needs to perform for a successful attack. As mentioned in the *Introduction*, the dynamic power consumption of cryptographic circuits P_{dyn} is

$$P_{dyn} = \alpha f_c V_{dd}^2. \tag{13}$$

After taking logarithm of both of the sides, (13) can be written as

$$log(P_{dyn}) = log(\alpha) + log(f_c) + 2log(V_{dd}), \tag{14}$$

where $log(\alpha)$ represents the side-channel signal related with DPA attacks. The amount of uncertain noise $N_{j,k}(f_c, V_{dd})$ that is inserted through different countermeasures that employ three different types of voltage regulators varies significantly, as shown in Table 1. When a cryptographic circuit employs the AVFS technique with an SC converter, the inserted noise would contain both random f_c and random V_{dd} due to the independent relationship between f_c and V_{dd}. When a cryptographic circuit employs the RDVS technique with an SC converter, the inserted noise would only contain random V_{dd} as the clock frequency f_c is fixed. The inserted noise would be zero when the RDVFS technique employs an LDO regulator or a buck converter as either f_c or V_{dd} would leak through the input power profile. By utilizing the correlation between f_c and V_{dd}, the inserted noise in the side-channel through the countermeasures may be eliminated. However, if a cryptographic circuit employs an SC converter with the RDVFS technique, the uncertain noise would contain both the random clock frequency and supply voltage. As compared to the AVFS technique, a linear relationship exists between the clock frequency f_c and supply voltage V_{dd} when the RDVFS technique employs an SC converter. The clock frequency can therefore be denoted as a function of the supply voltage (i.e., $f_c = F(V_{dd}) = K_1.V_{dd} + B$ where $K_1 = 975$ MHz/V and $B = -340$ MHz when $V_{dd} \in [0.8\text{ V}, 1.2\text{ V}]$ and $f_c \in [440\text{ MHz}, 830\text{ MHz}]$ [11]).

TABLE 1. Inserted Noise $N_{j,k}(f_c, V_{dd}), (j, k = 1, 2, 3)$ into the Power Consumption Profile of a Cryptographic Circuit Through Countermeasures That Employ Different Voltage Regulators Against DPA Attacks.

Technique \ Regulator	LDO regulator	Buck converter	SC converter
RDVFS	$N_{1,1}(f_c, V_{dd}) = 0$	$N_{1,2}(f_c, V_{dd}) = 0$	$N_{1,3}(f_c, V_{dd}) = \log(F(V_{dd})) + 2\log(V_{dd})$
RDVS	$N_{2,1}(f_c, V_{dd}) = 2\log(V_{dd})$	$N_{2,2}(f_c, V_{dd}) = 0$	$N_{2,3}(f_c, V_{dd}) = 2\log(V_{dd})$
AVFS	$N_{3,1}(f_c, V_{dd}) = 2\log(V_{dd})$	$N_{3,2}(f_c, V_{dd}) = \log(f_c)$	$N_{3,3}(f_c, V_{dd}) = \log(f_c) + 2\log(V_{dd})$

A. SECURITY OF ON-CHIP VOLTAGE REGULATION WITH TRUE RANDOM VFS TECHNIQUE AGAINST DPA ATTACKS

When all of the aforementioned techniques are true random, the clock frequency f_c and supply voltage V_{dd} would have uniform distributions. Let's assume that V_{DD1} and V_{DD2} are, respectively, the minimum and maximum voltage values that V_{dd} can operate. Similarly, f_1 and f_2 are, respectively, the minimum and maximum frequency values that f_c can take. When the number of discrete values that V_{dd} can take within $[V_{DD1}, V_{DD2}]$ is N, the resolution of supply voltage ΔV_{dd} and ith, $(i = 1, 2, 3, \ldots, N)$ possible value $V_{dd,i}$ within $[V_{DD1}, V_{DD2}]$ can be, respectively, denoted as

$$\Delta V_{dd,i} = \frac{V_{DD2} - V_{DD1}}{N-1}, \tag{15}$$

$$V_{dd,i} = \frac{(i-1) \times (V_{DD2} - V_{DD1})}{N-1} + V_{DD1}. \tag{16}$$

Similarly, assuming that frequency can get N different values within $[f_1, f_2]$, the ith possible value $f_{c,i}$ can be denoted as

$$f_{c,i} = \frac{(i-1) \times (f_2 - f_1)}{N-1} + f_1. \tag{17}$$

If the frequency[1] of the voltage scaling operation is f_v, the mean value of the inserted noise $E(N_{j,k}(f_c, V_{dd}))$ for on-chip voltage regulation based and uniformly distributed RDVFS technique ($j = 1$), RDVS technique ($j = 2$), and AVFS technique ($j = 3$), respectively, are

$$E(N_{1,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^{N} \left[\frac{f_{c,i}}{f_v}\right]} \sum_{i=1}^{N} \left[\frac{f_{c,i}}{f_v}\right] N_{1,k}(f_{c,i}, V_{dd,i}), \tag{18}$$

$$E(N_{2,k}(f_c, V_{dd})) = \frac{1}{N} \sum_{i=1}^{N} N_{2,k}(f_c, V_{dd,i}), \tag{19}$$

$$E(N_{3,k}(f_c, V_{dd})) = \frac{1}{N \sum_{l=1}^{N} \left[\frac{f_{c,l}}{f_v}\right]} \sum_{l=1}^{N} \sum_{i=1}^{N} \left[\frac{f_{c,l}}{f_v}\right] N_{3,k}(f_{c,l}, V_{dd,i}). \tag{20}$$

The corresponding variance of the inserted noise $Var(N_{j,k}(f_c, V_{dd}))$ can be denoted, respectively, as

$$Var(N_{1,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^{N} \left[\frac{f_{c,i}}{f_v}\right]} \sum_{i=1}^{N} \left[\frac{f_{c,i}}{f_v}\right] (N_{1,k}(f_{c,i}, V_{dd,i}) - E(N_{1,k}(f_c, V_{dd})))^2, \tag{21}$$

$$Var(N_{2,k}(f_c, V_{dd})) = \frac{1}{N} \sum_{i=1}^{N} (N_{2,k}(f_c, V_{dd,i}) - E(N_{2,k}(f_c, V_{dd})))^2, \tag{22}$$

[1]Since on-chip voltage regulator can generate variable supply voltage levels V_{dd}, we assume that the frequency of the voltage scaling is f_v.

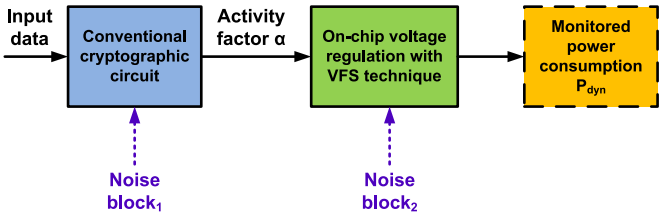


FIGURE 9. Relationship between the input data and monitored power consumption P_{dyn} of a cryptographic circuit that employs an on-chip voltage regulation based VFS technique (*Conventional cryptographic circuit* represents a cryptographic circuit without any countermeasure).

$$Var(N_{3,k}(f_c, V_{dd})) = \frac{1}{N \sum_{i=1}^{N} \left[\frac{f_{c,l}}{f_v}\right]} \times \sum_{l=1}^{N} \sum_{i=1}^{N} \left[\frac{f_{c,l}}{f_v}\right] (N_{3,k}(f_{c,l}, V_{dd,i}) - E(N_{3,k}(f_c, V_{dd})))^2. \tag{23}$$

A cryptographic circuit that employs on-chip voltage regulation based VFS technique can be modeled with two separate noise insertion blocks (noise block$_1$ and noise block$_2$), as shown in Figure 9. Accordingly, the correlation coefficient between the input data and monitored power consumption P_{dyn} of that cryptographic circuit can be represented with the correlation between the input data and monitored power dissipation of those two noise insertion blocks. The signal-to-noise ratio (SNR) at the output of the noise block$_2$ $SNR''_{j,k}$ can be denoted as

$$SNR''_{j,k} = \frac{Var(log(\alpha))}{Var(N_{j,k}(f_c, V_{dd}))}, \tag{24}$$

where $Var(log(\alpha))$ represents the variance of $log(\alpha)$. The correlation coefficient $\gamma''_{j,k}$ between the activity factor α and monitored power dissipation P_{dyn} of the cryptographic circuit can be obtained as [12]

$$\gamma''_{j,k} = \frac{1}{\sqrt{1 + \frac{1}{SNR''_{j,k}}}}. \tag{25}$$

Correlation coefficient between the input data and monitored power dissipation of the cryptographic circuit is widely used as a metric to evaluate the level of security [8], [12], [29]. Since the operations that take place in the noise block$_1$ are independent of the operations that take place in the noise block$_2$, the correlation coefficient $\gamma_{j,k}$ between the input data and monitored power consumption can be written as [12]

$$\gamma_{j,k} = \gamma' \times \gamma''_{j,k}, \tag{26}$$

where γ' is the correlation coefficient between the input data and activity factor. Therefore, $(1 - \gamma''_{j,k})$ can be defined as the *correlation coefficient reduction ratio* of a cryptographic

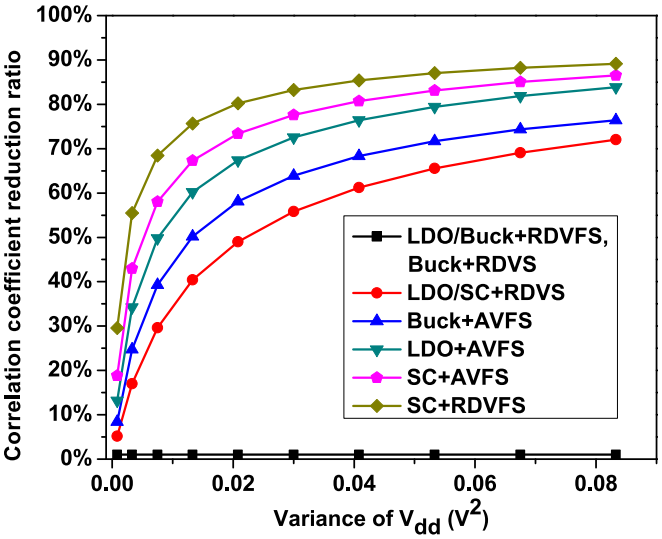


FIGURE 10. Variance of supply voltage V_{dd} versus the correlation coefficient reduction ratio of an-S-box that employs different VFS-based countermeasures (VFS techniques conform to uniform distribution and $N = 50$. Since a high f_v does not enhance the variance of noise induced by VFS technique, as explained in [5], [11], a moderate voltage scaling frequency of $f_v = 10$ MHz [28] is used for the security analysis to not increase the system design complexity).

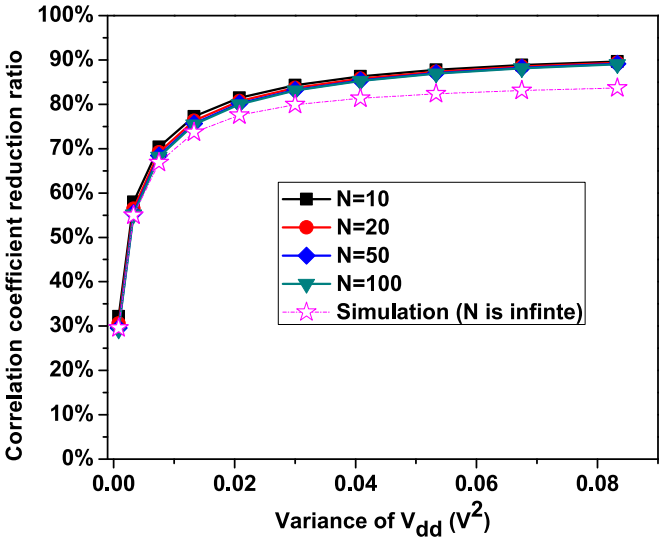


FIGURE 11. Variance of the supply voltage V_{dd} versus the correlation coefficient reduction ratio for an S-box that employs RDVFS technique with an SC converter with various possible (f_c, V_{dd}) pairs.

circuit that employs a VFS-based countermeasure with on-chip voltage regulation.

A low power and small area substitution-box (S-box) from [30] is implemented at the 130nm CMOS technology node and utilized as the cryptographic circuit under attack. The correlation coefficient reduction ratio that is achieved when different countermeasures are employed to protect the S-box is shown in Figure 10. The S-box that employs an SC converter based RDVFS technique exhibits the highest correlation coefficient reduction ratio under the same variance of V_{dd}. The security implications of the number of (f_c, V_{dd}) pairs N are investigated. As shown Figure 11, the number of possible (f_c, V_{dd}) pairs N has a negligible impact on the correlation coefficient reduction ratio of an S-box that employs RDVFS technique with an SC converter. Additionally, when the variance of V_{dd} exceeds $0.04V^2$, the correlation coefficient reduction ratio of an S-box that employs RDVFS technique with an SC converter starts converging, as shown in Figure 10. A higher variance of V_{dd} causes increased performance degradation for a cryptographic circuit that employs RDVFS technique [11]. Selecting the variance of V_{dd} as 0.04 V^2, therefore, provides a reasonable design tradeoff between security and performance. When the variance of V_{dd} is equal to $0.04V^2$, an S-box that employs RDVFS technique with an SC converter performs best against DPA attacks as compared to an S-box employs other techniques without significant performance degradation.

Since a true random VFS technique may be difficult to implement in practice, a statistically normally distributed VFS technique is used in the modern processors [31]–[33]. The detail security analysis of on-chip voltage regulation with normally distributed VFS technique against DPA attacks can be found in Appendix C.

IV. SECURITY EVALUATION OF ON-CHIP VOLTAGE REGULATION WITH VFS TECHNIQUE AGAINST LPA ATTACKS

A leakage power analysis (LPA) attack is a type of side-channel attack, which is utilized by an attacker to leak the secret key by exploiting the correlation between the input data and leakage power dissipation of a cryptographic circuit [8]. The side-channel leakage current of a cryptographic circuit I_{leak} can be denoted as [8]

$$I_{leak} = \omega I_H + (m - \omega) I_L, \tag{27}$$

where ω is the hamming weight of input data and m is the number of bits in the input data. $I_H(I_L)$ is the leakage current when the input bit is high (low). Since $I_H(I_L)$ is a function of the supply voltage V_{dd} [34], the leakage power dissipation P_{leak} of a cryptographic circuit can be written as

$$\begin{aligned} P_{leak} &= V_{dd} I_{leak} \\ &= V_{dd}(\omega I_H(V_{dd}) + (m - \omega) I_L(V_{dd})) \\ &= V_{dd} I_{leak,0} K(V_{dd}), \end{aligned} \tag{28}$$

where $I_{leak,0}$ is the component of leakage current which is independent of the supply voltage V_{dd} and $K(V_{dd})$ is the component of leakage current which is strongly correlated with V_{dd}.

In sub-micro CMOS integrated circuits (ICs), the relationship between the leakage current of the CMOS ICs and supply voltage V_{dd} can be approximated as an exponent relationship ($I_{leak} = I_{leak,0} K(V_{dd}) \approx I_{leak,0} exp(a V_{dd})$) [34]. In order to determine the value of the parameter a, two different

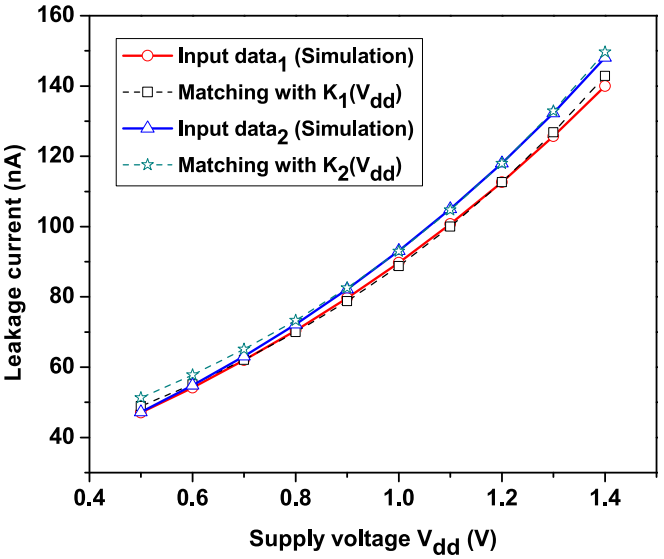


FIGURE 12. Supply voltage V_{dd} versus leakage current of an S-box implemented in 130 nm CMOS technology under two different input data.

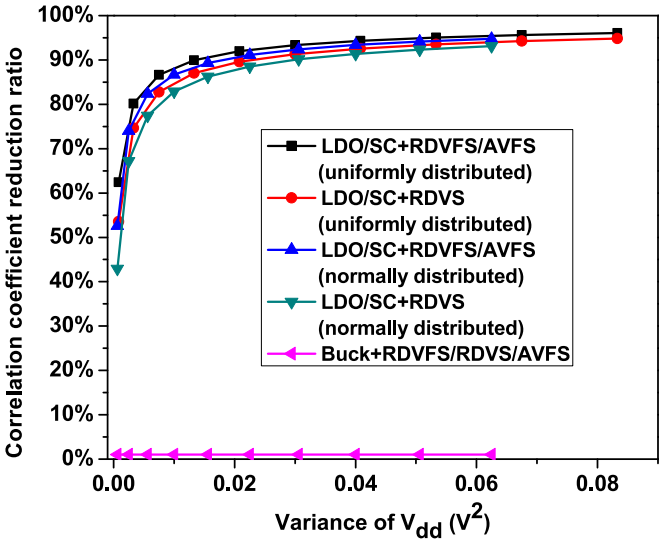


FIGURE 13. Variance of supply voltage V_{dd} versus the correlation coefficient reduction ratio of an S-box that employs different countermeasures ($f_v = 10$ MHz, and $N = 50$).

input data patterns (input data$_1$ and input data$_2$) are applied to a 130 nm CMOS based S-box [30]. The simulated relationship between the leakage current and supply voltage V_{dd} is shown in Figure 12. We use two different exponent functions $K_1(V_{dd}) = b_1 exp(aV_{dd})$ and $K_2(V_{dd}) = b_2 exp(aV_{dd})$ to curve-fit the relationship between the leakage current and supply voltage V_{dd} induced by input data$_1$ and input data$_2$, respectively. After fitting as shown in Figure 12, the expressions of $K_1(V_{dd})$ and $K_2(V_{dd})$ can be respectively determined as

$$K_1(V_{dd}) = 27 \times exp(1.19 \times V_{dd}) \approx 27K(V_{dd}), \quad (29)$$

$$K_2(V_{dd}) = 28.29 \times exp(1.19 \times V_{dd}) \approx 28.29K(V_{dd}). \quad (30)$$

Therefore, the leakage power dissipation of the S-box P_{leak} can be denoted as

$$\begin{aligned} P_{leak} &= V_{dd} I_{leak,0} K(V_{dd}), \\ &\approx V_{dd} \times I_{leak,0} \times exp(1.19 \times V_{dd}). \end{aligned} \quad (31)$$

After taking logarithm of both sides, (31) becomes

$$log(P_{leak}) \approx log(I_{leak,0}) + log(V_{dd}) + 1.19V_{dd}, \quad (32)$$

where $log(I_{leak,0})$ is the side-channel signal which may provide useful information under an LPA attack. The characteristics of the inserted noise $M_{j,k}(V_{dd})$ to an S-box through different countermeasures against LPA attacks are listed in Table 2. Since a buck converter leaks the supply voltage V_{dd} from the slope of input power, the uncertain noise $M_{j,2}(V_{dd})$ that is inserted by a buck converter based VFS technique becomes zero.

As shown in Figure 13, an S-box that employs the RDVFS technique with an SC converter can achieve a correlation coefficient reduction ratio of over 90 percent when the variance of supply voltage V_{dd} is greater than 0.04 V^2.

V. OVERHEAD ANALYSIS

The power overhead of several VFS-based countermeasures with on-chip voltage regulation is summarized in Table 3. An S-box [30] that houses an SC voltage converter exhibits the highest correlation coefficient reduction ratio (CCRR) of about 85.41 percent (80.94 percent) with true random (normally distributed) RDVFS technique under DPA attacks and about 94.3 percent (92.41 percent) with true random (normally distributed) RDVFS technique under LPA attacks. The corresponding dynamic power (D-Power) consumption of the S-box is $0.746X_d$ ($0.692X_d$) with true random (normally distributed) RDVFS technique whereas the corresponding leakage power (L-Power) dissipation is $0.7116X_l$ ($0.6948X_l$) with true random (normally distributed) RDVFS technique.

TABLE 2. Inserted Noise $M_{j,k}(V_{dd}), (j,k = 1,2,3)$ into the Power Consumption Profile of a Cryptographic Circuit Through Countermeasures That Employ Different Voltage Regulators Against LPA Attacks.

Regulator / Technique	LDO regulator	Buck converter	SC converter
RDVFS	$M_{1,1}(V_{dd}) = \log(V_{dd}) + 1.19V_{dd}$	$M_{1,2}(V_{dd}) = 0$	$M_{1,3}(V_{dd}) = \log(V_{dd}) + 1.19V_{dd}$
RDVS	$M_{2,1}(V_{dd}) = \log(V_{dd}) + 1.19V_{dd}$	$M_{2,2}(V_{dd}) = 0$	$M_{2,3}(V_{dd}) = \log(V_{dd}) + 1.19V_{dd}$
AVFS	$M_{3,1}(V_{dd}) = \log(V_{dd}) + 1.19V_{dd}$	$M_{3,2}(V_{dd}) = 0$	$M_{3,3}(V_{dd}) = \log(V_{dd}) + 1.19V_{dd}$

TABLE 3. Correlation Coefficient Reduction Ratio (CCRR), Dynamic Power (D-Power) Consumption, and Leakage Power (L-Power) Consumption of an S-Box That Houses On-Chip Voltage Regulators Implemented with True Random and Normally Distributed VFS-based Countermeasures Against DPA and LPA Attacks (Supply Voltage Range $V_{DD2} - V_{DD1} = 0.7V$). X_d and X_l are, Respectively, the Dynamic and Leakage Power Consumption of an S-box Without Any Countermeasure.

	DPA attacks				LPA attacks			
	True random		Normally distributed		True random		Normally distributed	
	CCRR	D-Power	CCRR	D-Power	CCRR	L-Power	CCRR	L-Power
LDO+RDVFS	0	$0.746X_d$	0	$0.692X_d$	94.3%	$0.7116X_l$	92.41%	$0.6948X_l$
Buck+RDVFS	0	$0.746X_d$	0	$0.692X_d$	0	$0.7116X_l$	0	$0.6948X_l$
SC+RDVFS	85.41%	$0.746X_d$	80.94%	$0.692X_d$	94.3%	$0.7116X_l$	92.41%	$0.6948X_l$
LDO+RDVS	61.2%	$2.0391X_d$	51.07%	$2.0195X_d$	92.56%	$2.7274X_l$	90.14%	$2.6820X_l$
Buck+RDVS	0	$2.0391X_d$	0	$2.0195X_d$	0	$2.7274X_l$	0	$2.6820X_l$
SC+RDVS	61.2%	$2.0391X_d$	51.07%	$2.0195X_d$	92.56%	$2.7274X_l$	90.14%	$2.6820X_l$
LDO+AVFS	76.43%	$0.6097X_d$	69.07%	$0.5427X_d$	94.3%	$0.7116X_l$	92.41%	$0.6948X_l$
Buck+AVFS	68.32%	$0.6097X_d$	59.52%	$0.5427X_d$	0	$0.7116X_l$	0	$0.6948X_l$
SC+AVFS	80.74%	$0.6097X_d$	77.31%	$0.5427X_d$	94.3%	$0.7116X_l$	92.41%	$0.6948X_l$

X_d represents the dynamic power consumption of an S-box without any countermeasure and X_l is the leakage power dissipation of an S-box without any countermeasure. A detailed explanation of power consumption overhead of different techniques tabulated in Table 3 can be found in Appendix B.

There are two main sources of the additional area overhead that need to be considered for an S-box that employs a VFS technique with an on-chip voltage regulator: area overhead induced by on-chip voltage regulator and area overhead induced by VFS technique. Since an on-chip voltage regulator utilized to generate fast VFS [22] causes less than 1 percent area overhead [23], the area overhead induced by on-chip voltage regulator can be neglected. The VFS techniques, RDVFS and RDVS, would not cause extra area overhead based on the analysis provided in [5], [11]. AVFS technique, however, has a 3 percent area overhead induced by the redundant register duplication to minimize the circuit contamination delay [11].

VI. DPA AND LPA ATTACK SIMULATIONS

DPA and LPA attacks are performed in Cadence on two different S-boxes that are implemented at 130 nm CMOS technology: one S-box [30] without any countermeasure and another S-box [30] that employs a true random RDVFS technique with an SC converter. As shown in Figure 14, the correct key[2] of the S-box without countermeasure can be obtained by performing DPA attacks or LPA attacks after inputting 1,000 plaintexts. However, the correlation coefficient of the correct key under LPA attacks is higher than the correlation coefficient of the correct key under DPA attacks. This can be interpreted as LPA attacks are able to leak a higher amount of critical information from the S-box as compared to DPA attacks when there is no countermeasure.

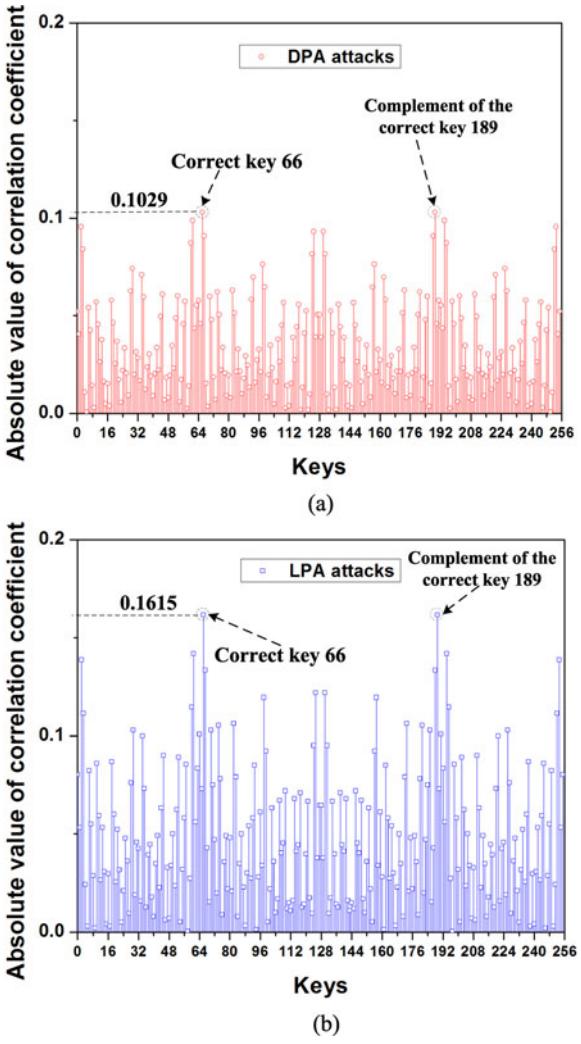


FIGURE 14. Absolute value of the correlation coefficient versus all of the possible keys after inputting 1,000 plaintexts with the hamming-weight model. (a) An S-box without countermeasure under DPA attacks. (b) An S-box without countermeasure under LPA attacks.

[2]In hamming-weight model, the correlation coefficient distinction between the correct key and complement of the correct key is the polarity [8]. The correlation coefficient of the correct key is positive, while the correlation coefficient of the complement of the correct key is negative. In order to make the highest correlation coefficient more obvious, in Figures 14 and 15, we normalized all of the correlation coefficients with absolute values.

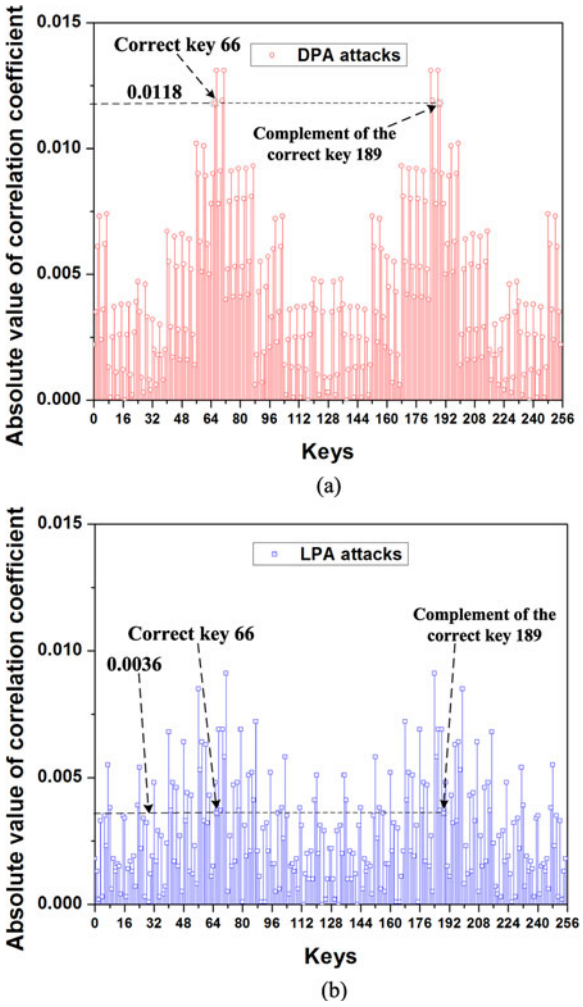


FIGURE 15. Absolute value of correlation coefficient versus all the possible keys after inputting 1 million plaintexts with hamming-weight model ($V_{DD2} - V_{DD1} = 0.7V$). (a) An S-box that employs RDVFS technique with an SC converter under DPA attacks. (b) An S-box that employs RDVFS technique with an SC converter under LPA attacks.

In the second experiment, DPA and LPA attacks are performed against an S-box that employs a true random RDVFS technique with an SC converter. After inputting one million plaintexts, neither DPA nor LPA attacks are able to fetch the correct key as shown in Figure 15. However, the correlation coefficient of the correct key under LPA attacks is much lower than the correlation coefficient of the correct key under DPA attacks when RDVFS technique with an SC converter is enabled. This behavior indicates that LPA attacks are more sensitive to noise.

After inputting one million plaintexts to the S-box that employs a true random RDVFS technique with an SC converter, the correlation coefficient reduction ratio of the correct key is 88.53 percent (97.77 percent) under DPA (LPA) attacks. These values are higher than the theoretical values of 85.41 percent (94.3 percent) which are listed in Table 3. An intuitive explanation is provided below.

- The theoretical values tabulated in Table 3 are the correlation coefficient reduction ratios of an S-box that employs different countermeasures assuming that the attacker can apply any number of attacks until the secret key within the S-box is obtained (i.e., more than one million plaintexts). However, in DPA and LPA attack simulations, we applied one million plaintexts and the S-box that employs a true random RDVFS technique with an SC converter could not be cracked after inputting one million plaintexts as shown in Figure 15. This indicates the presence of significant amount of noise in the S-box. If more plaintexts are applied to filter the noise, the correlation coefficient of the correct key would be enhanced and the correlation coefficient reduction ratio would decrease, approaching the theoretical value.

VII. CONCLUSION

The security implications of different on-chip voltage regulator topologies implemented within various voltage/frequency scaling-based countermeasures such as RDVFS, RDVS, and AVFS techniques against power analysis attacks are investigated. The side-channel leakage mechanisms of three widely used on-chip voltage regulator topologies are investigated. The security impact of on-chip voltage regulators is evaluated based on the correlation coefficient between the input data and monitored power consumption of a cryptographic circuit. Correlation coefficient reduction ratio is proposed to simplify the security evaluation. RDVFS technique implemented with a switched-capacitor voltage converter can reduce correlation coefficient over 80 percent (92 percent) against DPA (LPA) attacks and the measurement-to-disclose (MTD) value is enhanced over 1 million by masking the clock frequency, supply voltage, and dynamic power consumption information from a malicious attacker.

APPENDIX A
DETAILED EXPLANATION OF TABLES 1 AND 2

As demonstrated in Section II, the parameters that leak due to the usage of three different voltage regulators with a VFS load can be summarized in Table 4 a. As explained in Section II, an LDO regulator leaks the information regarding the clock frequency f_c of the VFS load, while a buck converter leaks information regarding the supply voltage V_{dd} of the VFS load. However, an SC converter with VFS load prevents the leakage of f_c and V_{dd} as demonstrated in Section II-C.

The inserted noise induced by three different VFS techniques against DPA attacks is shown in Table 4 b. For RDVFS technique against DPA attacks, the inserted noise can be written as $log(f_c) + 2log(V_{dd})$ based on Equation (14). Since, there is a one-to-one linear relationship between f_c and V_{dd} in RDVFS technique, the relationship between f_c and V_{dd} can be denoted as $f_c = F(V_{dd})$ or $V_{dd} = F^{-1}(f_c)$ where F^{-1} is the inverse function of F. Therefore, the inserted noise induced by RDVFS technique against DPA attacks also can be

TABLE 4. (a) Parameter Leakage of Three Different Voltage Regulators with VFS Load. (b) Inserted Noise Induced by Three Different VFS Techniques Against DPA Attacks. (c) Inserted Noise Induced by Three Different VFS Techniques Against LPA Attacks.

(a)

	LDO regulator	Buck Converter	SC converter
Leakage	f_c	V_{dd}	0

(b)

	RDVFS	RDVS	AVFS
Noise	$\log(F(V_{dd})) + 2\log(V_{dd})$ or $\log(f_c) + 2\log(F^{-}(f_c))$	$2\log(V_{dd})$	$\log(f_c) + 2\log(V_{dd})$

(c)

	RDVFS	RDVS	AVFS
Noise	$\log(V_{dd}) + 1.19V_{dd}$	$\log(V_{dd}) + 1.19V_{dd}$	$\log(V_{dd}) + 1.19V_{dd}$

written as $log(F(V_{dd})) + 2log(V_{dd})$ or $log(f_c) + 2log(F^{-1}(f_c))$. For RDVS technique against DPA attacks, since clock frequency f_c is fixed, from Equation (14), the inserted noise can be written as $2log(V_{dd})$. However, for AVFS technique against DPA attacks, from Equation (14), the inserted noise is $log(f_c) + 2log(V_{dd})$. Unlike RDVFS technique, the clock frequency f_c is independent of the supply voltage V_{dd} in AVFS technique, therefore, f_c can not be denoted as a function of V_{dd} in AVFS technique.

As shown in Table 1, when an LDO regulator is implemented within different VFS techniques against DPA attacks, the VFS noise related to f_c can be eliminated due to the leakage of f_c. Similarly, for a buck converter implemented within different VFS techniques against DPA attacks, the VFS noise related to V_{dd} can be eliminated due to the leakage of V_{dd}. Since an SC converter implemented within different VFS techniques against DPA attacks prevents the leakage of f_c and V_{dd}, the VFS noise is retained without reduction.

The inserted noise induced by three different VFS techniques against LPA attacks is shown in Table 4 c. Since all of the VFS techniques (RDVFS, RDVS, and AVFS) contain the information of the V_{dd} scaling as demonstrated in Equation (32), the inserted noise from all of the VFS techniques against LPA attacks can be written as $log(V_{dd}) + 1.19V_{dd}$. Since a buck converter with a VFS load leaks the supply voltage V_{dd}, the inserted noise from a buck converter with different VFS techniques related with V_{dd} against LPA attacks can be eliminated, as tabulated in Table 2.

APPENDIX B

DETAILED ANALYSIS OF POWER CONSUMPTION OVERHEAD OF DIFFERENT COUNTERMEASURES

The dynamic power dissipation P_{dyn} of the S-box mentioned in the paper is

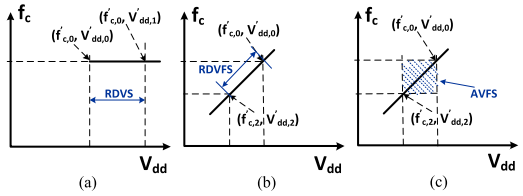


FIGURE 16. Supply voltage V_{dd} versus clock frequency f_c under different VFS techniques. (a) RDVS technique. (b) RDVFS technique. (c) AVFS technique.

$$P_{dyn} = \alpha f_c V_{dd}^2. \tag{33}$$

In Figure 16(a), $(f'_{c,0}, V'_{dd,0})$ is the clock frequency and supply voltage of an S-box that does not employ a VFS technique. When the S-box employs RDVS technique as shown in Figure 16(a), the supply voltage becomes higher than $V'_{dd,0}$, increasing the dynamic power dissipation of the S-box as compared to the dynamic power dissipation of the S-box without a VFS technique.

When an S-box employs RDVFS technique as shown in Figure 16(b), the clock frequency and supply voltage can be lower than $f'_{c,0}$ and $V'_{dd,0}$, respectively. As a result, the dynamic power dissipation of the S-box that employs RDVFS technique is lower than the dynamic power dissipation of the S-box without a VFS technique.

When an S-box employs AVFS technique as shown in Figure 16(c), the clock frequency and supply voltage can also be lower than $f'_{c,0}$ and $V'_{dd,0}$, respectively. However, as compared to RDVFS technique, the clock frequency and supply voltage of an S-box that employs AVFS technique no longer have a one-to-one relationship (i.e., the clock frequency is independent of the supply voltage). Therefore, when the supply voltage is high, the clock frequency does not need to be high in AVFS technique. This property of the AVFS technique can make the dynamic power dissipation of the S-box that employs AVFS technique lower than the dynamic power dissipation of the S-box that employs RDVFS technique.

The leakage power dissipation P_{leak} of an S-box as derived as

$$P_{leak} \approx V_{dd} \times I_{leak,0} \times exp(1.19 \times V_{dd}). \tag{31a}$$

Unlike the dynamic power dissipation P_{dyn} of an S-box, the leakage power dissipation P_{leak} is actually independent of the clock frequency f_c.

When an S-box employs RDVS technique as shown in Figure 16(a), since the the supply voltage is higher than $V'_{dd,0}$, the leakage power dissipation of the S-box employs RDVS technique is higher than the leakage power dissipation of the S-box that does not employ a VFS technique. For an S-box that employs either RDVFS or AVFS technique (respectively illustrated in Figures 16(b) and 16(c)), since the the supply voltage can be lower than $V'_{dd,0}$, the leakage power dissipation of the S-box that employs RDVFS or AVFS technique is lower than the leakage power dissipation of the S-box that does not employ a VFS technique.

APPENDIX C
SECURITY OF ON-CHIP VOLTAGE REGULATION WITH NORMALLY DISTRIBUTED VFS TECHNIQUE AGAINST DPA ATTACKS

Assuming that the clock frequency f_c and the supply voltage V_{dd} of a RDVFS technique conform to a normal distribution with the mean values μ_f and μ_v, respectively, as

$$\mu_f = \frac{f_1 + f_2}{2}, \tag{34}$$

$$\mu_v = \frac{V_{DD1} + V_{DD2}}{2}, \tag{35}$$

the relationship between the variance of the clock frequency σ_f^2 and the variance of the supply voltage σ_v^2 becomes

$$\sigma_f^2 = \left(\frac{\mu_f}{\mu_v}\right)^2 \sigma_v^2. \tag{36}$$

If ΔV_{dd} is the minimum supply voltage resolution that is defined as

$$\Delta V_{dd} = \frac{V_{DD2} - V_{DD1}}{N - 1}, \tag{37}$$

the below approximated equation is satisfied when N is sufficiently large

$$\sum_{i=1}^{N} \frac{\Delta V_{dd}}{\sigma_v \sqrt{2\pi}} exp\left(-\frac{(V_{dd,i} - \mu_v)^2}{2\sigma_v^2}\right) \approx 1. \tag{38}$$

Assuming that the total number of input (f_c, V_{dd}) data is W, the corresponding number of input $(f_{c,i}, V_{dd,i})$ data W_i is

$$W_i \approx \frac{W}{\sigma_v \sqrt{2\pi}} exp\left(-\frac{(V_{dd,i} - \mu_v)^2}{2\sigma_v^2}\right). \tag{39}$$

The mean value of the uncertain noise $E(N_{j,k}(f_c, V_{dd}))$ for on-chip voltage regulation based and normally distributed RDVFS technique ($j = 1$), RDVS technique ($j = 2$), and AVFS technique ($j = 3$) become

$$E(N_{1,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^{N} W_i \left[\frac{f_{c,i}}{f_v}\right]} \sum_{i=1}^{N} W_i \left[\frac{f_{c,i}}{f_v}\right] N_{1,k}(f_{c,i}, V_{dd,i}), \tag{40}$$

$$E(N_{2,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^{N} W_i} \sum_{i=1}^{N} W_i N_{2,k}(f_c, V_{dd,i}), \tag{41}$$

$$E(N_{3,k}(f_c, V_{dd})) = \frac{1}{\sum_{l=1}^{N} \sum_{i=1}^{N} W_l W_i \left[\frac{f_{c,l}}{f_v}\right]} \times \sum_{l=1}^{N} \sum_{i=1}^{N} W_l W_i \left[\frac{f_{c,l}}{f_v}\right] N_{3,k}(f_{c,l}, V_{dd,i}). \tag{42}$$

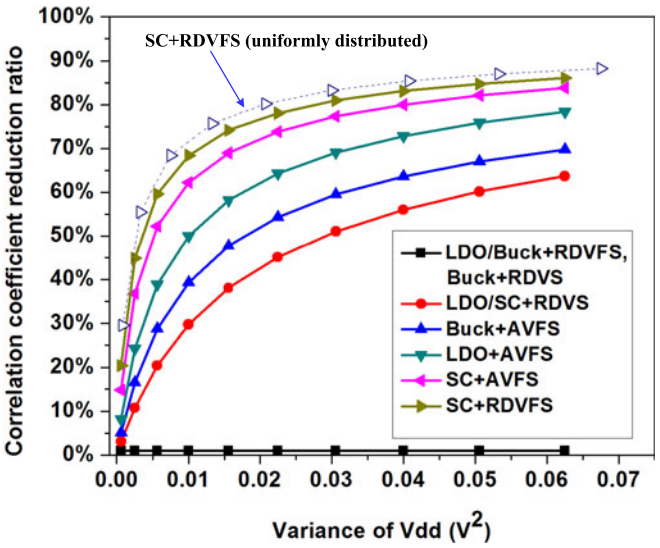


FIGURE 17. Variance of supply voltage V_{dd} versus correlation coefficient reduction ratio of an S-box that employs different techniques (VFS techniques conform to normal distribution, $f_v = 10$ MHz, and $N = 50$) as compared to uniformly distributed RDVFS with an SC voltage converter.

The corresponding variance of uncertain noise $Var(N_{1,k}(f_c, V_{dd}))$ can be written as

$$Var(N_{1,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^{N} W_i \left[\frac{f_{c,i}}{f_v}\right]} \times \sum_{i=1}^{N} W_i \left[\frac{f_{c,i}}{f_v}\right] (N_{1,k}(f_{c,i}, V_{dd,i}) - E(N_{1,k}(f_c, V_{dd})))^2, \tag{43}$$

$$Var(N_{2,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^{N} W_i} \times \sum_{i=1}^{N} W_i (N_{2,k}(f_c, V_{dd,i}) - E(N_{2,k}(f_c, V_{dd})))^2, \tag{44}$$

$$Var(N_{3,k}(f_c, V_{dd})) = \frac{1}{\sum_{l=1}^{N} \sum_{i=1}^{N} W_l W_i \left[\frac{f_{c,l}}{f_v}\right]} \times \sum_{l=1}^{N} \sum_{i=1}^{N} W_l W_i \left[\frac{f_{c,l}}{f_v}\right] (N_{3,k}(f_{c,l}, V_{dd,i}) - E(N_{3,k}(f_c, V_{dd})))^2. \tag{45}$$

As shown in Figure 17, an S-box [30] with the RDVFS technique employing an SC converter still exhibits the highest correlation coefficient reduction ratio as compared to the S-boxes that employ other techniques. Moreover, as compared to the S-box with uniformly distributed RDVFS technique employing an SC converter, the S-box with normally distributed RDVFS technique employing an SC converter has a slightly lower correlation coefficient reduction ratio under the same variance of the supply voltage. However, as shown in Figure 18, for achieving the same variance of supply voltage, the normally distributed RDVFS technique

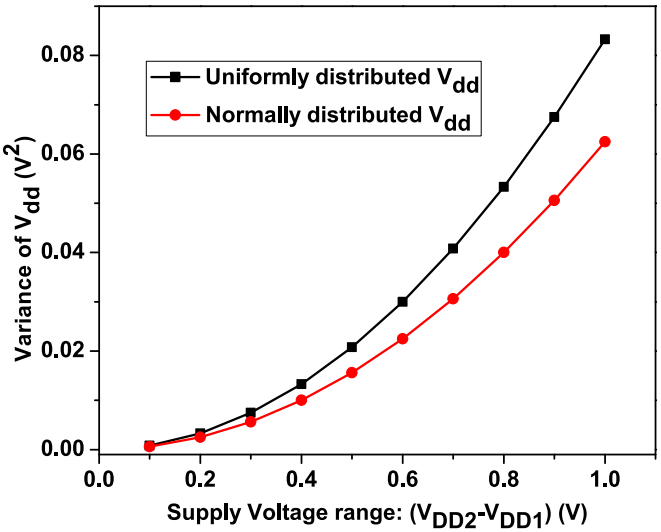


FIGURE 18. Variance of the supply voltage V_{dd} versus the supply voltage range $(V_{DD2} - V_{DD1})$ for uniformly and normally distributed V_{dd}.

needs to have a larger supply voltage range $(V_{DD2} - V_{DD1})$, which would degrade the performance of the cryptographic circuits as compared to the uniformly distributed RDVFS technique.

ACKNOWLEDGMENTS

This work is supported in part by the National Science Foundation CAREER award under Grant CCF-1350451 and by the USF Presidential Fellowship.

REFERENCES

[1] S. Mangard, E. Oswald, and T. Popp, "Power analysis attacks revealing the secrets of smart cards," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2007.

[2] W. Yu, O. A. Uzun, and S. Kose, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *Proc. 52nd Annu. Des. Autom. Conf.*, Jun. 2015, pp. 1–6.

[3] W. Yu and S. Kose, "A voltage regulator-assisted lightweight AES implementation against DPA attacks," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 63, no. 8, pp. 1152–1163, Aug. 2016.

[4] S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach," in *Proc. Conf. Des. Autom. Test Europe*, Mar. 2005, pp. 64–69.

[5] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *Proc. 20th Int. Conf. VLSI Des. Held Jointly 6th Int. Conf. Embedded Syst.*, Jan. 2007, pp. 854–862.

[6] W. Yu and S. Kose, "Charge-withheld converter-reshuffling: A countermeasure against power analysis attacks," *IEEE Trans. Circuits Syst. II: Express Briefs*, vol. 63, no. 5, pp. 438–442, May 2016.

[7] W. Yu and S. Kose, "Time-delayed converter-reshuffling: An efficient and secure power delivery architecture," *IEEE Embedded Syst. Lett.*, vol. 7, no. 3, pp. 73–76, Sep. 2015.

[8] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 57, no. 2, pp. 355–367, Feb. 2010.

[9] N.-H. Zhu, Y.-J. Zhou, and H.-M. Liu, "Employing symmetric dual-rail logic to thwart LPA attack," *IEEE Emedded Syst. Lett.*, vol. 5, no. 4, pp. 61–64, Dec. 2013.

[10] W. Yu and S. Kose, "Security implications of simultaneous dynamic and leakage power analysis attacks on nanoscale cryptographic circuits," *IET Electron. Lett.*, vol. 52, no. 6, pp. 466–468, Mar. 2016.

[11] N. D. P. Avirneni and A. K. Somani, "Countering power analysis attacks using reliable and aggressive designs," *IEEE Trans. Comput.*, vol. 63, no. 6, pp. 1408–1420, Jun. 2014.

[12] F.-X. Standaert, E. Peeters, G. Rouvroy, and J.-J. Quisquater, "An overview of power analysis attacks against field programmable gate arrays," *Proc. IEEE*, vol. 94, no. 2, pp. 383–394, Feb. 2006.

[13] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Conf. Des. Autom. Test Europe*, Feb. 2004, pp. 246–251.

[14] D. D. Huang, *et al.*, "AES-based security coprocessor IC in 0.18-μm CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–791, Apr. 2006.

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

[16] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A true random-based differential power analysis countermeasure circuit for an AES engine," *IEEE Trans. Circuits Syst. II: Express Briefs*, vol. 59, no. 2, pp. 103–107, Feb. 2012.

[17] Y. Wang and Y. Ha, "FPGA-based 40.9-Gbits/s masked AES with area optimization for storage area network," *IEEE Trans. Circuits Syst. II: Express Briefs*, vol. 60, no. 1, pp. 36–40, Jan. 2013.

[18] F. Regazzoni, Y. Wang, and F.-X. Standaert, "FPGA implementations of the AES masked against power analysis attacks," in *Proc. Int. Conf. Constructive Side-Channel Anal. Secure Des.*, Feb. 2011, pp. 56–66.

[19] N. S. Kim, K. Flautner, D. Blaauw, and T. Mudge, "Drowsy instruction caches. Leakage power reduction using dynamic voltage scaling and cache sub-bank prediction," in *Proc. Microarchitecture*, 2002, pp. 219–230.

[20] A. Moradi, "Side-channel leakage through static power-should we care about in practice?" in *Proc. 16th Int. Workshop Cryptographic Hardware Embedded Syst.*, 2014, pp. 562–579.

[21] S. M. D. Pozo, F.-X. Standaert, D. Kamel, and A. Moradi, "Side-channel attacks from static power: When should we care?" in *Proc. Des. Autom. Test Europe*, Mar. 2015, pp. 145–150.

[22] P. Zhou, A. Paul, C. H. Kim, and S. S. Sapatnekar, "Distributed on-chip switched-capacitor DC-DC converters supporting dvfs in multicore systems," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 22, no. 9, pp. 1954–1967, Sep. 2014.

[23] E. J. Fluhr, S. Baumgartner, D. Boerstler, J. F. Bulzacchelli, T. Diemoz, D. Dreps, G. English, J. Friedrich, A. Gattiker, T. Gloekler, C. Gonzalez, J. D. Hibbeler, K. A. Jenkins, Y. Kim, P. Muench, R. Nett, J. Paredes, J. Pille, D. Plass, P. Restle, R. Robertazzi, D. Shan, D. Siljenberg, M. Sperling, K. Stawiasz, G. Still, Z. Toprak-Deniz, J. Warnock, G. Wiedemeier, and V. Zyuban, "The 12-core POWER8 processor with 7.6 Tb/s IO bandwidth, integrated voltage regulation, and resonant clocking," *IEEE J. Solid-State Circuits*, vol. 50, no. 1, pp. 10–23, Jan. 2015.

[24] S. Kose, S. Tam, S. Pinzon, B. McDermott, and E. G. Friedman, "Active filter-based hybrid on-chip DC-DC converter for point-of-load voltage regulation," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 21, no. 4, pp. 680–691, Apr. 2013.

[25] X. Qu, Z.-K. Zhou, B. Zhang, and Z.-J. Li, "An ultralow-power fast-transient capacitor-free low-dropout regulator with assistant pushpull output stage," *IEEE Trans. Circuits Syst. II: Express Briefs*, vol. 60, no. 2, pp. 96–100, Feb. 2013.

[26] W. Kim, M. S. Gupta, G.-Y. Wei, and D. Brooks, "System level analysis of fast, per-core DVFS using on-chip switching regulators," in *Proc. IEEE 14th Int. Symp. High Performance Comput. Archit.*, Feb. 2008, pp. 123–134.

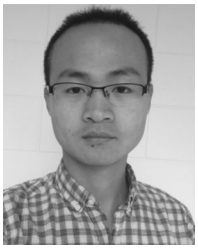
[27] T. M. Andersen, F. Krismer, J. W. Kolar, T. Toifl, C. Menolfi, L. Kull, T. Morf, M. Kossel, M. Brändli, P. Buchmann, and P. A. Francese, "A 4.6 W/mm^2 power density 86% efficiency on-chip switched capacitor DC-DC converter in 32 nm SOI CMOS," in *Proc. IEEE Int. Appl. Power Electron. Conf. Exposition*, Mar. 2013, pp. 692–699.

[28] B. Lee, E. Nurvitadhi, R. Dixit, C. Yu, and M. Kim, "Dynamic voltage scaling techniques for power efficient video decoding," *EUROMICRO J.*, vol. 51, no. 10, pp. 633–652, 2005.

[29] S. A. Seyyedi, M. Kamal, H. Noori, and S. Safari, "Securing embedded processors against power analysis based side channel attacks using reconfigurable architecture," in *Proc. IFIP 9th Int. Conf. Embedded Ubiquitous Comput.*, Oct. 2011, pp. 255–260.

[30] N. Ahmad and S. M. R. Hasan, "Low-power compact composite field AES S-Box/Inv S-Box design in 65 nm CMOS using novel XOR gate," *VLSI J. Integr.*, vol. 46, no. 4, pp. 333–344, Sep. 2013.

[31] J. Kim, S. Yoo, and C.-M. Kyung, "Program phase and runtime distribution-aware online DVFS for combined VDD/VBB scaling," in *Proc. Conf. Des. Autom. Test Europe*, Apr. 2009, pp. 417–422.
[32] S. Garg, D. Marculescu, R. Marculescu, and U. Ogras, "Technology-driven limits on DVFS controllability of multiple voltage-frequency island designs: A system-level perspective," in *Proc. Conf. Des. Autom. Conf.*, Jul. 2009, pp. 818–821.
[33] Q. Wu, P. Juang, M. Martonosi, and D. W. Clark, "Voltage and frequency control with adaptive reaction time in multiple-clock-domain processors," in *Proc. 11th Int. Symp. High-Performance Comput. Archit.*, Feb. 2005, pp. 178–189.
[34] C. Gopalakrishnan, "High level techniques for leakage power estimation and optimization in VLSI ASICs," Ph.D. dissertation, Dept. Comput. Sci., Univ. South Florida, Tampa, Sep. 2003.



WEIZE YU received the BS and MS degrees in electrical engineering from the University of Electronic Science and Technology of China, Chengdu, China, and the Institute of Microelectronics of Chinese Academy of Sciences, Beijing, China, respectively, in 2009 and 2012. Currently, he is working toward the PhD degree at the University of South Florida. His current research interests include on-chip power management and hardware security.

SELÇUK KÖSE (S'10-M'12) received the BS degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2006, and the MS and PhD degrees in electrical engineering from the University of Rochester, Rochester, New York, in 2008 and 2012, respectively. He is currently an assistant professor in the Department of Electrical Engineering, University of South Florida, Tampa, Florida. He previously worked with VLSI Design Center of the Scientific and Technological Research Council (TUBITAK), Ankara, Turkey, the Central Technology and Special Circuits Team in the enterprise microprocessor division of Intel Corporation, Santa Clara, California, and the RF, Analog, and Sensor Group, Freescale Semiconductor, Tempe, Arizona. His current research interests include the analysis and design of high performance integrated circuits, on-chip DC-DC converters, and hardware security. He is an associate editor of the *Journal of Circuits, Systems, and Computers* and the *Microelectronics Journal*. He has served on the Technical Program Committee and Organization Committee of various IEEE and ACM conferences. He received the NSF CAREER Award, Cisco Research Award, USF Outstanding Faculty Award, and USF College of Engineering Outstanding Researcher Award. He is a member of the IEEE.