A Voltage Regulator-Assisted Lightweight AES Implementation Against DPA Attacks

Weize Yu and Selçuk Köse, *Member, IEEE*

***Abstract*—In this paper, the mathematical foundations of the security implications of utilizing various on-chip voltage converters as a countermeasure against differential power analysis (DPA) attacks are investigated. An exhaustive mathematical analysis of a recently proposed converter-reshuffling (CoRe) technique is presented where measurement to disclose (MTD) is used to compare the security of the proposed on-chip CoRe regulator with the security of conventional on-chip voltage regulators. A DPA-resistant and lightweight advanced encryption standard (AES) engine implementation that leverages the CoRe technique is proposed. The impact of the centralized and distributed placement of the voltage regulators on the security of a pipelined AES engine is explored. The security implications of the relationship between the clock frequency of the device under attack and the switching frequency of the voltage regulator are investigated. As compared to an unprotected AES engine, the MTD value of the proposed improved pipelined AES engine with a centralized on-chip CoRe regulator is enhanced over 9100 times.**

***Index Terms*—Advanced encryption standard engine, centralized, converter-reshuffling, measurement to disclose.**

I. Introduction

POWER analysis attacks (PAAs) are non-invasive side-channel attacks to acquire critical information from cryptographic circuits (CCs) by monitoring the power consumption profile. A differential power analysis (DPA) attack is an advanced PAA that statistically analyzes multiple power traces to determine whether a secret key guess is correct or not [1]. DPA attacks are widely utilized by attackers due to the high efficiency and low cost. Various countermeasures have been proposed against DPA attacks [2]–[8]. Although certain countermeasures are quite effective to increase the trustworthiness of modern integrated circuits (ICs), the corresponding power, area, and performance overheads of existing countermeasures are typically quite large to be widely utilized.

There is a growing trend to integrate voltage regulators (VRs) fully on-chip in modern ICs to reduce the power noise, improve transient response time and increase power efficiency [9]–[12]. A one-to-one relationship exists between the input current I_{in} and load current I_{load}, as shown in Fig. 1, when a conventional on-chip VR (such as a low-dropout (LDO) regulator, a buck converter, and a switched-capacitor (SC) converter) is utilized.

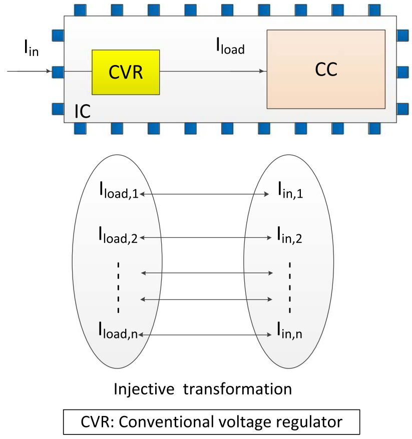


Fig. 1. One-to-one relationship between the input current and load current in conventional voltage regulator.

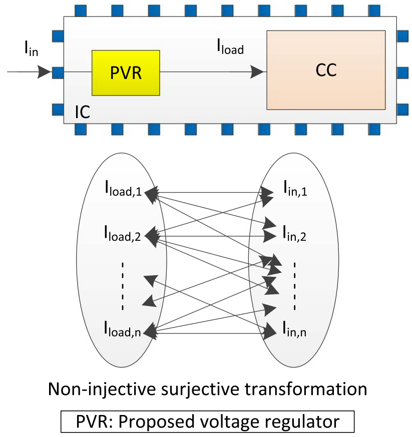


Fig. 2. One-to-one relationship between the input current and load current can be scrambled by powering the critical circuit blocks with the proposed voltage regulator.

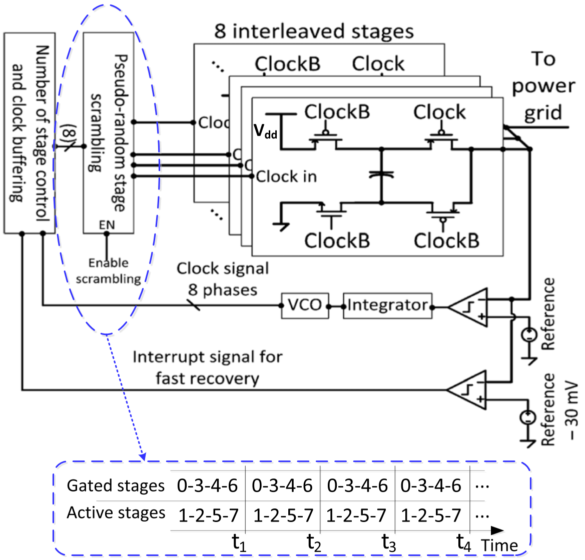
Therefore, an attacker can determine *what is going on inside a CC* by monitoring the input power profile of a conventional on-chip VR. To break the one-to-one relationship between the input current and load current, converter-gating (CoGa) technique is proposed in [13] to achieve a non-injective relationship between the input current and output current, as shown in Fig. 2. A multi-phase SC converter is utilized in the CoGa technique where the total number of active converter phases is adaptively altered based on the load power requirement to achieve a high power conversion efficiency [13]. A pseudo-random number generator (PRNG) is also inserted to randomize the sequence of the activated phases when the load current changes. However, if the variation in the load current is small, as shown in Fig. 3, CoGa technique is not activated. To increase the variance of injected random power noise by the on-chip VR,

Manuscript received January 7, 2016; revised March 9, 2016; accepted April 10, 2016. Date of publication July 7, 2016; date of current version August 9, 2016. This work is supported in part by the National Science Foundation CAREER award under Grant CCF-1350451 and by the USF Presidential Fellowship. This paper was recommended by Associate Editor Y. Ha.

The authors are with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: weizeyu@mail.usf.edu; kose@usf.edu).

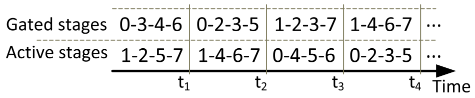
Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSI.2016.2555810



Gated stages	0-3-4-6	0-3-4-6	0-3-4-6	0-3-4-6	···
Active stages	1-2-5-7	1-2-5-7	1-2-5-7	1-2-5-7	···

Fig. 3. CoGa regulator in [13] (8-phase) exhibits a constant sequence of active stages if the variation in load current is small.


t_1
t_2
t_3
t_4
Time

Gated stages	0-3-4-6	0-2-3-5	1-2-3-7	1-4-6-7	···
Active stages	1-2-5-7	1-4-6-7	0-4-5-6	0-2-3-5	···

Fig. 4. Sequence of active stages is reshuffled in every switching cycle with the proposed CoRe technique.

converter-reshuffling (CoRe) technique is proposed to randomly reshuffle the sequence of active and gated stages in every switching cycle, as shown in Fig. 4, even when the change in the load current is small [14]–[16]. The primary difference between the CoGa and CoRe techniques is the design of the PRNG. As compared to the CoGa regulator, the correlation coefficient between the input power and load power of the CoRe regulator is significantly reduced due to the larger variance of the inserted random power noise by reshuffling the active and gated stages. Multiphase on-chip VRs can be distributed across the die or implemented at a centralized location [17]–[19]. Therefore, the security implications of the centralized and distributed on-chip voltage regulation with the proposed CoRe technique are investigated based on the correlation coefficient between the input power and side-channel power.[1]

A pipelined advanced encryption standard (AES) engine is a widely used CC due to the low path delay [20]–[22]. In a typical 128-bit pipelined AES engine, 16 substitution-boxes (S-boxes) are required in the 1st round encryption (each S-box is 8-bit), where each of the 16 S-boxes works independently. In a practical attack, if the attacker intends to attack one of those 16 S-boxes during the 1st encryption round, the attacker can dynamically alter the 8-bit input plaintext that corresponds to the input of the S-box under attack. The other plaintexts that are applied to the other 15 S-boxes which are not under attack are kept constant. As a result, the transient power noise generated by these 15 S-boxes which are not under attack would be greatly reduced and only a small amount of leakage power is dissipated within these S-boxes.

If the 15 S-boxes which are not under attack can exhibit a high dynamic power consumption even when the attacker applies a constant input plaintext, this dynamic power consumption can be randomized with the CoRe technique to further decrease the correlation between the input power and side-channel power. Therefore, an improved pipelined AES engine is proposed where invert boxes are added at the inputs of the S-boxes with a negligible area and power overhead. A clock signal with half of the frequency of the input plaintext is utilized to control all of the added invert boxes to ensure that all of the S-boxes would always have a high dynamic power consumption even if their input plaintexts are constant.

A preliminary version of this work appeared in [14]–[16]. We introduce the CoRe technique in [14] where we demonstrate the working principle with simulation results without providing a detailed analytic model. In [15], a certain time delay is inserted in the CoRe technique while activating the phases to eliminate the possibility of having zero entropy under machine learning attacks. A finite amount of charge is withheld in the flying capacitor for a random amount of time in [16] to increase the entropy of the input power profile. The key contributions of this paper are to lay the mathematical foundations of the CoRe technique through a detailed analysis of the correlation between the input and output power of both conventional and proposed voltage regulation techniques. The correlation coefficient and measurement to disclose (MTD) are used as the security metric in this paper instead of the power trace entropy used in [14]–[16]. The implications of the physical placement of the VRs on the correlation coefficient are investigated with centralized and distributed implementations of the CoRe regulators. We have recently noticed that the CoRe technique with an improved pipelined AES engine inserts both additive and multiplicative noise to the input power profile. An improved lightweight AES engine is accordingly proposed to further scramble the input power even if the attacker applies a constant plaintext to the S-boxes that are not under attack. The security implications of the proposed techniques are analytically proven using the correlation coefficient and MTD.

The rest of the paper is organized as follows. The security of a switching converter against power analysis attacks is explained in Section II. The correlation analysis between the input and load power of different on-chip VRs is discussed in Section III. In Section IV, a conventional pipelined AES engine with on-chip CoRe technique is analyzed. An improved pipelined AES engine with the centralized CoRe technique is proposed in Section V to reduce the correlation coefficient between the input power and side-channel power. The analytical analysis is further supported by circuit level simulations in Section VI while the conclusions are offered in Section VII.

II. Security of a Switching Converter Against Power Analysis Attacks

The correlation coefficient between the input data and actual dynamic power dissipation of a cryptographic circuit (CC) γ is [23]

$$\gamma \simeq \sqrt{\frac{m_0}{m_1}} \tag{1}$$

and the corresponding MTD value is [23]

$$\text{MTD} \propto \frac{1}{\gamma^2} \tag{2}$$

[1] Side-channel power represents the power consumption induced by the S-box under attack.

where m_1 is the total number of bits of the input data and m_0 is the number of bits which strongly correlates with the actual dynamic power consumption in the input data. The correlation coefficient γ between the input data and actual dynamic power consumption is determined by the architecture of a CC. If the architecture of a CC is not modified at runtime γ and MTD would not have a significant variation.

A switching converter has two phases in each switching period: charging phase and discharging phase. The average input power within a switching period strongly correlates with the load power within that switching period. Let us assume that the switching frequency of the converter is f_s and the clock frequency of the CC is f_c. In modern ICs, f_c is typically greater than f_s [19], [24] (we assume $f_c = M_1 f_s$). To obtain accurate power data generated by a CC from the input side of the switching converter, the attacker needs to sample the average input power within a switching period as one sample of the power data. However, from a CC without a switching converter, the attacker can obtain M_1 different power data samples within that switching period. As a result, if a CC is powered with a switching converter, the MTD is inherently enhanced M_1 times, as compared to the MTD of a CC without a switching converter. Decreasing the switching frequency is therefore an effective way to enhance the MTD value, but lower switching frequency may increase the area of output capacitance of the voltage converter. So there is a trade-off between the area and security of switching converters.

III. Correlation Analysis of On-Chip Voltage Regulators

In this section, the correlation coefficient models are presented for the CoGa and CoRe techniques as well as for the conventional on-chip VRs.

A. Modeling Correlation Coefficient of Converter-Gating (CoGa) and Converter-Reshuffling (CoRe) Regulators

The CoGa regulator [13] consists of two types of modulations: frequency modulation and number of activated phases modulation. The switching frequency f_s in CoGa regulator has a narrow variation range $[f_{s,pk} - \Delta f_s/2, f_{s,pk} + \Delta f_s/2]$, where $f_{s,pk}$ is the corresponding switching frequency to achieve the peak power conversion efficiency and Δf_s is the amplitude of the variation in the switching frequency f_s. If f_s is higher than $f_{s,pk} + \Delta f_s/2$, an additional phase is activated to provide more power to the load. When an additional phase is activated, f_s is reduced to a nominal value. If f_s is lower than $f_{s,pk} - \Delta f_s/2$, an active phase is gated to reduce the output power while f_s is increased to a nominal value.

To investigate the security implications of CoGa or CoRe regulator, the type of power noise generated by CoGa and CoRe regulators needs to be determined. Two different types of noise can be inserted into a system: additive noise and multiplicative noise. The input power of CoGa or CoRe regulator P_{in} can be defined as

$$P_{\text{in}} = a_o \times P_{\text{load}} + b_o \tag{3}$$

where P_{load} is the load power dissipation of CoGa or CoRe regulator. a_o and b_o, respectively, represent multiplicative and additive noise. If the load power P_{load} is zero, the input power P_{in} is also equal to zero. Therefore, $b_o = 0$ and only the multiplicative noise exists in CoGa or CoRe regulator. Since signal-to-noise ratio (SNR) is not a convenient metric for modeling multiplicative noise, correlation coefficient between the input power and load power is used as the metric to evaluate the security of on-chip VR [2], [3].

The dynamic power consumption $P_d[m]$ of a single S-box in an AES engine induced by the mth, $(m = 1, 2, \ldots)$ input plaintext conforms to a normal distribution [23], where the mean and variance of $P_d[m]$ are, respectively, μ_s and σ_s^2. Assuming that the clock frequency of the AES engine is M_1 times greater than the switching frequency of the CoGa or CoRe regulator (i.e., $f_c = M_1 f_s$), the average dynamic power consumption of a single S-box within a switching period $\overline{P_d[m]}$ can be written as

$$\overline{P_d[m]} = \sum_{p=0}^{M_1-1} \frac{P_d[m+p]}{M_1}. \tag{4}$$

When $P_d[m], P_d[m+1], \ldots, P_d[m+M_1-1]$ are mutually independent, the average dynamic power consumption of a single S-box within a switching period $\overline{P_d[m]}$ also conforms to a normal distribution with mean $\overline{\mu_s}$ and variance $\overline{\sigma_s^2}$ as

$$\overline{\mu_s} = \sum_{p=0}^{M_1-1} \frac{\mu_s}{M_1} = \mu_s \tag{5}$$

$$\overline{\sigma_s^2} = \sum_{p=0}^{M_1-1} \left(\frac{\sigma_s}{M_1}\right)^2 = \frac{\sigma_s^2}{M_1}. \tag{6}$$

The minimum and maximum average dynamic power dissipation of a single S-box within a single switching period are, respectively, $j_{\min} P_0$ and $j_{\max} P_0$ where P_0 is the power resolution. Assuming P_0 is sufficiently small, the following approximated equation can be written as

$$\sum_{j=j_{\min}}^{j_{\max}} \frac{P_0\sqrt{M_1}}{\sigma_s\sqrt{2\pi}} \exp^{\left(-\frac{(j\times P_0-\mu_s)^2}{\frac{2\sigma_s^2}{M_1}}\right)} \approx 1. \tag{7}$$

If the total number of input plaintexts applied by the attacker is W, the number W_j which corresponds to the average dynamic power of a single S-box jP_0, $(j \in [j_{\min}, j_{\max}])$ within a switching period can be approximated as

$$W_j \approx W \frac{P_0\sqrt{M_1}}{\sigma_s\sqrt{2\pi}} \exp^{\left(-\frac{(j\times P_0-\mu_s)^2}{\frac{2\sigma_s^2}{M_1}}\right)}. \tag{8}$$

If the attacker intends to sample K, $(K = 1, 2, \ldots)$ consecutive switching periods as one sample of power data, as shown in Fig. 5, the input power distribution among the $(n+u)T_s$ and $(n+u+1)T_s$, $(n = 0, 1, \ldots, u = 0, 1, 2, \ldots)$ period can be denoted by array A_{n+u} as

$$A_{n+u} = [a_{n+u,1}, a_{n+u,2}, \ldots, a_{n+u,N}]P \tag{9}$$

where P is the power consumed by each phase, N is the total number of phases of CoGa or CoRe regulator, and $a_{n+u,i} \in \{0, 1\}$, $(i = 1, 2, \ldots, N)$. Another array $G(\theta) = [g_1(\theta), g_2(\theta), \ldots, g_N(\theta)]$ is used to store the range of sampled input power

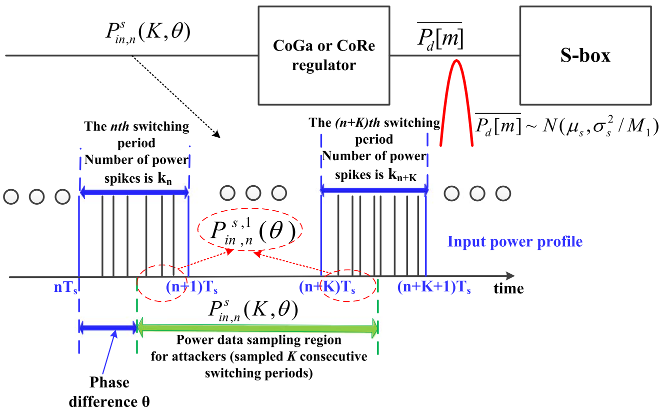

$P^s_{in,n}(K,\theta)$
CoGa or CoRe regulator
$\overline{P_d[m]}$
S-box
$\overline{P_d[m]} \sim N(\mu_s, \sigma_s^2/M_1)$
The *nth* switching period
Number of power spikes is k_n
The *(n+K)th* switching period
Number of power spikes is k_{n+K}
$P^{s,1}_{in,n}(\theta)$
Input power profile
nT_s
$(n+1)T_s$
$(n+K)T_s$
$(n+K+1)T_s$
time
$P^s_{in,n}(K,\theta)$
Power data sampling region for attackers (sampled *K* consecutive switching periods)
Phase difference θ

Fig. 5. Input power data sampling for the attacker within K consecutive switching periods when the CoGa or CoRe techniques are enabled (T_s is the switching period of the CoGa or CoRe regulator).

spikes within the nth switching period where θ is the phase difference between the switching frequency and frequency of data sampling. The elements $g_i(\theta)$ in $G(\theta)$ array are

$$g_i(\theta) = \begin{cases} 0 & , i \leq [\theta/2\pi \times N] \\ 1 & , [\theta/2\pi \times N] < i \leq N. \end{cases} \tag{10}$$

The total sampled input power by the attacker within K consecutive switching periods $P^s_{\text{in},n}(K,\theta)$, as shown in Fig. 5, is

$$\begin{aligned} P^s_{\text{in},n}(K,\theta) &= A_n G(\theta)^T + A_{n+K}\overline{G(\theta)}^T + \sum_{u=1}^{K-1} \frac{j_{n+u}P_0}{\eta_0} \\ &= P^{s,1}_{\text{in},n}(\theta) + \sum_{u=1}^{K-1} \frac{j_{n+u}P_0}{\eta_0} \end{aligned} \tag{11}$$

where a complementary array $\overline{G(\theta)} = [\overline{g_1(\theta)}, \overline{g_2(\theta)}, \ldots, \overline{g_N(\theta)}]$ is used to represent the range of input power sampling within the $(n+K)$th switching period, where η_0 is the power efficiency of CoGa or CoRe regulator and $j_{n+u} \in [j_{\min}, j_{\max}]$.

For the CoRe regulator, the total number of power spikes k_{n+u} within the $(n+u)$th switching period can be determined as

$$k_{n+u} = \left\lceil \frac{j_{n+u} \times P_0}{\eta_0 \times P} \right\rceil. \tag{12}$$

Additionally, the element $a_{n+u,i}$ in A_{n+u} needs to satisfy $\sum_{i=1}^{N} a_{n+u,i} = k_{n+u}$.

In the CoRe regulator, the total sampled input power within the nth switching period and the $(n+K)$th switching period is $P^{s,1}_{\text{in},n}(\theta) = lP$, $(l = 0, 1, 2, \ldots, N)$. The number of the corresponding input power samples can be counted as $x_{l,j_n,j_{n+K}}(\theta)$ after all of the possible A_n and A_{n+K} are enumerated. When W input plaintexts are applied by the attacker, the number of total input power samples $x_l(\theta)$ for the corresponding sampled input power $P^{s,1}_{\text{in},n}(\theta)$ can be calculated as

$$x_l(\theta) = \sum_{j_{n+K}=j_{\min}}^{j_{\max}} \sum_{j_n=j_{\min}}^{j_{\max}} W_{j_n} W_{j_{n+K}} x_{l,j_n,j_{n+K}}(\theta). \tag{13}$$

The mean value of the total sampled input power within K consecutive switching periods $\mu_{\text{in}}(K,\theta)$ becomes[2]

$$\begin{aligned} \mu_{\text{in}}(K,\theta) &= E\left(P^s_{\text{in},n}(K,\theta)\right) \\ &= E\left(P^{s,1}_{\text{in},n}(\theta)\right) + E\left(\sum_{u=1}^{K-1} \frac{j_{n+u}P_0}{\eta_0}\right) \\ &= \frac{\sum_{l=0}^{N} lP \times x_l(\theta)}{\sum_{l=0}^{N} x_l(\theta)} + (K-1)\mu'_s \end{aligned} \tag{14}$$

where μ'_s is

$$\mu'_s \approx \sum_{j=j_{\min}}^{j_{\max}} \frac{jP_0\sqrt{M_1}}{\eta_0 \sigma_s \sqrt{2\pi}} \exp^{\left(-\frac{(j \times P_0 - \mu_s)^2}{2\sigma_s^2/M_1}\right)}. \tag{15}$$

The variance of total sampled input power within K consecutive switching periods $\sigma^2_{\text{in}}(K,\theta)$ can be written as[3]

$$\begin{aligned} \sigma^2_{\text{in}}(K,\theta) &= \text{Var}\left(P^s_{\text{in},n}(K,\theta)\right) \\ &= \text{Var}\left(P^{s,1}_{\text{in},n}(\theta)\right) + \text{Var}\left(\sum_{u=1}^{K-1} \frac{j_{n+u}P_0}{\eta_0}\right) \\ &= \frac{\sum_{l=0}^{N} \left(x_l(\theta) \times (lP - \mu_{\text{in}}(\theta))^2\right)}{\sum_{l=0}^{N} x_l(\theta)} + (K-1)(\sigma'_s)^2 \end{aligned} \tag{16}$$

where $(\sigma'_s)^2$ is

$$(\sigma'_s)^2 = \frac{1}{j_{\max} - j_{\min} + 1} \sum_{j=j_{\min}}^{j_{\max}} (jP_0/\eta_0 - \mu'_s)^2. \tag{17}$$

The load power of the CoRe regulator $P_{\text{load},n}(K,\theta)$ that corresponds to the sampled input power $P^s_{\text{in},n}(K,\theta)$ can be written as

$$\begin{aligned} P_{\text{load},n}(K,\theta) = \left(1 - \frac{\theta}{2\pi}\right) j_{n+1}P_0 + \frac{\theta}{2\pi} j_{n+K+1}P_0 \\ + \sum_{u=2}^{K} j_{n+u}P_0. \end{aligned} \tag{18}$$

The mean value of the load power $\mu_L(K,\theta)$ and variance of the load power $\sigma^2_L(K,\theta)$, respectively, are

$$\mu_L(K,\theta) = \left(1 - \frac{\theta}{2\pi}\right)\mu_s + \frac{\theta}{2\pi}\mu_s + (K-1)\mu_s = K\mu_s \tag{19}$$

$$\sigma^2_L(K,\theta) = \left(1 - \frac{\theta}{2\pi}\right)\frac{\sigma_s^2}{M_1} + \frac{\theta}{2\pi}\frac{\sigma_s^2}{M_1} + (K-1)\frac{\sigma_s^2}{M_1} = \frac{K\sigma_s^2}{M_1}. \tag{20}$$

The correlation coefficient of the on-chip CoRe regulator $\gamma(K,\theta)$ is determined as[4]

$$\begin{aligned} \gamma(K,\theta) = \frac{E\left(P^s_{\text{in},n}(K,\theta) \times P_{\text{load},n}(K,\theta)\right)}{\sigma_{\text{in}}(K,\theta) \times \sqrt{K/M_1}\sigma_s} \\ - \frac{\mu_{\text{in}}(K,\theta) \times K\mu_s}{\sigma_{\text{in}}(K,\theta) \times \sqrt{K/M_1}\sigma_s} \end{aligned} \tag{21}$$

[2] E represents the sign for the calculation of the mean value.

[3] Var represents the sign for the calculation of the variance.

[4] The attacker sampled the total input power within K consecutive switching periods as one sample of the power data.

where $E(P^s_{\mathrm{in},n}(K,\theta)\times P_{\mathrm{load},n}(K,\theta))$ is

$$\begin{aligned}&E\big(P^s_{\mathrm{in},n}(K,\theta)\times P_{\mathrm{load},n}(K,\theta)\big)\\&=\frac{1}{(j_{\max}-j_{\min}+1)^{K+2}}\\&\times\left(\sum_{j_{n+K+1}=j_{\min}}^{j_{\max}}\cdots\sum_{j_n=j_{\min}}^{j_{\max}}\right.\\&\times\left(\left(P^{s,1}_{\mathrm{in},n}(\theta)+\sum_{u=1}^{K-1}\frac{j_{n+u}P_0}{\eta_0}\right)\right.\\&\left.\left.\times\left(\left(1-\frac{\theta}{2\pi}\right)j_{n+1}P_0+\frac{\theta}{2\pi}j_{n+K+1}P_0+\sum_{u=2}^{K}j_{n+u}P_0\right)\right)\right).\end{aligned}\tag{22}$$

The average correlation coefficient of the CoRe regulator $\overline{\gamma(K)}$ can be denoted as

$$\overline{\gamma(K)}=\frac{1}{2\pi}\int_0^{2\pi}\gamma(K,\theta)d\theta.\tag{23}$$

The correlation coefficient modeling of the CoGa regulator is quite similar to the modeling of the CoRe regulator with one extra condition that needs to be added to the element $a_{n+u,i}$ in A_{n+u} as

$$\begin{cases}a_{n+u+1,i}-a_{n+u,i}\geq 0, & \text{if } k_{n+u+1}\geq k_{n+u}\\ a_{n+u,i}-a_{n+u+1,i}\geq 0, & \text{if } k_{n+u}<k_{n+u+1}.\end{cases}\tag{24}$$

B. Modeling Correlation Coefficient of Conventional On-Chip Voltage Regulators

Conventional on-chip (COC) VRs such as LDO regulator/buck converter/SC converter typically do not insert any randomness in the input or output power profile unless their architectures are tailored to scramble the input and output impedance characteristics. The relationship between the input power and load power of a COC VR can be modeled as

$$P'_{\mathrm{in}}(t+\Delta t)=\frac{1}{\eta_1}\times P_{\mathrm{load}}(t)\tag{25}$$

where Δt is the time delay between the input power and load power, η_1 is the power efficiency, $P'_{\mathrm{in}}(t+\Delta t)$ is the transient input power, and $P_{\mathrm{load}}(t)$ is the load power of a COC VR.

The detailed correlation coefficient derivation of COC VRs can be found in Appendix A.

C. Validation of the Proposed Correlation Coefficient Models With Practical Parameters

Substitution-box (S-box) is a circuit which is widely used in cryptography to mask the relationship between the secret key and ciphertext [25]–[27]. Since an S-box can perform a nonlinear transformation, for an S-box with m_1 bits of input data, the output data can be m_2 bits that are masked through the nonlinear transformations. An S-box with a clock frequency f_c of 200 MHz is designed [28] with 130 nm CMOS and simulated in Cadence. The dynamic power dissipation of the S-box $P_d[m]$ conforms to a normal distribution with a mean value μ_s of 264 μW and a standard deviation σ_s of 26.8 μW. The total number of phases N in the CoGa and CoRe regulators is 32.

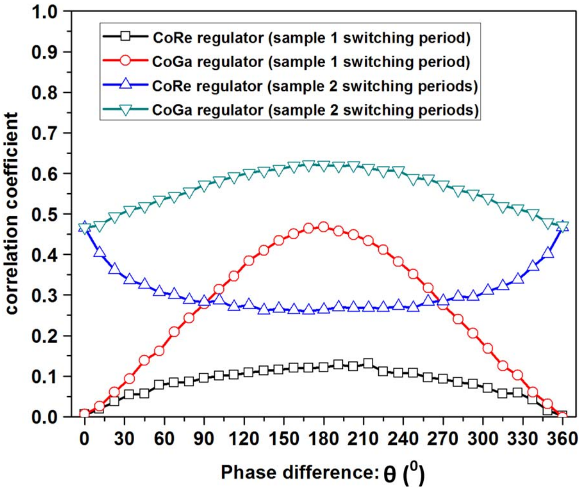


Fig. 6. Phase difference versus correlation coefficient of CoGa and CoRe techniques.

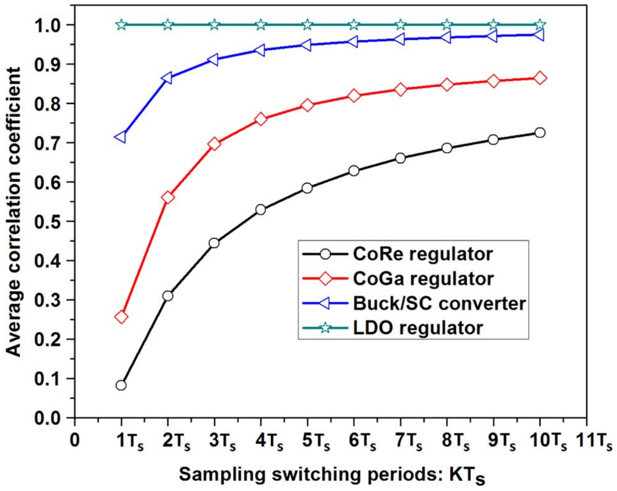


Fig. 7. Sampling switching periods versus average correlation coefficient.

As shown in Fig. 6, the correlation coefficient between the input power and load power of CoGa and CoRe regulators is not constant when the phase difference between the switching frequency and data sampling frequency changes. Unlike CoGa, CoRe regulator has a lower correlation coefficient due to the increased randomness with the reshuffling operation.

The relationship between the sampling switching period and average correlation coefficient is shown in Fig. 7. The correlation coefficient of an LDO regulator is around 1 due to the negligible time delay between the input power and load power. CoRe regulator exhibits the lowest correlation coefficient among the existing on-chip VRs due to the high randomness obtained with phase reshuffling. When the attacker increases the number of sampling switching periods, the average correlation coefficient of the CoRe regulator increases. The reason is that a certain portion of the noise inserted by the CoRe regulator can be filtered by the attacker by increasing the number of switching periods for each sampling. The cost is that more measurements are required for a successful attack, potentially increasing the MTD.

Let’s assume that the correlation coefficient between the predicted and actual dynamic power consumption of an S-box

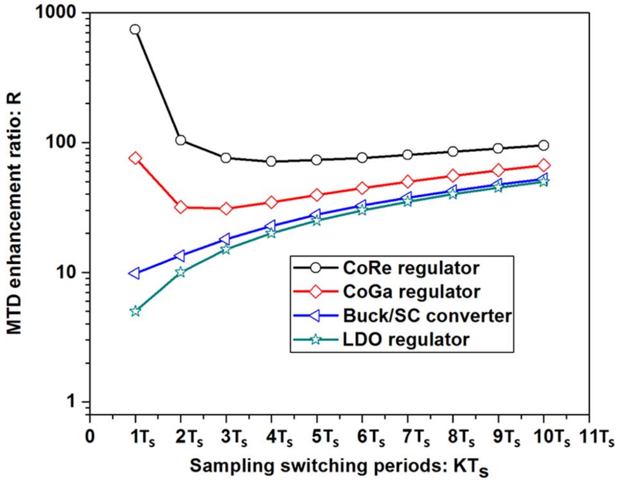


Fig. 8. Sampling switching periods versus MTD enhancement ratio ($M_1 \approx 5$).

is γ_1 and the correlation coefficient between the actual dynamic power consumption of an S-box and input power of an on-chip VR is γ_2. Since the operations that occur in the S-box are independent of the operations of the on-chip VR, the correlation coefficient between the input data and input power of an on-chip VR γ_3 can be denoted as [23]

$$\gamma_3 = \gamma_1 \times \gamma_2. \tag{26}$$

For a single S-box, the relationship between MTD value MTD_0 and correlation coefficient γ_1 is [23]

$$\mathrm{MTD}_0 \simeq \frac{C}{\gamma_1^2} \tag{27}$$

where C is the success rate dependent constant [23]. Accordingly, for a single S-box powered by an on-chip VR, the measurement to disclose MTD_1 becomes

$$\mathrm{MTD}_1 \simeq \frac{M_1 K}{\gamma_2^2} \times \mathrm{MTD}_0 = R \times \mathrm{MTD}_0 \tag{28}$$

where R is the MTD enhancement ratio of a single S-box powered by an on-chip VR. As compared to an S-box without an on-chip VR, as shown in Fig. 8, a single S-box with the CoRe regulator has the highest MTD enhancement ratio. The lowest MTD enhancement ratio of the CoRe regulator with S-box is 71.4 when the attacker optimizes the sampling duration of the attack and selects the total input power within 4 consecutive switching periods as a single sample of the power data.

The average correlation coefficient of the CoRe regulator decreases when the total number of phases N increases, as shown in Fig. 9. The reason is that when N increases, more number of gated phases are utilized to increase the randomness of the CoRe regulator. Additionally, if the power P consumed by each phase increases, the average correlation coefficient of the CoRe regulator reduces due to the larger variance of the random noise caused by the phase reshuffling within every switching cycle.

IV. Conventional Pipelined (CP) AES Engine With Converter-Reshuffling

In this section, the security concerns of a conventional pipelined AES engine are presented. Additionally, the implications of centralized and distributed on-chip voltage regulations with the CoRe technique on the security of the AES engine are investigated.

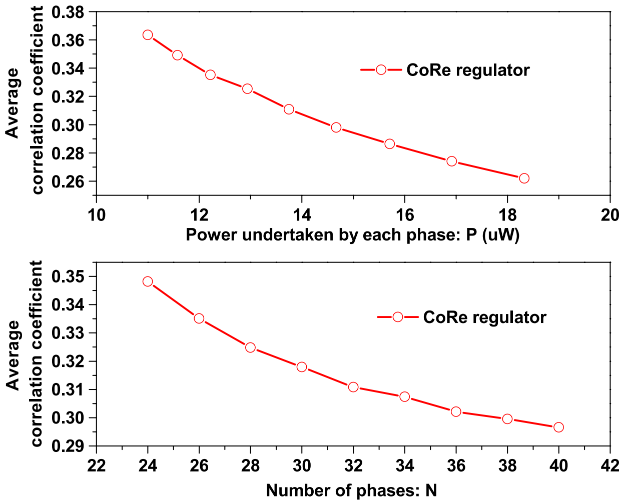


Fig. 9. Number of phases and power undertaken by each phase versus average correlation coefficient.

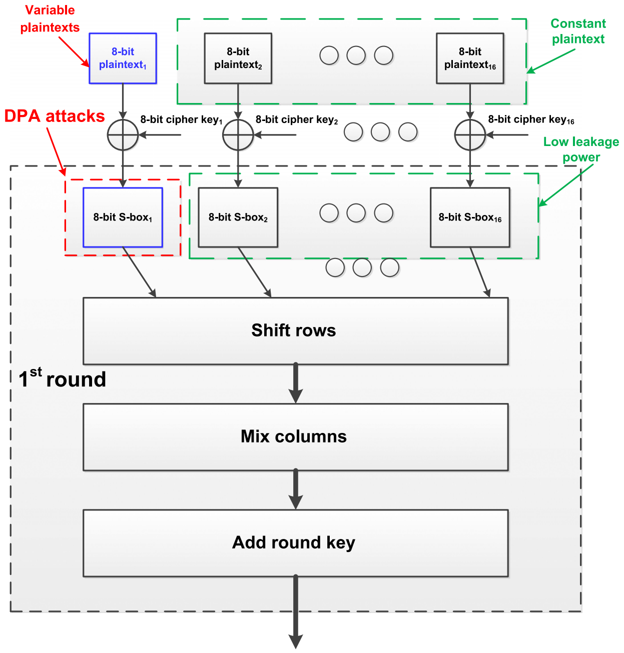


Fig. 10. 1st encryption round of a typical 128-bit pipelined AES engine.

A. Practical Power Attacks on a Pipelined AES Engine Without On-Chip Voltage Regulation

For a conventional 128-bit pipelined AES Engine, 16 S-boxes need to be placed in the 1st round encryption block, as shown in Fig. 10. If an attacker intends to implement a DPA attack on one of the 16 S-boxes in the 1st encryption round, the attacker can apply a suitable input plaintext combination to simplify the attack. For example, when S-box_1 is being targeted with a DPA attack, the attacker can input a different 8-bit plaintext_1 to combine the 8-bit cipher key_1 with the input side of S-box_1 sequentially while also maintaining the rest of the input plaintexts $(\text{plaintext}_2, \text{plaintext}_3, \ldots, \text{plaintext}_{16})$ as constant. As a result, S-box_1 would exhibit a high dynamic power consumption while the other 15 S-boxes would show a

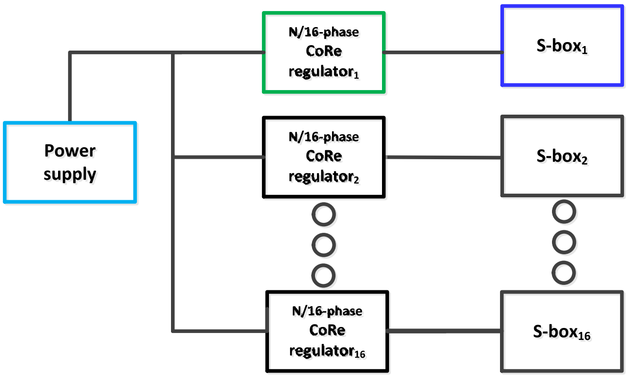

Power supply
N/16-phase CoRe regulator₁
N/16-phase CoRe regulator₂
N/16-phase CoRe regulator₁₆
S-box₁
S-box₂
S-box₁₆

Fig. 11. A conventional pipelined AES engine with a distributed on-chip CoRe technique.

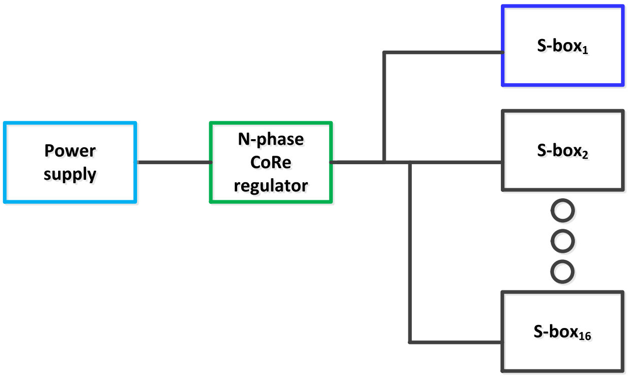


Fig. 12. A conventional pipelined AES engine with a centralized on-chip CoRe technique.

low leakage power dissipation. The leakage power generated by the other 15 S-boxes with a constant input plaintext can be treated as an additive power noise to the S-box$_1$ that is under attack.

B. Conventional Pipelined (CP) AES Engine With a Distributed CoRe Technique

Since 16 S-boxes exist in the 1st round encryption block of the CP AES engine, if a distributed CoRe technique is employed, 16 CoRe regulators are needed to power all of the S-boxes, as shown in Fig. 11. Let us assume that the total number of phases in the distributed CoRe regulators is N and the number of phases in each distributed CoRe regulator is $N/16$. In this case, the phase shift $\beta_{y,z}$ in each distributed CoRe regulator can be written as

$$\beta_{y,z} = \frac{2\pi}{N}\left(y + 16 \times (z-1)\right) \tag{29}$$

where y represents the yth $(y = 1, 2, \ldots, 16)$ CoRe regulator and z is the zth $(z = 1, 2, \ldots, N/16)$ phase in the yth CoRe regulator. The total sampled input power $P^{s,d}_{\mathrm{in},n}(K,\theta)$ of a CP AES engine with 16 distributed CoRe regulators within K consecutive switching periods can be expressed as[5]

$$P^{s,d}_{\mathrm{in},n}(K,\theta) = \sum_{y=2}^{16} A^d_y(K,\theta)\left(\frac{P_{\mathrm{leak},y}}{\eta_0}\right) + A^d_1(K,\theta)\left(\frac{(1-\frac{\theta}{2\pi})j_nP_0 + \frac{\theta}{2\pi}j_{n+K}P_0 + \sum_{u=1}^{K-1} j_{n+u}P_0}{\eta_0}\right) \tag{30}$$

where $A^d_y(K,\theta)$ is the yth multiplicative noise inserted by the yth CoRe regulator and $P_{\mathrm{leak},y}$ is the leakage power dissipation of the yth S-box. For a 128-bit CP AES engine with a distributed CoRe architecture, the total number of phases can be utilized to scramble the side-channel power is $16/N$. However, if a centralized CoRe architecture is used to power a CP AES engine, all of the phases can be utilized to scramble the input power consumption. The variance of noise in a CP AES engine with a distributed CoRe architecture may therefore not be high, which can be enhanced by utilizing a centralized CoRe technique in the following section.

C. Conventional Pipelined (CP) AES Engine With a Centralized CoRe Technique

When all of the 16 S-boxes use a centralized on-chip VR, as shown in Fig. 12, a common on-chip CoRe regulator is utilized to deliver power to all S-boxes. In this case, the total sampled input power $P^{s,c}_{\mathrm{in},n}(K,\theta)$ within K consecutive switching cycles can be denoted as

$$P^{s,c}_{\mathrm{in},n}(K,\theta) = A^c(K,\theta)\left(\frac{(1-\frac{\theta}{2\pi})j_nP_0 + \frac{\theta}{2\pi}j_{n+K}P_0}{\eta_0} + \frac{\sum_{u=1}^{K-1} j_{n+u}P_0 + P_{\mathrm{leak}}}{\eta_0}\right) \tag{31}$$

where $A^c(K,\theta)$ is the multiplicative noise generated by randomly reshuffling the active and gated phases in a CP AES engine with a centralized CoRe regulator. P_{leak} is the total leakage power generated by the 15 S-boxes with constant input plaintext where $\sum_{y=2}^{16} P_{\mathrm{leak},y} = P_{\mathrm{leak}}$.

Assuming that the correlation coefficient of a centralized CoRe regulator within a CP AES engine is γ_0, the signal-to-noise ratio (SNR) of the centralized CoRe regulator within a CP AES engine SNR$_0$ is [23]

$$\mathrm{SNR}_0 = \frac{\sigma_f^2}{\sigma_q^2} = \frac{1}{\frac{1}{\gamma_0^2} - 1} \tag{32}$$

where σ_f^2 and σ_q^2 are, respectively, the variance of the signal and noise. Accordingly, the variance of the noise of the centralized CoRe regulator within a CP AES engine can be denoted as

$$\sigma_q^2 = \left(\frac{1}{\gamma_0^2} - 1\right)\sigma_f^2. \tag{33}$$

As shown in Fig. 13, the average correlation coefficient of a centralized CoRe technique is lower than the average correlation coefficient of a distributed CoRe technique. The reason is that an increased number of gated phases are utilized during the reshuffling operation. As a result, the variance of the power noise inserted by the phase reshuffling operation in every switching cycle in a centralized CoRe architecture is enhanced significantly as compared to the total variance of power noise in a distributed CoRe architecture. As shown in Fig. 14, the minimum MTD enhancement ratio of a CP AES engine with a centralized CoRe architecture is around 544 when the attacker samples 10 consecutive switching cycles. Alternatively, the minimum MTD enhancement ratio of a CP AES engine with a

[5] Assuming S-box$_1$ is under DPA attacks.

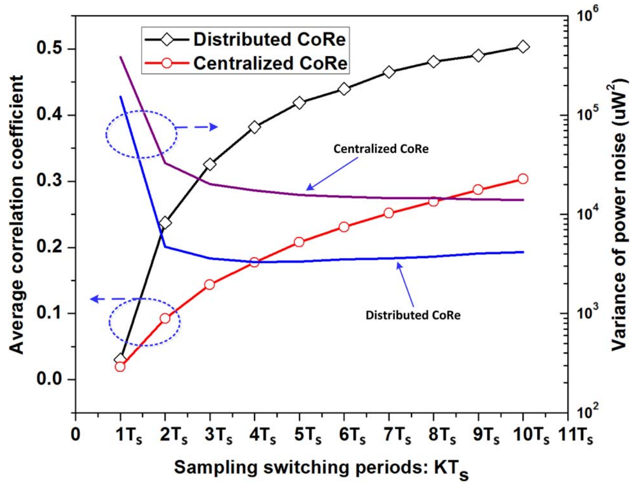


Fig. 13. Sampling switching periods versus average correlation coefficient and variance of power noise of the distributed and centralized CoRe architectures.

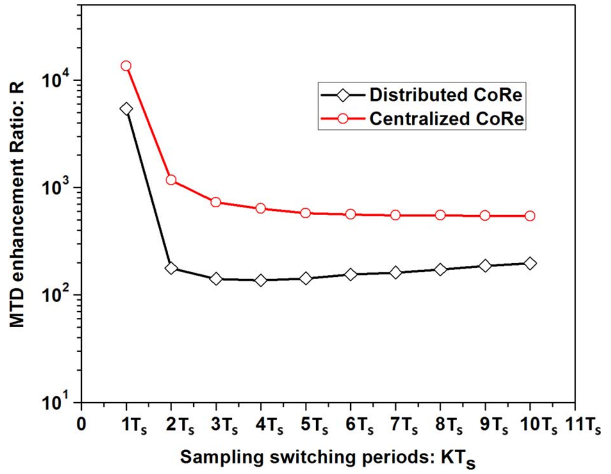


Fig. 14. Sampling switching periods versus MTD enhancement ratios of the distributed and centralized CoRe architectures $(M_1 \approx 5)$.

distributed CoRe architecture is about 137.1 when the attacker samples 4 consecutive switching cycles. After adopting the centralized CoRe technique, the minimum MTD enhancement ratio is also significantly increased.

V. Improved Pipelined (IP) AES Engine With Centralized CoRe Technique

In a CP AES engine, the S-boxes which are fed with a constant input plaintext would generate a low leakage power dissipation. If those S-boxes that are not under attack can exhibit a high dynamic power dissipation all the time even when constant input plaintext is applied, this high dynamic power dissipation may act as a power noise to scramble the dynamic power generated by the S-box under attack.

An improved pipelined (IP) AES engine is proposed to ensure that all of the S-boxes have high dynamic power dissipation at all times. As shown in Figs. 15 and 16 invert boxes (the internal logic circuits of each invert box are shown in Fig. 16) are inserted at the inputs of the S-boxes. After the 11th round of CP AES engine, a mask removal operation is performed, similar to [29]. CLK$_1$ is the clock signal for controlling the frequency of the input plaintext (CLK$_1$ also represents the clock frequency f_c as mentioned before). CLK$_2$ is the clock signal to control the frequency of the invert operations in each invert box. When the frequency of CLK$_1$ f_c is two times of the frequency of CLK$_2$ f_I, $(f_c = 2f_I)$, the input data of each S-box can be inverted with a frequency of f_c if constant input plaintext is enabled. As shown in Fig. 16, if $E_y = (10010100)_2, (10010100)_2, \ldots,$ after adding the corresponding invert box, the output data of invert box becomes $F_y = (10010100)_2, (01101011)_2, (10010100)_2, (01101011)_2, \ldots$. All of the S-boxes can therefore exhibit a high dynamic power consumption even if a constant input plaintext is applied by the attacker.

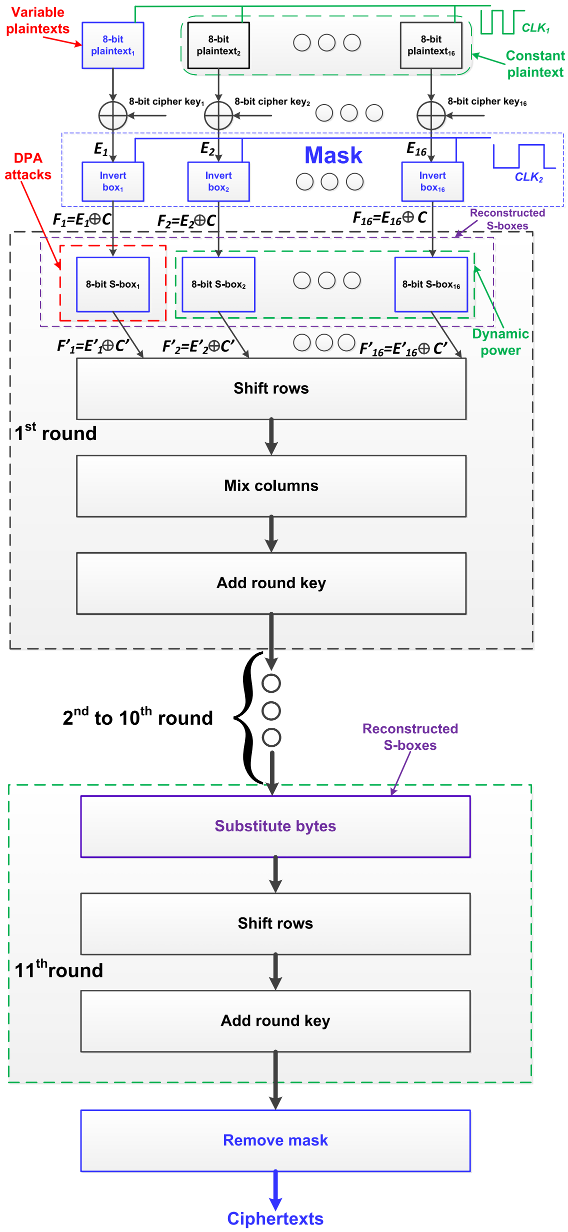


Fig. 15. Full encryption rounds of an 128-bit improved pipelined (IP) AES engine. Note that invert boxes are added before the 1st round and the mask removal operation is performed after the 11th round (the architecture of the reconstructed S-box can be founded in [29], [30]).

For the IP AES engine with constant input plaintext, if the output data of the yth invert box is $F_y = (f_{y,1}, f_{y,2}, \ldots, f_{y,8})_2$, and F_y makes a transition from $(f_{y,1}, f_{y,2}, \ldots, f_{y,8})_2$ to

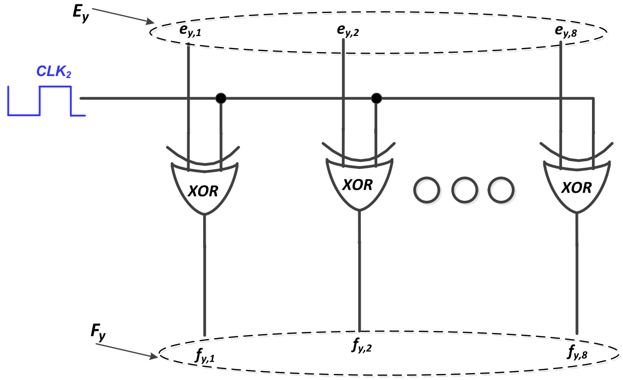


Fig. 16. Internal logic circuits of the yth invert box.

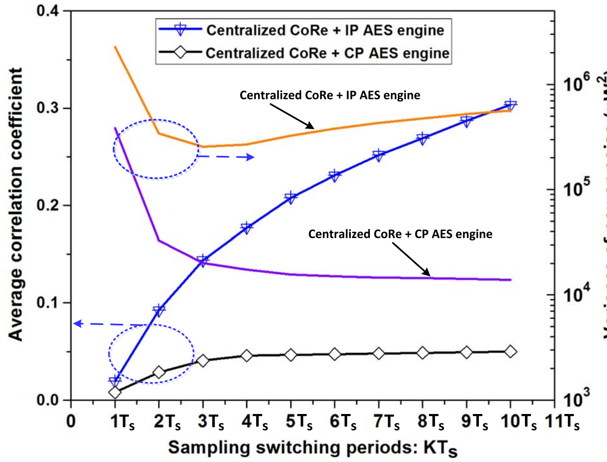


Fig. 17. Sampling switching periods versus average correlation coefficient and variance of power noise of the CP AES engine with a centralized CoRe regulator and the IP AES engine with a centralized CoRe regulator.

$(\overline{f_{y,1}}, \overline{f_{y,2}}, \ldots, \overline{f_{y,8}})_2$, the dynamic power consumption of the yth S-box is $P_{d,y,1}$. When F_y makes a transition from $(\overline{f_{y,1}}, \overline{f_{y,2}}, \ldots, \overline{f_{y,8}})_2$ to $(f_{y,1}, f_{y,2}, \ldots, f_{y,8})_2$, the dynamic power consumption of the yth S-box is $P_{d,y,2}$. The total dynamic power dissipation $\overline{P_{d,y}}$ of the yth S-box within a switching period can be denoted as

$$\overline{P_{d,y}} = \frac{M_1 \times (P_{d,y,1} + P_{d,y,2})}{2}. \tag{34}$$

The mean value $\mu_{I,y}$ and variance $\sigma^2_{I,y}$ of the dynamic power dissipation of the yth S-box within a switching period respectively, are

$$\mu_{I,y} = \frac{(\mu_s + \mu_s) \times \frac{M_1}{2}}{M_1} = \mu_s \tag{35}$$

$$\sigma^2_{I,y} = \frac{(\sigma^2_s + \sigma^2_s) \times \left(\frac{M_1}{2}\right)^2}{M_1^2} = \frac{\sigma^2_s}{2}. \tag{36}$$

Accordingly, the mean value μ_I and variance σ^2_I of the total dynamic power consumption generated by the other 15 S-boxes with constant input plaintext within a switching period become

$$\mu_I = 15\,\mu_s \tag{37}$$

$$\sigma^2_I = 15 \times \frac{\sigma^2_s}{2} = 7.5\,\sigma^2_s. \tag{38}$$

If a centralized CoRe regulator is utilized to deliver power to an IP AES engine, the total sampled input power within K consecutive switching periods $P^{s,I,c}_{\text{in},n}(K,\theta)$ can be obtained as[6]

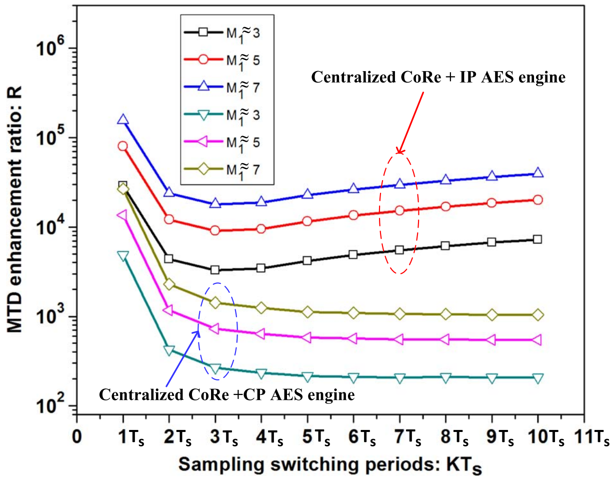
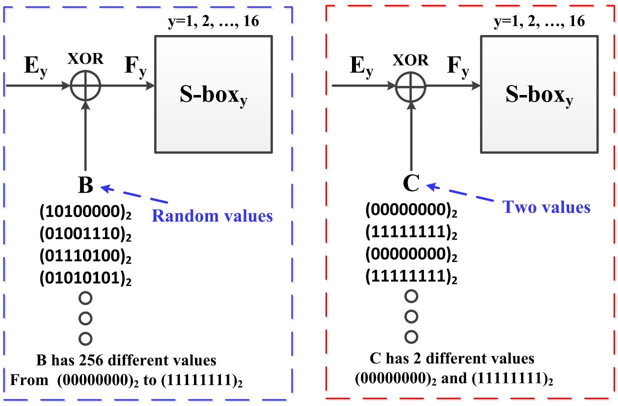


Fig. 18. Sampling switching periods versus MTD enhancement ratio of the CP AES engine with a centralized CoRe regulator and the IP AES engine with a centralized CoRe regulator ($M_1 \approx 3, 5,$ and 7).



(a) (b)

Fig. 19. (a) Masking operation in conventional masked AES engine. (b) Masking operation in the IP AES engine that we proposed.

$$P^{s,I,c}_{\text{in},n}(K,\theta) = A^{I,c}(K,\theta)\left(\frac{\sum_{y=2}^{16}\overline{P_{d,y}}}{\eta_0}\right) + A^{I,c}(K,\theta)\left(\frac{\left(1-\frac{\theta}{2\pi}\right)j_n P_0 + \frac{\theta}{2\pi} j_{n+K} P_0 + \sum_{u=1}^{K-1} j_{n+u} P_0}{\eta_0}\right) \tag{39}$$

where $A^{I,c}(K,\theta)$ is the multiplicative noise. The total dynamic power consumption within a switching period induced by the 15 S-boxes with constant input plaintext is $\sum_{y=2}^{16}\overline{P_{d,y}} \sim N(15\,\mu_s, 7.5\,\sigma^2_s)$. With phase reshuffling operation, the multiplicative noise $A^{I,c}(K,\theta)$ would convert the high dynamic power $\sum_{y=2}^{16}\overline{P_{d,y}}$ into a large additive power noise in the input power profile. As a result, the large additive noise $A^{I,c}(K,\theta)(\sum_{y=2}^{16}\overline{P_{d,y}}/\eta_0)$ can successfully scramble the correlation between the input power and side-channel power in an IP AES engine with a centralized CoRe regulator.

As shown in Fig. 17, as compared to the CP AES engine with a centralized CoRe regulator, the IP AES engine with

[6] Assuming S-box$_1$ is under DPA attacks.

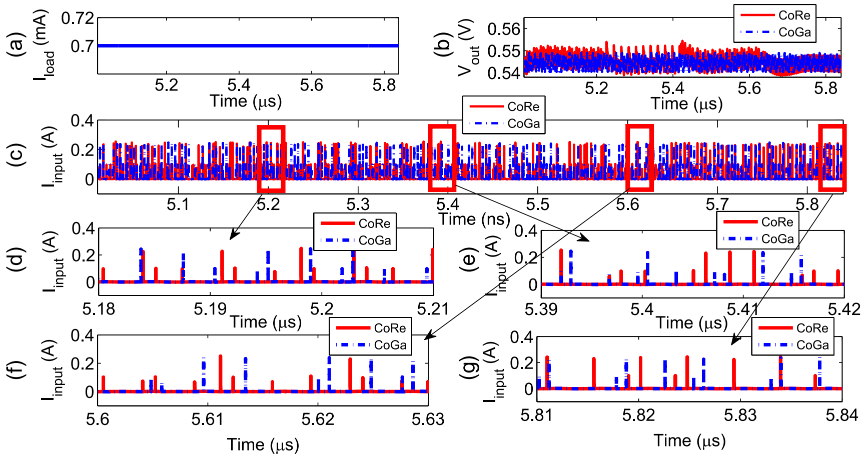


Fig. 20. 8-phase CoGa regulator and 8-phase CoRe regulator are simulated. (a) Distribution of load current, (b) transient output voltage profile, and (c) input current profile of CoGa regulator and CoRe regulator. Sequence of active stages in CoRe regulator is variable while sequence of active stages in CoGa regulator is invariable if a constant load current is enabled, as shown in (d), (e), (f), and (g).

a centralized CoRe regulator has lower correlation coefficient due to the larger variance of the power noise in the IP AES engine with a centralized CoRe regulator. The large power noise arises from the high dynamic power consumption caused by the 15 S-boxes with constant input plaintext. In Fig. 18, the lowest MTD enhancement ratio of the IP AES engine with a centralized CoRe regulator is 9100 when $M_1 \approx 5$ (if $M_1 \approx 3, 7$, the lowest MTD enhancement ratios are 3290, 17 850, respectively) when the attacker samples 3 consecutive switching cycles as one sample of the power data. This value is about 15.7 times higher than the minimum MTD enhancement ratio of the CP AES engine with a centralized CoRe regulator.

The power overhead of the proposed IP AES engine can be justified as follows. When a CP AES engine is working during regular operation (not under attack), all of the 16 S-boxes would show high dynamic power consumption due to the variable input plaintexts. Henceforth, adding invert boxes in the IP AES engine would actually not bring extra power overhead to the S-boxes. The proposed IP AES engine can be considered as a voltage regulator-assisted masked AES engine, which can recover the correct output data by using the same way as a conventional masked AES engine. For the conventional masked AES engine, as shown in Fig. 19(a), the masking random data B is added at the beginning of encryption. The corresponding masking component would be removed at the end of encryption [29], [30]. For the conventional masked AES engine, the input data of S-box $F_y = E_y \oplus B$. However, for the IP AES engine, the input data of S-box is $F_y = E_y \oplus C$ where the masking data C is also added at the beginning of encryption and the corresponding masking component can be removed at the end of encryption by using the same way as the conventional masked AES engine, as shown in Figs. 15 and 19(b).

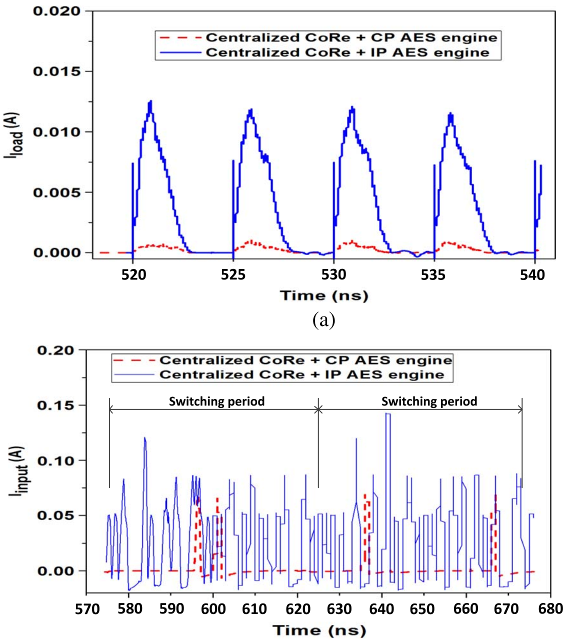
The primary difference between the conventional masked AES engine and IP AES engine we proposed is the masking data. For the conventional AES engine, the masking data B is an 8-bit random value, so B can have $2^8 = 256$ different values. 256 masking values would increase the size of look-up table (LUT) and computational complexity of the AES engine significantly [30]. As a result, the area and performance overhead of the conventional masked AES engine is quite large [30]. For an implemented masked AES engine based on field-programmable gate array (FPGA) [31], the area overhead is 60.1% and the frequency decreases about 11% [31].

However, for the proposed IP AES engine, the masking data C can only have two values: $(00000000)_2$ and $(11111111)_2$ ($E_y \oplus (00000000)_2 = E_y$ and $E_y \oplus (11111111)_2 = \overline{E_y}$). As compared to the conventional masked AES engine, the overhead of IP AES engine would therefore be reduced to $2/256 = 1/128$. The approximate area overhead of the proposed IP AES engine would be around $60.1\% * (1/128) = 0.47\%$ and the frequency reduction of the IP AES engine would be around $11\% * (1/128) = 0.09\%$.

VI. Circuit Level Simulation

The CoGa and CoRe techniques are designed with 130 nm IBM CMOS technology and simulated in Cadence where the switching frequency is swept between 30 and 60 MHz. As shown in Fig. 20, when the load current I_{load} is constant, the CoGa regulator is not triggered, and the active and gated phases do not change as long as the variations in the load current demand are small. However, the sequence of active and passive stages continuously alters over time in the CoRe regulator regardless of the variations in the workload demand. Therefore, as compared to CoGa, input power consumption of the CoRe regulator shows an uncertain sequence of active stages even if the load current demand does not change, increasing the variance of multiplicative power noise in input power profile.

As shown in Fig. 21(a), the dynamic power consumption of an IP AES engine is much higher than the dynamic power consumption of a CP AES engine. The reason is that all 16 S-boxes have high dynamic power dissipation in an IP AES engine while only the S-box under attack contributes to the dynamic power dissipation in a CP AES engine. As shown in Fig. 21(b), only 2 stages are activated in the CP AES engine with a centralized CoRe regulator in a switching cycle while a greater number of stages are turned-on in the centralized CoRe regulator. Hence, the power noise generated by those 15 S-boxes which are not under attack are reshuffled in the input power profile, further reducing the correlation between the input power and side-channel power in the IP AES engine with a centralized CoRe regulator.



(a)

(b)

Fig. 21. (a) Load current profile of a CP AES engine with a centralized CoRe regulator and an IP AES engine with a centralized CoRe regulator. (b) Input current profile of a CP AES engine with a centralized CoRe regulator and an IP AES engine with a centralized CoRe regulator (The total number of phases of the centralized CoRe regulator is 64).

VII. Conclusion

An on-chip CoRe technique is utilized to reinforce a lightweight AES engine as an efficient countermeasure against power analysis attacks due to the high multiplicative power noise induced by reshuffling active and gated converter stages. A detailed analytical analysis of the correlation between the input and output power of both conventional and proposed voltage regulation techniques is presented. The security implications of the physical placement of the voltage regulators are investigated with centralized and distributed implementations of the CoRe regulators. An improved AES engine is proposed to further scramble the input power even when the attacker applies a constant plaintext to the S-boxes that are not under attack. The security implications of the proposed techniques are analytically proven using the correlation coefficient. When a centralized CoRe regulator is combined with the proposed improved pipelined AES engine, the MTD value is enhanced over 9100 times as compared to an unprotected AES engine.

Appendix
Correlation Coefficient Derivation of Conventional On-Chip Voltage Regulators

If the attacker decides to sample the total input power consumption within K consecutive switching periods as one sample of the power data in a COC VR that provides power to a single S-box, the total sampled input power $P'_{\mathrm{in},n}(K,\theta)$ within K consecutive switching periods is

$$P'_{\mathrm{in},n}(K,\theta) = \left(1-\frac{\theta}{2\pi}+\frac{\Delta t}{T_s}\right)\frac{j_{n+1}P_0}{\eta_1} + \left(\frac{\theta}{2\pi}-\frac{\Delta t}{T_s}\right)\frac{j_{n+K+1}P_0}{\eta_1} + \sum_{u=2}^{K}\frac{j_{n+u}P_0}{\eta_1}. \quad (40)$$

The mean value of the total sampled input power within K consecutive switching periods of a COC VR $\mu_c(K,\theta)$ is

$$\mu_c(K,\theta) = \left(1-\frac{\theta}{2\pi}+\frac{\Delta t}{T_s}\right)\mu'_c + \left(\frac{\theta}{2\pi}-\frac{\Delta t}{T_s}\right)\mu'_c + (K-1)\mu'_c = K\mu'_c \quad (41)$$

where μ'_c is

$$\mu'_c \approx \sum_{j=j_{\min}}^{j_{\max}} \frac{jP_0\sqrt{M_1}}{\eta_1\sigma_s\sqrt{2\pi}} \exp^{\left(-\frac{(j\times P_0-\mu_s)^2}{2\sigma_s^2/M_1}\right)}. \quad (42)$$

The variance of total sampled input power within K consecutive switching periods of a COC VR $\sigma_c^2(K,\theta)$ is

$$\sigma_c^2(K,\theta) = \left(1-\frac{\theta}{2\pi}+\frac{\Delta t}{T_s}\right)(\sigma'_c)^2 + \left(\frac{\theta}{2\pi}-\frac{\Delta t}{T_s}\right)(\sigma'_c)^2 + (K-1)\left(\sigma'_c\right)^2 = K\left(\sigma'_c\right)^2 \quad (43)$$

where $(\sigma'_c)^2$ is

$$(\sigma'_c)^2 = \frac{1}{j_{\max}-j_{\min}+1}\sum_{j=j_{\min}}^{j_{\max}}\left(jP_0/\eta_1-\mu'_c\right)^2. \quad (44)$$

The correlation coefficient $\gamma_c(K,\theta)$ of a COC VR can therefore be obtained as

$$\gamma_c(K,\theta) = \frac{E\left(P'_{\mathrm{in},n}(K,\theta)\times P_{\mathrm{load},n}(K,\theta)\right)}{\sigma_c(K,\theta)\times\sqrt{K/M_1\sigma_s}} - \frac{\mu_c(K,\theta)\times K\mu_s}{\sigma_c(K,\theta)\times\sqrt{K/M_1\sigma_s}} \quad (45)$$

where

$$\begin{aligned} &E\left(P'_{\mathrm{in},n}(K,\theta)\times P_{\mathrm{load},n}(K,\theta)\right)\\ &= \frac{1}{(j_{\max}-j_{\min}+1)^{K+1}}\\ &\times\left(\sum_{j_{n+K+1}=j_{\min}}^{j_{\max}}\cdots\sum_{j_{n+1}=j_{\min}}^{j_{\max}}\right.\\ &\times\left(\left(\left(1-\frac{\theta}{2\pi}+\frac{\Delta t}{T_s}\right)\frac{j_{n+1}P_0}{\eta_1}\right.\right.\\ &\left.+\left(\frac{\theta}{2\pi}-\frac{\Delta t}{T_s}\right)\frac{j_{n+K+1}P_0}{\eta_1}+\sum_{u=2}^{K}\frac{j_{n+u}P_0}{\eta_1}\right)\\ &\left.\left.\times\left(\left(1-\frac{\theta}{2\pi}\right)j_{n+1}P_0+\frac{\theta}{2\pi}j_{n+K+1}P_0+\sum_{u=2}^{K}j_{n+u}P_0\right)\right)\right). \end{aligned} \quad (46)$$

Accordingly, the average correlation coefficient of a COC VR $\overline{\gamma_c(K)}$ can be denoted as

$$\overline{\gamma_c(K)} = \frac{1}{2\pi}\int_0^{2\pi}\gamma_c(K,\theta)d\theta. \quad (47)$$

References

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

[2] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *Proc. VLSI Design*, Jan. 2007, pp. 854–862.

[3] 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.

[4] D. Wu, X. Cui, W. Wei, R. Li, D. Yu, and X. Cui, "Research on circuit level countermeasures for differential power analysis attacks," in *Proc. Solid-State Integr. Circuit Technol.*, Oct. 2012, pp. 1–3.

[5] 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.

[6] 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 *Proc. Design Autom. Conf. (DAC)*, Jun. 2013, pp. 1–9.

[7] G. Khedkar, D. Kudithipudi, and G. S. Rose, "Power profile obfuscation using nanoscale memristive devices to counter DPA attacks," *IEEE Trans. Nanotechnol.*, vol. 14, no. 1, pp. 26–35, Jan. 2015.

[8] F. Regazzoni, T. Eisenbarth, J. Grobschadl, L. Breveglieri, P. Ienne, I. Koren, and C. Paar, "Power attacks resistance of cryptographic S-boxes with added error detection circuits," in *Proc. 22nd IEEE Int. Symp. Defect Fault-Tolerance VLSI Syst.*, Sep. 2007, pp. 508–516.

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

[10] J. D. Vos, D. Flandre, and D. Bol, "A sizing methodology for on-chip switched-capacitor DC/DC converters," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 5, pp. 1597–1606, May 2014.

[11] Y. Lu, Y. Wang, Q. Pan, W.-H. Ki, and C. P. Yue, "A fully-integrated low-dropout regulator with full-spectrum power supply rejection," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 3, pp. 707–716, Mar. 2015.

[12] S.-W. Hong and G.-H. Cho, "High-gain wide-bandwidth capacitor-less low-dropout regulator (LDO) for mobile applications utilizing frequency response of multiple feedback loops," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 1, pp. 46–57, Jan. 2016.

[13] O. A. Uzun and S. Kose, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 4, no. 2, pp. 169–179, Jun. 2014.

[14] W. Yu, O. A. Uzun, and S. Kose, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *Proc. Design Autom. Conf. (DAC)*, Jun. 2015, pp. 1–6.

[15] 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.

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

[17] Z. Toprak-Deniz, M. Sperling, J. F. Bulzacchelli, G. Still, R. Kruse, S. Kim, D. Boerstler, T. Gloekler, R. Robertazzi, K. Stawiasz, T. Diemoz, G. English, D. Hui, P. Muench, and J. Friedrich, "Distributed system of digitally controlled microregulators enabling per-core DVFS for the POWER8 microprocessor," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Feb. 2014, pp. 98–99.

[18] S. Kose and E. G. Friedman, "Distributed on-chip power delivery," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 2, no. 4, pp. 704–713, Dec. 2012.

[19] 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. (VLSI) Syst.*, vol. 22, no. 9, pp. 1954–1967, Sep. 2014.

[20] A. Hodjat and I. Verbauwhede, "Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors," *IEEE Trans. Comput.*, vol. 55, no. 4, pp. 366–372, Apr. 2006.

[21] F. Wu, L. Wang, and J. Wan, "A low cost and inner-round pipelined design of ECB-AES-256 crypto engine for solid state disk," in *Proc. Netw., Archit., Storage (NAS)*, Jul. 2010, pp. 485–491.

[22] T. Good and M. Benaissa, "Very small FPGA application-specific instruction processor for AES," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 7, pp. 1477–1486, Jul. 2006.

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

[24] E. A. Burton, G. Schrom, F. Paillet, J. Douglas, W. J. Lambert, K. Radhakrishnan, and M. J. Hill, "FIVR-fully integrated voltage regulators on 4th generation Intel Core SoCs," in *Proc. Appl. Power Electron. Conf. Expo. (APEC)*, Mar. 2014, pp. 432–439.

[25] P. A. Hung, K. Klomkarn, and P. Sooraksa, "Image encryption based on chaotic map and dynamic S-box," in *Proc. Intell. Signal Process. Commun. Syst. (ISPACS)*, Nov. 2013, pp. 435–439.

[26] A. Joshi, P. K. Dakhole, and A. Thatere, "Implementation of S-Box for advanced encryption standard," in *Proc. Eng. Technol. (ICETECH)*, Mar. 2015, pp. 1–5.

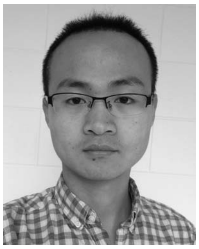
[27] J. Park, S. Moon, D. Choi, Y. Kang, and J. Ha, "Fault attack for the iterative operation of AES S-Box," in *Proc. Comput. Sci. Convergence Inf. Technol. (ICCIT)*, Nov. 2010, pp. 550–555.

[28] 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," *Integr., VLSI J.*, vol. 46, no. 4, pp. 333–344, Sep. 2013.

[29] 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.

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

[31] N. Kamoun, L. Bossuet, and A. Ghazel, "Correlated power noise generator as a low cost DPA countermeasures to secure hardware AES cipher," in *Proc. Signals, Circuits, Syst. (SCS)*, Nov. 2009, pp. 1–6.



Weize Yu received the B.S. and M.S. degrees in electrical engineering from University of Electronic Science and Technology of China, Chengdu, and Institute of Microelectronics of Chinese Academy of Sciences, Beijing, in 2009 and 2012, respectively. Currently, he is working toward the Ph.D. degree in University of South Florida, Tampa, FL, USA.

His current research interests are on-chip power management and hardware security.

Selçuk Köse (S'10–M'12) received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from the University of Rochester, Rochester, NY, USA, in 2008 and 2012, respectively.

He is currently an Assistant Professor with the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA. He previously worked at the VLSI Design Center of the Scientific and Technological Research Council (TUBITAK), Ankara, the Central Technology and Special Circuits Team in the enterprise microprocessor division of Intel Corporation, Santa Clara, CA, USA, and the RF, Analog, and Sensor Group, Freescale Semiconductor, Tempe, AZ, USA. His current research interests include the analysis and design of high performance integrated circuits, on-chip DC-DC converters, and hardware security.

Prof. Köse is an Associate Editor of the *Journal of Circuits, Systems, and Computers* and *Microelectronics Journal*. He has served on the Technical Program and Organization Committees of various conferences. He is the recipient of NSF CAREER Award, Cisco Research Award, USF College of Engineering Outstanding Junior Researcher Award, and USF Outstanding Faculty Award.