Transactions Briefs

Security-Adaptive Voltage Conversion as a Lightweight Countermeasure Against LPA Attacks

Weize Yu and Selçuk Köse

***Abstract*— A voltage converter with adaptive security features is proposed as a lightweight countermeasure against leakage power analysis (LPA) attacks. When an LPA attack is sensed by the proposed security-adaptive (SA) voltage converter, a discharging resistor starts sinking redundant current to alter the signature of the load power dissipation. The power dissipation induced by the discharging resistor is scrambled by the SA voltage converter to maximize the amount of the inserted noise to the input power profile of the cryptographic against LPA attacks. As compared with a conventional cryptographic circuit that does not house any countermeasure, the lowest measurement-to-disclose value of a cryptographic circuit that employs the proposed voltage converter can be enhanced over 6145 times against LPA attacks.**

***Index Terms*— Discharging resistor, inserted noise, leakage power analysis (LPA) attacks, measurement-to-disclose (MTD), security-adaptive (SA).**

I. Introduction

The power consumption of CMOS-based cryptographic circuits depends strongly on the data that is being processed. The correlation between the power consumption and processed data can be exploited by a malicious attacker with side-channel attacks (SCAs) to obtain the stored critical information [1]. Differential power analysis (DPA) attacks are one of the most widely studied SCAs that exploit the switching activities within the cryptographic circuits while processing different input data. Recently leakage power analysis (LPA) attacks have been proposed by Alioto *et al.* [2] to obtain the critical information by analyzing the correlation between the input data and leakage power dissipation. LPA attacks exploit the fact that the leakage current signature of nMOS and pMOS transistors is different [2]. The amplitude of the leakage power is on the orders of magnitude smaller than the amplitude of dynamic power consumption. To perform a successful LPA attack, the attacker must mitigate the measurement noise that can make the analysis quite difficult due to the small signal-to-noise ratio (SNR) of the monitored leakage power. An effective technique to mitigate the measurement noise is to lower the operating frequency of the cryptographic circuit [3].

Since the leakage mechanisms in the DPA and the LPA attacks are quite different, DPA-resistant cryptographic circuits may still be vulnerable against LPA attacks [4]. There is, therefore, a strong need for effective countermeasures against LPA attacks. Converter-reshuffling (CoRe) technique has been proposed in [5] and [6] as a countermeasure against DPA attacks with low overhead. CoRe technique utilizes a multiphase switched-capacitor (SC) voltage converter where each phase delivers a portion of the required power to the cryptographic circuit with a different time delay. A pseudorandom number generator (PRNG) is used to scramble the sequence of activate phases to insert a varying amount of uncertain power noise in each switching period against DPA attacks. However, if the attacker implements an LPA attack on a cryptographic circuit with a CoRe voltage converter, the low leakage power dissipation generated by the cryptographic circuit would only activate a small number of converter phases. The small number of active phases would significantly reduce the entropy of the PRNG in the CoRe voltage converter, making the CoRe technique vulnerable against LPA attacks.

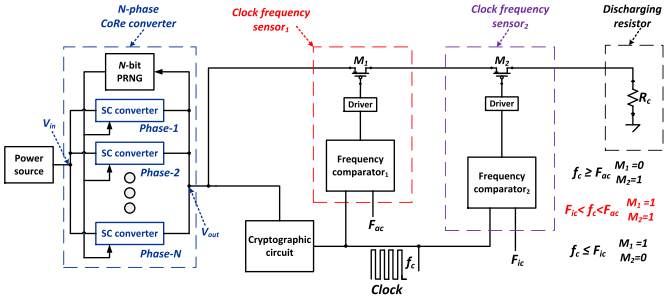


Fig. 1. Architecture of the proposed SA voltage converter. N is the total number of phases (N is an even). Switch $M_{i_1} = 1$ ($i_1 = 1, 2$) represents that it is in ON-state and *vice versa*.

To increase security against LPA attacks with negligible overhead, in this brief, the voltage regulator is designed in a security-adaptive (SA) fashion. The SA voltage converter is designed based on the CoRe voltage converter [5], [6] but modified to monitor LPA attacks and insert noise with a discharging resistor only when the device is under an LPA attack. When the SA voltage converter is utilized as the supply voltage of the cryptographic circuit, during the normal[1] and idle[2] modes of operation, no redundant current is being consumed and the SA voltage converter operates conventionally as a CoRe voltage converter. The SA voltage converter is triggered to sink redundant current when the operating clock frequency f_c is within a certain range, as explained in Section II. The activity of the discharging resistor is controlled by the PRNG to scramble the inserted noise profile. Since the proposed SA converter is only triggered to sink current when the device is under an LPA attack, the power overhead of this countermeasure is negligible.

The rest of this paper is organized as follows. The architecture and parameter design of the SA voltage converter are introduced in Sections II and III, respectively. Security evaluation against LPA attacks is offered in Section IV. Circuit level verification and LPA attack simulations are provided in Sections V and VI, respectively. Conclusions are given in Section VII.

II. Architecture Design

The proposed SA voltage converter consists of a CoRe voltage converter, two clock frequency sensors, and a discharging resistor, as shown in Fig. 1. When a cryptographic circuit is in a normal

Manuscript received August 22, 2016; revised November 24, 2016 and January 5, 2017; accepted February 9, 2017. Date of publication March 1, 2017; date of current version June 23, 2017. This work was supported in part by the NSF CAREER Award under Grant CCF-1350451, in part by the USF Presidential Fellowship, and in part by the Cisco Research Award.

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/TVLSI.2017.2670537

[1] In a normal working mode, clock frequency f_c is high.

[2] In the idle mode, the clock frequency f_c is low.

working mode, the cryptographic circuit exhibits a high dynamic power consumption (i.e., the clock frequency f_c is high), M_1 transistor would be in OFF-state to let the SA voltage converter operate similar to the CoRe voltage converter. Under an LPA attack, however, the attacker would lower the clock frequency f_c to mitigate the measurement noise [3]. If the clock frequency f_c is lower than the active critical frequency F_{ac} and higher than the idle critical frequency F_{ic}, both M_1 transistor and M_2 transistor would be in ON-state, letting some amount of redundant current flow through the discharging resistor R_c. The redundant power dissipation induced by R_c is then reshuffled by the N-phase CoRe converter to scramble the inserted power noise.

When the clock frequency f_c is lower than the idle critical frequency F_{ic}, the M_2 transistor would be turned-OFF, deactivating the discharging resistor R_c as shown in Fig. 1. When the cryptographic circuit is in an idle mode ($f_c \ll F_{ic}$), the discharging resistor R_c is therefore inactive to avoid power overhead. The design guidelines on the selection of suitable F_{ic} and F_{ac} to maximize security are provided in Section IV and Appendix, respectively.

III. Parameter Design

To maximize the entropy of the N-bit PRNG that resides within the SA voltage converter, the number of active phases of an SA voltage converter in each switching period should be around $N/2$ (the entropy of the N-bit PRNG reaches the maximum value $-\binom{N}{N/2} \times (1/\binom{N}{N/2}) \log_2^{(1/\binom{N}{N/2})} = \log_2^{\binom{N}{N/2}}$). Let us assume that the mean value of leakage power dissipation of the cryptographic circuit within a switching period under LPA attacks is μ_c and the output voltage of an N-phase CoRe converter within the SA voltage converter is V_{out}. When the cryptographic circuit employs an SA voltage converter, if the discharging resistor R_c is activated, the power dissipation P_c consumed by the discharging resistor R_c can be denoted as $P_c = V_{\text{out}}^2/R_c$. The mean value μ_t of the total load power dissipation of the SA voltage converter within a switching period can be approximated as

$$\mu_t \approx \mu_c + \frac{V_{\text{out}}^2}{R_c}. \tag{1}$$

The output current I_{out} of a single SC converter phase is [7]

$$I_{\text{out}} = 2C_f(V_{\text{in}} - 2V_{\text{out}})kf_s \tag{2}$$

where C_f is the flying capacitance within each phase, V_{in} is the input voltage, f_s is the switching frequency of the SC converter, and k is an f_s- and C_f-dependent parameter, which can be found in [7].

Since around half of the total phases should be active in each switching period to maximize the entropy of the N-bit PRNG, the following approximated equation should be satisfied

$$V_{\text{out}} \times \frac{N}{2} \times I_{\text{out}} \approx \mu_c + \frac{V_{\text{out}}^2}{R_c'} \tag{3}$$

where R_c' is the optimized resistance value of the discharging resistor R_c that maximizes the security of the cryptographic circuit. R_c', therefore, can be determined as

$$R_c' \approx \frac{V_{\text{out}}^2}{V_{\text{out}}NC_f(V_{\text{in}} - 2V_{\text{out}})kf_s - \mu_c}. \tag{4}$$

IV. Security Evaluation Against LPA Attacks

To quantify the security of a cryptographic circuit that employs the proposed SA voltage converter against LPA attacks, the correlation coefficient γ between the input and load power profile of the SA voltage converter is modeled as

$$\gamma = \frac{\sum_{i=1}^{n}(P_{l,i} - \overline{P_l})(P_{\text{in},i} - \overline{P_{\text{in}}})}{\sqrt{\sum_{i=1}^{n}(P_{l,i} - \overline{P_l})^2 \sum_{i=1}^{n}(P_{\text{in},i} - \overline{P_{\text{in}}})^2}} \tag{5}$$

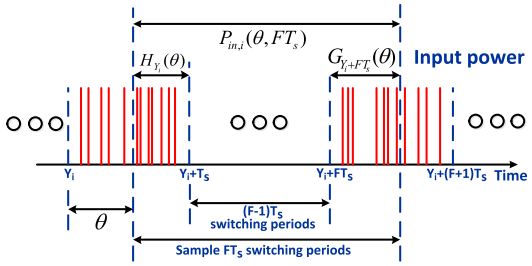


Fig. 2. Input power profile of a cryptographic circuit that employs an SA voltage converter under LPA attacks when the attacker selects a single clock period as one sample of input power data. T_s is the switching period of the SA voltage converter, Y_i is the starting time point of the first switching period for sampling the ith input power data, and θ is the phase difference between the switching period and input power data sampling.

where n is the total number of the input or load power data samples, $P_{l,i}$ ($P_{\text{in},i}$) is the ith, ($i = 1, 2, \ldots, n$) load (input) power of the voltage converter, and $\overline{P_l}$ ($\overline{P_{\text{in}}}$) is the corresponding total average load (input) power.

A. Sampling a Single Clock Period as One Sample of Input Power

In LPA attacks, to filter the measurement noise, the clock frequency f_c of the cryptographic circuit needs to be sufficiently reduced [3] (i.e., $f_c \approx (1/F_0)f_s$ where F_0 is an integer that can reasonably filter out the measurement noise). However, when a cryptographic circuit implemented with a CoRe or an SA voltage converter is under LPA attacks, in addition to filtering the measurement noise, the reshuffling noise induced by PRNG can also be reduced if the clock frequency f_c is further reduced. For example, the clock frequency f_c can be reduced to $f_c \approx (1/F)f_s$ (F is an integer and $F > F_0$) to also filter the reshuffling noise.

If the attacker selects a single clock period (F number of switching periods) as one sample of the input power data as shown in Fig. 2, the sampled input power $P_{\text{in},i}(\theta, FT_s)$ is

$$P_{\text{in},i}(\theta, FT_s) = (H_{Y_i}(\theta) + G_{Y_i+FT_s}(\theta))P_0 + \frac{(F-1)\left(P_i + \frac{V_{\text{out}}^2}{R_c}\right)}{\eta_c} \tag{6}$$

where η_c is the power efficiency of the N-phase CoRe converter in the SA voltage converter, P_0 is the power consumed by a single active phase, and P_i is the leakage power dissipation of the cryptographic circuit induced by the ith input data. $H_{Y_i}(\theta)$ and $G_{Y_i+FT_s}(\theta)$ are the number of active phases, as shown in Fig. 2. The corresponding load power $P_{l,i}(\theta, FT_s)$ of the SA voltage converter (which is correlated with $P_{\text{in},i}(\theta, FT_s)$ that can be written as

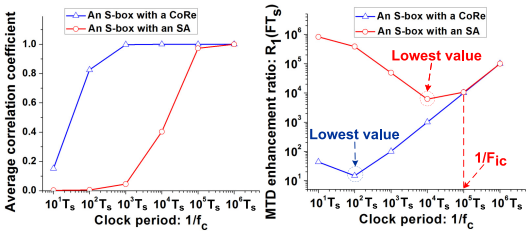
$$P_{l,i}(\theta, FT_s) = (1 - \frac{\theta}{2\pi})P_i + (F-1)P_i + \frac{\theta}{2\pi}P_i = FP_i. \tag{7}$$

As compared with a conventional cryptographic circuit (i.e., without any countermeasure), the measurement-to-disclose (MTD) enhancement ratio $R(FT_s)$ of a cryptographic circuit that employs a voltage converter is [6]

$$R(FT_s) \propto \frac{1}{\left(\frac{1}{2\pi}\int_0^{2\pi}\gamma(\theta, FT_s)d\theta\right)^2} \tag{8}$$

where $(1/2\pi)\int_0^{2\pi}\gamma(\theta, FT_s)d\theta$ is the average correlation coefficient between the input and output power profile of the voltage converter.

As compared with an LPA attack on a conventional cryptographic circuit with clock frequency $f_c \approx \left(\frac{1}{F_0}\right)f_s$, the MTD value would be enhanced by F/F_0 times if the attacker implements an LPA attack on a cryptographic circuit, which employs a voltage converter with a slower clock frequency $f_c \approx (1/F)f_s$. As a result, the MTD enhancement ratio $R_1(FT_s)$ of a cryptographic circuit that employs a voltage converter with a variable clock frequency can be



(a) (b)

Fig. 3. (a) Average correlation coefficient versus clock period $1/f_c$. (b) MTD enhancement ratio $R_1(FT_s)$ versus clock period $1/f_c$.

written as

$$R_1(FT_s) \simeq \frac{F}{F_0} \frac{1}{\left(\frac{1}{2\pi}\int_0^{2\pi} \gamma(\theta, FT_s)d\theta\right)^2}. \tag{9}$$

Advanced encryption standard utilizes multiple substitution-boxes (S-boxes) to perform nonlinear mathematical transformations to mask the relationship between the ciphertext and the secret key [2]. To validate the mathematical analysis, a 130-nm CMOS S-box [8] is used as the cryptographic circuit that is powered, respectively, by a CoRe voltage converter and by an SA voltage converter. Both circuits are simulated in Cadence where $\{F_0 = 10\}$[3] and $N = 32$. The average correlation coefficient of the SA voltage converter is quite lower than the average correlation coefficient of the CoRe voltage converter when the attacker selects a fast clock frequency to perform the LPA attack, as shown in Fig. 3(a). The lowest MTD enhancement ratio of an S-box that employs an SA voltage converter under LPA attacks is ~6145 when clock period is about $10^4 T_s$ while the lowest MTD enhancement ratio of an S-box that employs a CoRe voltage converter under LPA attacks is about 14.7 when clock period is about $10^2 T_s$, as shown in Fig. 3(b).

B. Sampling Multiple Clock Periods as One Sample of Input Power

The technique of sampling multiple clock/switching periods as one sample of input power data is quite efficient for filtering the power noise generated from reshuffling-based voltage converters in DPA attacks [6]. When an attacker implements an LPA attack on a cryptographic circuit that houses a CoRe voltage converter or an SA voltage converter, the attacker can also filter the reshuffling noise by sampling $K, (K \geq 2)$ number of clock periods as one sample of input power data instead of lowering the clock frequency ($f_c \approx (1/F_0) f_s$) further, as shown in Fig. 4. The corresponding input power $P_{\text{in},i}(\theta, KF_0T_s)$ and load power $P_{l,i}(\theta, KF_0T_s)$ of the SA voltage converter can be, respectively, written as

$$\begin{aligned} P_{\text{in},i}(\theta, KF_0T_s) &= (W_{X_i}(\theta) + U_{X_i+KF_0T_s}(\theta))P_0 \\ &\quad + \frac{(F_0-1)\left(P_{(i-1)K+1} + \frac{V_{\text{out}}^2}{R_c}\right)}{\eta_c} \\ &\quad + F_0 \sum_{j=2}^{K} \frac{\left(P_{(i-1)K+j} + \frac{V_{\text{out}}^2}{R_c}\right)}{\eta_c} \end{aligned} \tag{10}$$

$$\begin{aligned} P_{l,i}(\theta, KF_0T_s) &= \left(1 - \frac{\theta}{2\pi}\right)P_{(i-1)K+1} + (F_0-1)P_{(i-1)K+1} \\ &\quad + F_0 \sum_{j=2}^{K} P_{(i-1)K+j} + \frac{\theta}{2\pi} P_{(i-1)K+K+1} \end{aligned} \tag{11}$$

[3]From the experimental results in [3], the measurement noise can be reasonably filtered if the clock frequency f_c is lowered 100 times. In the simulation, the clock frequency in a normal working mode is about ten times of the switching frequency and 100 times of the clock frequency in the idle mode, therefore, F_0 is selected as 10.

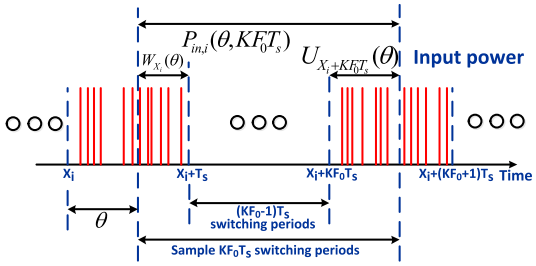
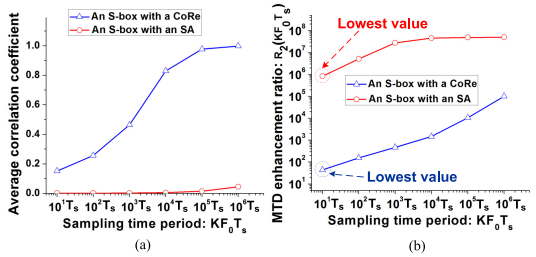
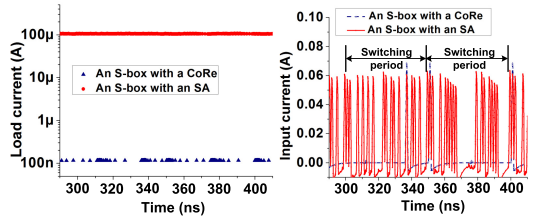


Fig. 4. Input power profile of a cryptographic circuit that employs an SA voltage converter under LPA attacks when the attacker selects a variable number of clock periods as one sample of input power data. X_i is the starting time point of the first switching period for sampling the ith input power data.



(a) (b)

Fig. 5. (a) Average correlation coefficient versus sampling time period KF_0T_s. (b) MTD enhancement ratio $R_2(KF_0T_s)$ versus sampling time period KF_0T_s ($F_0 = 10$ and $N = 32$).



(a) (b)

Fig. 6. (a) Load current profile of an S-box that employs a CoRe voltage converter and an S-box that employs an SA voltage converter. (b) Input current profile of an S-box that employs a CoRe voltage converter and an S-box that employs an SA voltage converter.

where $P_{(i-1)K+j}$, $(j = 1, 2, \ldots)$ is the leakage power dissipation of the cryptographic circuit induced by the $((i-1)K + j)$th input data. $W_{X_i}(\theta)$ and $U_{X_i+KF_0T_s}(\theta)$ are the corresponding number of active phases, as shown in Fig. 4.

As compared with sampling a single clock period as one sample of input power data, sampling K number of clock periods as one sample of input power data would enhance the MTD value by K times [6]. Therefore, the MTD enhancement ratio $R_2(KF_0T_s)$ of a cryptographic circuit that employs a voltage converter is

$$R_2(KF_0T_s) \simeq K \frac{1}{\left(\frac{1}{2\pi}\int_0^{2\pi} \gamma(\theta, KF_0T_s)d\theta\right)^2} \tag{12}$$

when utilizing K number of clock periods as one sample of input power data.

When the attacker increases the sampling time period to KF_0T_s, the average correlation coefficient of the SA voltage converter has a marginal enhancement, as shown in Fig. 5(a). This indicates that sampling multiple clock periods as one sample of input power data to mitigate noise is not sufficiently effective. The lowest MTD enhancement ratio of an S-box with an SA (CoRe) voltage converter is 826446 (43) [shown in Fig. 5(b)], which is much higher than

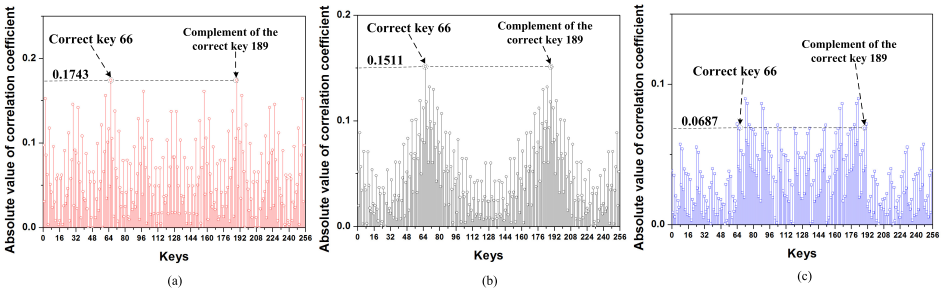


Fig. 7. LPA attacks simulation ($N = 32$ and $F_0 = 10$. Hamming-weight model is utilized where the correct key and complement of the correct key can be discriminated from the polarity of the correlation coefficient [2]. Absolute value of the correlation coefficient is used to make the highest correlation coefficient visually more distinguishable). (a) All of the possible keys versus absolute value of the correlation coefficient for an S-box without countermeasure after analyzing 500 leakage power traces. (b) All of the possible keys versus absolute value of correlation coefficient for an S-box that employs a CoRe voltage converter after analyzing two million leakage power traces. (c) All of the possible keys versus absolute value of the correlation coefficient for an S-box that employs an SA voltage converter after analyzing two million leakage power traces.

the lowest MTD enhancement ratio 6145 (14.7) [shown in Fig. 3(b)]. That means further reducing the clock frequency f_c is more effective than sampling multiple clock periods as one sample of input power data to enhance the power of LPA attacks on an S-box with a voltage converter. The primary reason is that under the same sampling time period ($FT_s = KF_0T_s$), the variance of the load power of a voltage converter with a variable clock frequency $D(P_{l,i}(\theta, FT_s))$ is

$$D(P_{l,i}(\theta, FT_s)) = D(FP_i) = D(KF_0P_i) = K^2F_0^2\sigma_s^2 \quad (13)$$

where σ_s^2 is the variance of the leakage power dissipation. However, the variance of load power of a voltage converter while sampling K number of clock periods as one sample of input power data $D(P_{l,i}(\theta, KF_0T_s))$ is ($F_0 > 1$)

$$\begin{aligned} &D(P_{l,i}(\theta, KF_0T_s)) \\ &= \left(F_0 - \frac{\theta}{2\pi}\right)^2\sigma_s^2 + F_0^2(K-1)\sigma_s^2 + \left(\frac{\theta}{2\pi}\right)^2\sigma_s^2 \\ &= KF_0^2\sigma_s^2 - \frac{\theta}{\pi}F_0\sigma_s^2 + \frac{\theta^2}{2\pi^2}\sigma_s^2 < KF_0^2\sigma_s^2 - \frac{\theta}{\pi}\sigma_s^2 + \frac{\theta^2}{2\pi^2}\sigma_s^2 \\ &\leq KF_0^2\sigma_s^2 - \frac{\theta}{\pi}\frac{\theta}{2\pi}\sigma_s^2 + \frac{\theta^2}{2\pi^2}\sigma_s^2 = KF_0^2\sigma_s^2. \end{aligned} \quad (14)$$

As compared with sampling K number of clock periods as one sample of input power, lowering clock frequency f_c can therefore enhance the variance of the load power of the voltage converter over K times. A larger variance of the load power enhances the SNR of the voltage converter and decreases the lowest MTD enhancement ratio.

Lowering clock frequency f_c further is more efficient than sampling multiple clock periods as one sample of input power data to enhance the power of LPA attacks. When the attacker further lowers clock frequency f_c, as shown in Fig. 3(b), the idle critical frequency F_{ic} can be selected as $1/(10^5T_s)$. The intuitive explanation is that when the clock frequency f_c is lower than the idle critical frequency $F_{ic} = 1/(10^5T_s)$, the M_2 transistor would be turned-OFF to make the SA voltage converter behave as a CoRe voltage converter. The MTD enhancement ratio of an S-box with an SA voltage converter is almost the same as the MTD enhancement ratio of an S-box with a CoRe voltage converter when the clock frequency f_c is lower than $1/(10^5T_s)$, as shown in Fig. 3(b). The security of an S-box with an SA voltage converter against LPA attacks therefore would not be compromised when $F_{ic} = 1/(10^5T_s)$.

V. Circuit Level Verification

To validate the proposed countermeasure with circuit level simulations, a 130-nm CMOS S-box [8] is used as the load to simulate the correlations between the input and load power profile of different voltage converters. A 32-phase 2:1 CoRe voltage converter and a 32-phase 2:1 SA voltage converter are used in the simulations. The detailed architecture and control algorithm of the CoRe voltage converter can be found in [6]. The input voltage V_{in} and output voltage V_{out} of the voltage converters used in the simulations are, respectively, 2.4 and 1.2 V. Additionally, the clock frequency f_c of the S-box to perform an LPA attack is reduced to 2 MHz and the variation range of the switching frequency f_s of the voltage converter is $f_s \in [19, 21\ \text{MHz}]$.

The load current of the SA voltage converter is significantly higher than the CoRe voltage converter when the S-box is under an LPA attack, as shown in Fig. 6(a). The high load power dissipation from the discharging resistor R_c is reshuffled in the input power profile to generate high power noise against LPA attacks. As shown in Fig. 6(b), only a single phase is active in a switching period in an S-box that employs a CoRe voltage converter while 16 phases are activated in a switching period in an S-box that employs an SA voltage converter. The large number of active phases in each switching period would enhance the entropy of the PRNG from $\log_2\binom{32}{1}$ to $\log_2\binom{32}{16}$, generating a large amount of uncertain power noise in the input power profile against LPA attacks.

VI. LPA Attacks Simulation

When LPA attacks are implemented (simulated) on an S-box [8] that does not house any countermeasure, the correct key [which is $(66)_{10}$ in this example] is leaked to the attacker after analyzing 500 leakage power traces, as shown in Fig. 7(a). When the attacker implements an LPA attack on an S-box that employs an SA voltage converter and lowers the clock frequency f_c to $1/(10^4T_s)$ [clock frequency with lowest MTD enhancement ratio as shown in Fig. 3(b)], the correct key cannot be obtained by the attacker even after analyzing two million leakage power traces, as shown in Fig. 7(c). By contrast, when the attacker lowers the clock frequency f_c to $1/(10^4T_s)$ and implements an LPA attack on an S-box, which employs a CoRe voltage converter, after analyzing two million leakage power traces, the correct key is leaked to the attacker, as shown in Fig. 7(b).

Therefore, as compared with an S-box that employs a CoRe voltage converter, the reshuffled redundant load power dissipation in the SA voltage converter can successfully act as noise to enhance the MTD value.

VII. Conclusion

An SA voltage converter is utilized as a lightweight countermeasure against LPA attacks. The discharging resistor in the SA voltage

converter can significantly increase the amount of noise insertion in the input power profile when LPA attacks are sensed by the proposed technique. Through scrambling the redundant load power dissipation in the input power profile, the MTD value of a cryptographic circuit that employs the SA voltage converter is enhanced over 6145 times as compared with the MTD value of a conventional cryptographic circuit that has no countermeasure.

APPENDIX
GUIDELINES ON THE SELECTION OF A SUITABLE ACTIVE CRITICAL FREQUENCY F_{ac} TO MAXIMIZE SECURITY

Two different noise mechanisms may impact the MTD enhancement ratio of a cryptographic circuit that employs a CoRe voltage converter: 1) measurement power noise from devices that are used to perform the measurement and 2) reshuffling power noise from the CoRe voltage converter.

When a cryptographic circuit is in a normal working mode (i.e., clock frequency $f_c \approx F_1 f_s$ and F_1 is an integer), the measured input power $P_{\text{MIP},i}$ of the CoRe voltage converter induced by the ith input data is

$$P_{\text{MIP},i} = P^*_{\text{in},i}(\theta, 1/(F_1 f_s)) + P_{M,i} \tag{15}$$

where $P^*_{\text{in},i}(\theta, 1/(F_1 f_s))$ is the actual input power of the CoRe voltage converter induced by the ith input data and $P_{M,i}$ is the corresponding measurement power noise. When the variance of $P^*_{\text{in},i}(\theta, 1/(F_1 f_s))$ is $\sigma_1^2(\theta, 1/(F_1 f_s))$, the average variance $\overline{\sigma_1^2(1/(F_1 f_s))}$ of $P^*_{\text{in},i}(\theta, 1/(F_1 f_s))$ becomes

$$\overline{\sigma_1^2(1/(F_1 f_s))} = \frac{1}{2\pi}\int_0^{2\pi} \sigma_1^2(\theta, 1/(F_1 f_s))d\theta. \tag{16}$$

Accordingly, the SNR of the input power profile $\text{SNR}_M(1/(F_1 f_s))$ can be written as

$$\text{SNR}_M(1/(F_1 f_s)) = \frac{\overline{\sigma_1^2(1/(F_1 f_s))}}{\sigma_M^2} \tag{17}$$

where σ_M^2 is the variance of the measurement power noise.

However, when the attacker lowers the clock frequency from $F_1 f_s$ to f_c (i.e., $F_1 f_s / f_c$ is an integer, and the attacker can measure $F_1 f_s / f_c$ number of leakage power data), the total measured input power $P_{\text{TMIP},i}$ of the CoRe voltage converter induced by the ith input data is

$$P_{\text{TMIP},i} = P^*_{\text{in},i}(\theta, 1/f_c) + \sum_{j_1=1}^{F_1 f_s/f_c} P_{M,i,j_1} \tag{18}$$

where P_{M,i,j_1} is the corresponding measurement power noise related with the j_1th measurement under the ith input data. Therefore, the SNR of the input power profile $\text{SNR}_M(1/f_c)$ can be written as

$$\text{SNR}_M(1/f_c) = \frac{\overline{\sigma_1^2(1/f_c)}}{\frac{F_1 f_s}{f_c}\sigma_M^2}. \tag{19}$$

The correlation coefficient $\gamma_M(1/f_c)$ between the actual input power and measured input power of the CoRe voltage converter with measurement power noise when the clock frequency is f_c can be written as [9]

$$\gamma_M(1/f_c) = \frac{1}{\sqrt{1 + \frac{1}{\text{SNR}_M(1/f_c)}}}. \tag{20}$$

When the clock frequency is f_c and the average correlation coefficient between the actual input power and load power of the CoRe voltage converter is $\overline{\gamma_{Re}(1/f_c)}$,[4] the measurement power noise and reshuffling power noise from the CoRe voltage converter are independent. The correlation coefficient $\gamma_t(1/f_c)$ between the measured input power and load power of the CoRe voltage converter can therefore be written as [9]

$$\gamma_t(1/f_c) = \gamma_M(1/f_c) \times \overline{\gamma_{Re}(1/f_c)}. \tag{21}$$

The total MTD enhancement ratio $MTD_t(1/f_c)$ induced by the measurement power noise and reshuffling power noise from the CoRe voltage converter is [9]

$$\text{MTD}_t(1/f_c) \propto \frac{1}{(\gamma_t(1/f_c))^2}. \tag{22}$$

As compared with a cryptographic circuit with the clock frequency of $(1/F_0) f_s$, the MTD value of a cryptographic circuit with the clock frequency of f_c would be enhanced $f_s/(f_c F_0)$ times. $\text{MTD}_t(1/f_c)$ therefore becomes

$$\text{MTD}_t(1/f_c) \simeq \frac{\frac{1}{F_0} f_s}{f_c} \times \frac{1}{(\gamma_t(1/f_c))^2}. \tag{23}$$

As shown in Fig. 3(b), the minimum MTD enhancement ratio of a cryptographic circuit with the SA voltage converter is 6145. When the MTD enhancement ratio induced by the measurement power noise and reshuffling power noise from the CoRe voltage converter is lower than the minimum MTD enhancement ratio induced by the SA voltage converter, the discharging resistor R_c needs to be activated to trigger the SA voltage converter to enhance the security. Therefore, an approximately optimum active critical frequency F_{ac} can be determined by solving

$$MTD_t(1/F_{ac}) \simeq \frac{\frac{1}{F_0} f_s}{F_{ac}} \times \frac{1}{(\gamma_t(1/F_{ac}))^2} = 6145. \tag{24}$$

REFERENCES

[1] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks Revealing the Secrets of Smart Cards* (Advances in Information Security). Berlin, Germany: Springer-Verlag, 2007.

[2] 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, Reg. Papers*, vol. 57, no. 2, pp. 355–367, Feb. 2010.

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

[4] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti, "Effectiveness of leakage power analysis attacks on DPA-resistant logic styles under process variations," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 2, pp. 429–442, Feb. 2014.

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

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

[7] T. M. Andersen *et al.*, "A 4.6 W/mm^2 power density 86% efficiency on-chip switched capacitor DC-DC converter in 32 nm SOI CMOS," in *Proc. Appl. Power Electron. Conf. Expo. (APEC)*, Mar. 2013, pp. 692–699.

[8] 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.

[9] O.-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.

[4] Modeling of the average correlation coefficient of voltage converter with a variable clock frequency is analyzed in Section IV-A.