Charge-Withheld Converter-Reshuffling: A Countermeasure Against Power Analysis Attacks

Weize Yu and Selçuk Köse, *Member, IEEE*

***Abstract*—Converter-reshuffling (CoRe) technique has recently been proposed as a power-efficient countermeasure against differential power analysis (DPA) attacks by randomly reshuffling the individual stages within a multiphase switched-capacitor voltage converter. This randomized reshuffling of the converter stages inserts noise to the monitored power profile and prevents an attacker from extracting the correct input power data. The total number of activated phases within a switch period, however, still correlates with the dynamic power consumption of the workload. To break the one-to-one relationship between the monitored and actual power consumption, a charge-withheld CoRe technique is proposed in this brief by utilizing the flying capacitors to withhold a random amount of charge for a random time period. As compared to the conventional CoRe technique, the proposed charge-withheld CoRe technique eliminates the possibility of having a zero power trace entropy (PTE) even under machine-learning-based DPA attacks. The average PTE of the monitored power profile is increased $\sim$46.1% with a 64-phase charge-withheld CoRe technique.**

***Index Terms*—Charge-withheld, converter-reshuffling (CoRe), differential power analysis (DPA) attacks, multiphase switched capacitor (SC), side-channel attacks.**

I. Introduction

DIFFERENTIAL power analysis (DPA) attacks can obtain the secret key in a cryptographic device within feasible time and at a reasonable cost [4]. In order to protect cryptographic devices from DPA attacks, various techniques have been proposed as a countermeasure [2], [3], [5]. All existing countermeasures, however, consume a significant amount of dynamic power to hide or mask the load power information.

Converter-reshuffling (CoRe) technique [10] utilizes a multiphase switched-capacitor (SC) voltage converter and is based on converter-gating [6] as a countermeasure against DPA attacks with negligible power overhead. The number of required converter stages is determined based on the workload information, whereas the activation pattern of these stages is determined by a pseudorandom number generator (PRNG) to scramble the input power profile of the voltage converter. As a result, if an attacker is unable to synchronize the sampling frequency of the power data with the switching frequency of the on-chip voltage converter, a large amount of noise is inserted within the leakage data that are sampled by the attacker. Alternatively, if the attacker is able to synchronize the attack with the switching frequency of the on-chip voltage converter by using machine-learning (ML) attacks, the scrambled power data can be unscrambled by the attacker, and the CoRe technique may effectively be neutralized. The reason is that the total number of activated phases within a switch period has a high correlation with the load power dissipation. A charge-withheld CoRe technique is proposed in this brief to prevent the attacker from acquiring accurate load power information, even if the attacker can synchronize the data sampling.

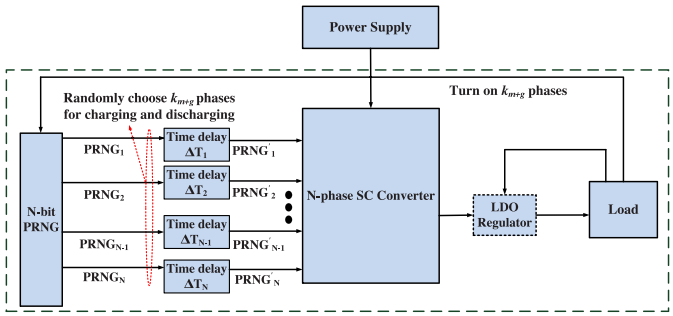

Fig. 1. Architecture of the conventional CoRe technique.

The switching frequency f_s of an SC voltage converter is proportional to the output power P_{out} [1]. The fluctuations in f_s therefore can leak critical workload information to the attacker. In the proposed charge-withheld CoRe technique, f_s is kept constant under varying workload conditions (i.e., f_s is workload-agnostic) to minimize the leakage of workload information. Instead, the number of activated phases is adaptively changed to satisfy the workload demand. As compared to the CoRe technique whereby only a single PRNG is utilized, as shown in Fig. 1, the charging and discharging states of the flying capacitors in the charge-withheld CoRe technique are controlled by two independent PRNGs (PRNG_1 and PRNG_2), as illustrated in Fig. 4. For instance, for an N-phase charge-withheld CoRe technique, if the load requires to activate k_{m+g} additional phases based on the workload, the PRNG_1 would randomly select $V_{m+g}, (k_{m+g} \leq V_{m+g} \leq N)$ phases for charging. When the charging period ends, the PRNG_2 would choose k_{m+g} phases out of the selected V_{m+g} phases for discharging. As a result, the energy stored in the corresponding $(V_{m+g} - k_{m+g})$ phases is used for power delivery in the next couple of switch cycles. With this charge-withholding technique, the total number of activated phases within a switching period is no longer highly correlated with the actual load power consumption.

This brief is organized as follows. The conventional and charge-withheld CoRe architectures are discussed in Section II.

Manuscript received April 20, 2015; revised July 22, 2015 and September 28, 2015; accepted November 21, 2015. Date of publication December 3, 2015; date of current version April 28, 2016. This work was supported in part by the National Science Foundation CAREER award under Grant CCF-1350451 and by the University of South Florida Presidential Fellowship. This brief was recommended by Associate Editor V. Saxena.

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 brief are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSII.2015.2505261

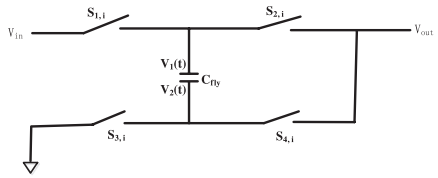

Fig. 2. One of the identical 2:1 SC voltage converter stages in CoRe.

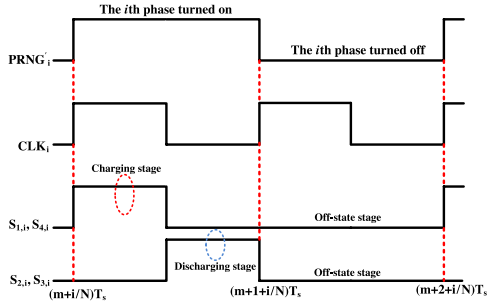

Fig. 3. Logic level of the signals that control the switches $(S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i})$ within the CoRe technique.

The security-performance models of these two techniques against DPA attacks and ML-based DPA attacks are developed in Section III. In Section IV, the power efficiency of the charge-withheld CoRe technique is investigated. The power trace entropy (PTE) levels of the conventional and charge-withheld CoRe techniques are discussed in Section V. The conclusion is offered in Section VI.

II. Architecture Design

A. Architecture of the CoRe Technique

In the conventional CoRe technique, the activation/deactivation pattern of a multiphase SC voltage converter is controlled by an N-bit PRNG, as shown in Fig. 1. The PRNG produces an N-bit random sequence $\text{PRNG}_i, (i = 1, 2, \ldots, N)$ that is delayed by ΔT_i to get synchronized with the clock signal CLK_i generated by a phase shifter. The time delay ΔT_i is

$$\Delta T_i = \frac{i}{N} T_s \tag{1}$$

where $T_s = 1/f_s$ is the switch period. An optional low-dropout regulator can be utilized at the output of the CoRe technique if the number of phases N in the SC converter is not sufficient to meet the accuracy requirement of the load.

A high-level schematic of one of the identical phases within the multiphase SC converter is shown in Fig. 2. The time-delayed signal $\text{PRNG}'_i, (i = 1, 2, \ldots, N)$, as illustrated in Fig. 1, with the clock signal CLK_i controls the states of switches $(S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i})$ in the ith converter stage as follows:

$$\{S_{1,i}, S_{4,i}\} = \text{PRNG}'_i \otimes \text{CLK}_i \tag{2}$$
$$\{S_{2,i}, S_{3,i}\} = \text{PRNG}'_i \otimes \overline{\text{CLK}_i}. \tag{3}$$

The corresponding signal waveforms controlling the switches $(S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i})$ are illustrated in Fig. 3. The signal PRNG'_i is a binary variable and utilized to determine whether the ith phase should be turned on or turned off within the next switching cycle. The circuit level implementation details of the CoRe technique can be found in [6] and [10].

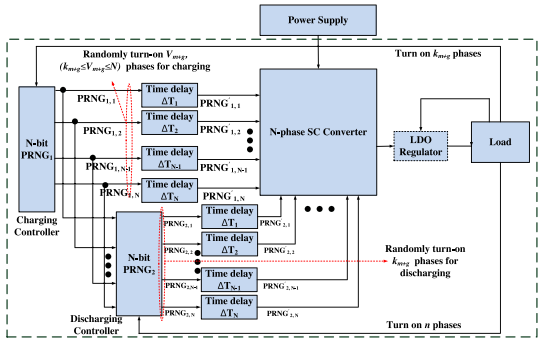

Fig. 4. Architecture of the proposed charge-withheld CoRe technique.

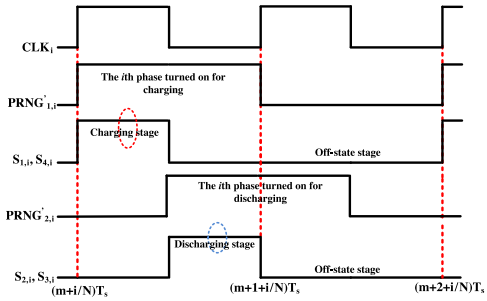

Fig. 5. Logic level of the signals that control the switches $(S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i})$ within the charge-withheld CoRe technique.

B. Architecture of the Charge-Withheld CoRe Technique

Two PRNGs (PRNG_1 and PRNG_2) are utilized in the proposed charge-withheld CoRe technique, as shown in Fig. 4. When the load demand changes, a certain number of gated stages, e.g., k_{m+g} stages, need to turn on. PRNG_1 randomly selects $V_{m+g}, (k_{m+g} \leq V_{m+g} \leq N)$ stages and concurrently transmits the logic signal $\text{PRNG}_{1,i}, (i = 1, 2, \ldots, N)$ both to the corresponding converter stages and to PRNG_2. The ith converter stage turns on if the corresponding $\text{PRNG}'_{1,i}$ value is 1. During the discharging stage, when PRNG_2 receives data generated by PRNG_1, after half a switch period, PRNG_2 sends out signal $\text{PRNG}_{2,i}, (i = 1, 2, \ldots, N)$ to discharge k_{m+g} phases out of the selected V_{m+g} phases by PRNG_1. Under this condition, the stages that charge and discharge are independent and controlled, respectively, by PRNG_1 and PRNG_2. The states of the switches $(S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i})$ in the charge-withheld CoRe technique are

$$\{S_{1,i}, S_{4,i}\} = \text{PRNG}'_{1,i} \otimes \text{CLK}_i \tag{4}$$
$$\{S_{2,i}, S_{3,i}\} = \text{PRNG}'_{2,i} \otimes \overline{\text{CLK}_i} \tag{5}$$

where $\text{PRNG}'_{1,i}$ and $\text{PRNG}'_{2,i}$ are, respectively, the delayed output signal from PRNG_1 and PRNG_2. As compared to the conventional CoRe technique, the signal waveforms of switches $(S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i})$ in the charge-withheld CoRe are controlled by two different PRNGs, as shown in Fig. 5. PRNG_1 controls the switches $(S_{1,i}, S_{4,i})$ for charging, while PRNG_2 controls the switches $(S_{2,i}, S_{3,i})$ for discharging.

III. Security Evaluation Model

A. Security Evaluation Against DPA Attacks

In information theory, entropy is widely used to quantify the amount of leakage from critical systems [7]–[9]. To quantify

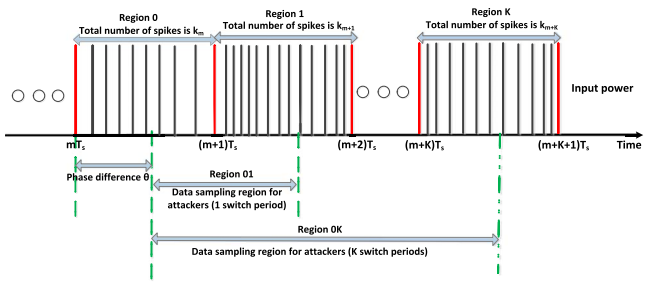

Fig. 6. Input power profile of the CoRe technique.

the amount of leakage in the power side-channels, the PTE of the power profile information that is monitored by an attacker is adopted in this brief to quantify the security levels of the conventional and charge-withheld CoRe techniques against DPA attacks. When there is a one-to-one relationship between the input power P_{in} and load power P_{out} of a voltage converter, the PTE value becomes zero. Alternatively, if the voltage converter has a many-to-one or one-to-many relationship between the P_{in} and P_{out} such that $f_1(P_{\text{out}})$, $f_2(P_{\text{out}}), \ldots, f_k(P_{\text{out}})$ lead to a series of input power $P_{\text{in}}^1, P_{\text{in}}^2, \ldots, P_{\text{in}}^k$ and the probability of each input power $P_{\text{in}}^l, (l = 1, 2, \ldots, k)$ is p_l, the PTE of the converter becomes

$$\text{PTE} = -\sum_{l=1}^{k} p_l \log_2^{p_l}. \tag{6}$$

For a cryptographic device with an embedded CoRe technique, an attacker can sample the average input power within a switch period $\overline{P_{\text{in},1}}$, $\overline{P_{\text{in},2}}, \ldots$, and exploit these input data to predict the average dynamic power within a switch period $\overline{P_{pr,1}}$, $\overline{P_{pr,2}}, \ldots$. The attacker can then perform a correlation analysis between the monitored input power and the predicted power to estimate the correct key. Alternatively, the attacker can sample the average input power for a couple of switch cycles to strengthen the attack. For example, the attacker may sample K switch cycles to obtain the average input power where the average input power and predicted power are, respectively, $\sum_{j=1}^{K}(\overline{P_{\text{in},j}}/K)$ and $\sum_{j=1}^{K}(\overline{P_{pr,j}}/K)$. The attacker can utilize these data to perform a correlation analysis.

Let us assume that the total number of SC converter phases in the CoRe technique is N and the attacker intends to sample the average input power within K switch cycles. Since there is a phase difference between the switching frequency and data sampling rate, we record the input power information in $(K + 1)$ switch cycles to obtain all the possible power information of K switch cycles which may be sampled by the attacker. The input power distribution between mT_s and $(m + K + 1)T_s$, as shown in Fig. 6, can be denoted by an array A_m as follows:

$$A_m = [a_{m,1}, a_{m,2}, \ldots, a_{m,N}, a_{m+1,1}, a_{m+1,2}, \ldots, a_{m+1,N}, \ldots, a_{m+K,1}, a_{m+K,2}, \ldots, a_{m+K,N}]P_0 \tag{7}$$

where $a_{m+g,i} \in \{0, 1\}, (g = 0, 1, \ldots, K$ and $i = 1, 2, \ldots, N)$ and $\sum_{i=1}^{N} a_{m+g,i} = k_{m+g}$. P_0 is the power consumed by each converter stage within the CoRe technique, and $k_{m+g}, (g = 0, 1, \ldots, K)$ is the total number of active phases[1] within a switch period, as shown in Fig. 6. Another array $W_m = [w_1, w_2, \ldots, w_{(K+1)N}]$ is used to represent the position of the spikes that would be recorded by the attacker within K switch periods, and the value of the elements $w_q, (q = 1, 2, \ldots, (K + 1)N)$ in W_m becomes

$$w_q = \begin{cases} 0, & q \le [\theta/360 * N] \\ 1, & [\theta/360 * N] < q \le [\theta/360 * N] + K * N \\ 0, & q > [\theta/360 * N] + K * N \end{cases} \tag{8}$$

where θ is the phase difference, as illustrated in Fig. 6. The average input power within K switch periods $\overline{P_{m,K}}$ sampled by the attacker therefore becomes

$$\overline{P_{m,K}} = \frac{A_m W_m^T}{KN}. \tag{9}$$

When all of the possible A_m and W_m arrays are analyzed, the probability $\alpha_l(\theta, k_m, \ldots, k_{m+K})$ of the average input power $\overline{P_{m,K}}$ can be written as

$$\alpha_l(\theta, k_m, \ldots, k_{m+K}) = \frac{x_l(\theta, k_m, \ldots, k_{m+K})}{\sum_{l=1}^{G} x_l(\theta, k_m, \ldots, k_{m+K})} \tag{10}$$

where $x_l(\theta, k_m, \ldots, k_{m+K}), (l = 1, 2, \ldots, G)$ is the number of all possible values of $\overline{P_{m,K}}$ induced by different A_m and W_m arrays, and G represents the total number of possible values of $\overline{P_{m,K}}$. The PTE of the CoRe technique $\text{PTE}_{\text{CR}}(\theta)$ then becomes

$$\text{PTE}_{\text{CR}}(\theta) = -\sum_{l=1}^{G} H_l \log_2^{H_l} \tag{11}$$

$$H_l = \alpha_l(\theta, k_m, \ldots, k_{m+K}) \tag{12}$$

and the average PTE value of the CoRe technique $\overline{\text{PTE}_{\text{CR}}}$ is

$$\overline{\text{PTE}_{\text{CR}}} = \frac{\int_0^{360} \text{PTE}_{\text{CR}}(\theta) d\theta}{360}. \tag{13}$$

For the charge-withheld CoRe technique, we define a matrix $B_m(K + 1, N)$ to denote the phase sequences that are selected for charging within $(K + 1)$ consecutive switch cycles by PRNG_1. $B_m(K + 1, N)$ can be written as

$$B_m(K+1, N) = \begin{pmatrix} b_{m,1} & \cdot & \cdot & \cdot & b_{m,N} \\ b_{m+1,1} & \cdot & \cdot & \cdot & b_{m+1,N} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{m+K,1} & \cdot & \cdot & \cdot & b_{m+K,N} \end{pmatrix} \tag{14}$$

where $b_{m+g,i} \in \{0, 1\}, (g = 0, 1, \ldots, K$ and $i = 1, 2, \ldots, N)$ and $k_{m+g} \le V_{m+g} = \sum_{i=1}^{N} b_{m+g,i} \le N$. Another matrix $C_m(K + 1, N)$ is defined to record whether the flying capacitor in the corresponding converter stage has already withheld charge before being selected by PRNG_1 for charging. Note that the elements $c_{m+g,i}$ in matrix $C_m(K + 1, N)$ are also binary. Accordingly, only the ith converter stage which is selected for charging and does not have withheld charge from the previous cycles can exhibit the related power spike in the input power profile. Additionally, we define a matrix $D_m(K + 1, N)$ to reflect the input power information within

[1]Note that the number of active phases is equal to the number of spikes in a switch period.

the $(K+1)$ consecutive switch periods. Note that the elements $d_{m+g,i}$ in $D_m(K+1,N)$ satisfy the following expression:

$$d_{m+g,i} = (b_{m+g,i} \otimes 1) \otimes (\overline{c_{m+g,i}} \otimes 1). \tag{15}$$

Another binary $(K+1) \times N$ matrix $E_m(K+1,N)$ is used to record the phases that are chosen by PRNG_2 for discharging. The relationship between the elements $e_{m+g,i}$ in $E_m(K+1,N)$ and $b_{m+g,i}$ is

$$b_{m+g,i} - e_{m+g,i} \geq 0 \tag{16}$$

$$\sum_{i=1}^{N} (b_{m+g,i} \otimes e_{m+g,i}) = k_{m+g}. \tag{17}$$

Finally, in the voltage conversion system, the number of charged phases needs to be equal to the number of discharged phases plus the number of charge-withheld phases all the time. This constraint is satisfied as

$$c_{m+g+1,i} = c_{m+g,i} + d_{m+g,i} - e_{m+g,i}. \tag{18}$$

After all the elements $d_{m+g,i}$ in $D_m(K+1,N)$ have been obtained, the matrix $D_m(K+1,N)$ can be converted into a $1 \times (K+1)N$ array A'_m, which is similar to the array A_m as

$$A'_m = [d_{m,1}, d_{m,2}, \ldots, d_{m,N}, d_{m+1,1}, d_{m+1,2}, \ldots, d_{m+1,N}, \ldots, d_{m+K,1}, d_{m+K,2}, \ldots, d_{m+K,N}]P_0. \tag{19}$$

After satisfying all the above constraints, the PTE value of the proposed charge-withheld CoRe technique can be determined with (11).

B. Security Evaluation Against ML-Based DPA Attacks

To perform a successful ML-based DPA attack, two steps are required. The first step is to determine the switch period and phase difference (T_s, θ) with ML attacks. The second step is to synchronize the data sampling rate with the switching frequency. To estimate the switch period T_s, the attacker can apply a number of random input data to determine the minimum time gap ΔT_s between the two adjacent spikes in the input power profile. For an N-phase SC converter, the switch period T_s is equal to $N\Delta T_s$; therefore, the attacker only needs to determine the number of phases N to acquire the correct T_s.

Assume that the attacker estimates the switch period as $T_s = F\Delta T_s$, $(F = 1, 2, \ldots)$ and sequentially applies two different input data (data_1 and data_2) with the frequency $f_0 = 1/(F\Delta T_s)$. The attacker then estimates $\theta = [0 : 360/F : 360]$ as all of the possible phase difference scenarios between the attack and switching frequency to synchronize the attack. If the estimation of (F, θ) is correct, the total number of spikes k_{m+g}, as illustrated in Fig. 6, can be written as

$$k_{m+g} = k', (g = 0, 2, 4, \ldots) \tag{20}$$

$$k_{m+g} = k'', (g = 1, 3, 5, \ldots) \tag{21}$$

where k' and k'' are, respectively, the total number of input power spikes due to inputs data_1 and data_2. In this case, the total number of input power spikes within two consecutive switch periods is $(k' + k'')$, which is a constant value. If the attacker can synchronize the attack such that a constant average power profile in any two consecutive switch periods is obtained, the correct switch period and phase difference (T_s, θ) are successfully determined. Once the correct (T_s, θ) are obtained, the attacker can eliminate all the noise inserted by the CoRe technique and perform a successful DPA attack.

ML-based DPA attacks are rather difficult to implement for the charge-withheld CoRe technique as the total number of spikes within a switch period is variable. Even if the attacker can obtain the information about (T_s, θ) and synchronize the attack with the switching frequency, the attacker can eliminate only the noise data induced by the CoRe technique. However, the noise data due to the charge-withholding operation cannot be eliminated with ML-based DPA attacks.

IV. Efficiency Analysis

During the charge-withholding operation, a number of flying capacitors within a multistage SC voltage converter are charged. Some of these capacitors maintain the charge for a random number of cycles, instead of discharging after each charging phase. The power dissipation in the form of leakage from the flying capacitors is investigated in this section.

For a multiphase 2:1 SC converter, as shown in Fig. 2, the top plate voltage $V_1(t)$ and the bottom plate voltage $V_2(t)$ of the flying capacitor in a charge-withheld phase can be denoted as follows:

$$V_1(t) = (V_{\text{in}} - V_{\text{out}})e^{(-t/R_{\text{off}}C_{\text{fly,top}})} + V_{\text{out}} \tag{22}$$

$$V_2(t) = V_{\text{out}}e^{(-t/R_{\text{off}}\alpha C_{\text{fly,top}})} \tag{23}$$

where V_{in} and V_{out} are, respectively, the input and output voltages. t is the discharging time, R_{off} is the OFF-state resistance of the MOSFET switch, $C_{\text{fly,top}}$ is the top plate flying capacitance, and α is the bottom plate capacitance ratio. The total dissipated energy ratio $\mu(t)$ of the flying capacitor due to the charge leakage can be written as

$$\mu(t) = 1 - \frac{\frac{1}{2}C_{\text{fly,top}}V_1^2(t) + \frac{1}{2}\alpha C_{\text{fly,top}}V_2^2(t)}{\frac{1}{2}C_{\text{fly,top}}V_{\text{in}}^2 + \frac{1}{2}\alpha C_{\text{fly,top}}V_{\text{out}}^2}. \tag{24}$$

By substituting (22) and (23) into (24), the number of switch cycles M $(M = t/T_s)$ required to deplete the corresponding energy in a flying capacitor can be obtained.

The number of switch cycles M required to dissipate 1% of the total stored energy in the flying capacitor through leakage is about 101 cycles, assuming a flying capacitor $C_{\text{fly,top}} = 1$ pF, the bottom plate capacitance ratio $\alpha = 6.5\%$ [11], input voltage $V_{\text{in}} = 1.2$ V [12], switching frequency $f_s = 60$ MHz [12], and OFF-state resistance of a MOSFET in 90 nm [12] $R_{\text{off}} = 240$ MΩ. The proposed charge-withholding technique therefore practically does not cause any efficiency degradation due to the charge leakage from the flying capacitors during the withholding operation.

V. Results and Discussions

The input PTE versus the phase difference θ for the 64-phase CoRe and the 64-phase charge-withheld CoRe techniques are shown in Fig. 7, when the load power varies from $(1/4)\eta NP_0$ to $(1/2)\eta NP_0$. Here, η is the power efficiency, and the number of switch cycles K sampled by the attackers is 1. As compared to the conventional CoRe technique, the charge-withheld CoRe has two advantages. The proposed technique eliminates the possibility of having zero PTE even when the phase difference θ is 0° or 360°. Additionally, the average PTE value of the proposed

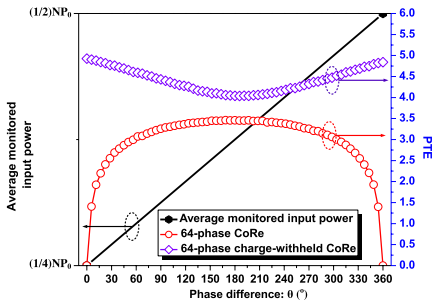

Fig. 7. PTE value versus the phase difference θ between the switching frequency and data sampling frequency for the CoRe and charge-withheld CoRe techniques.

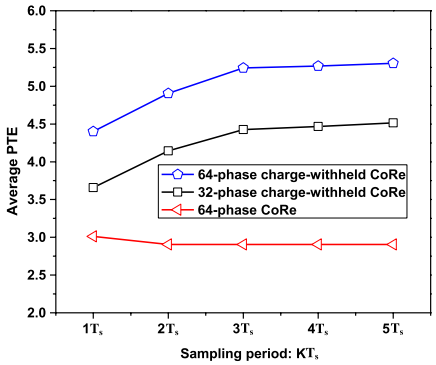

Fig. 8. Average PTE value versus the number of switch cycles sampled by the attacker for the CoRe and charge-withheld CoRe techniques.

charge-withheld CoRe technique is enhanced by about 46.1% as compared to the conventional CoRe technique.

The effect of the sampling period KT_s on the average PTE value is also investigated. The average PTE value of the conventional CoRe technique slightly decreases when KT_s increases (Fig. 8). Alternatively, the average PTE value of the proposed charge-withheld CoRe technique increases more than 20% when KT_s increases threefold. Further increasing KT_s does not result in a significant change in PTE as PTE converges to a certain value. The primary reason for the convergence of PTE is that, as the attacker increases the sampling period, the probability for the withheld charge to be delivered to the power grid within the same sampling period increases. Since the effective number of charge withholding from one sampling cycle to another sampling cycle reduces by increasing the attacker's sampling period, the PTE value converges to a constant value. Finally, the impact of the number of stages within the SC voltage converter on the average PTE value is investigated, as shown in Fig. 9. The average PTE value increases with a larger number of phases N for both conventional and charge-withheld CoRe techniques. The average PTE value of the proposed charge-withheld CoRe technique, however, has a steeper slope, indicating better security-performance against DPA attacks with a larger number of converter phases.

The flying capacitors that withhold charge in the charge-withheld CoRe technique cannot be utilized as a filter capacitor, as these capacitors are not connected to the output node during the charge-withholding operation. This would slightly increase the output voltage ripple. For example, the amplitude of the output ripple voltage increases less than 2.5 mV for a 32-phase SC voltage converter when only eight of the stages are active. Alternatively, the ripple amplitude increases less than 1 mV when more than half of the stages are active. The increase in

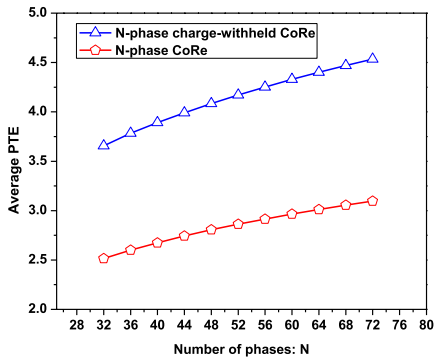

Fig. 9. Average PTE value versus the number of SC voltage converter phases N for the CoRe and charge-withheld CoRe techniques.

the ripple voltage can be mitigated by increasing the number of SC converter stages. If the number of stages is increased from 32 to 48, the ripple amplitude would be reduced by 40%.

VI. Conclusion

The proposed charge-withheld CoRe technique withholds a random portion of input charge and delivers this charge to the power network after a random time period. This proposed technique is more effective than the conventional CoRe technique against DPA attacks and ML-based DPA attacks. The possibility of having zero PTE under certain conditions is successfully eliminated, and the average PTE value is increased more than 46% with negligible power loss due to the leakage of flying capacitors. Since the charge that is withheld for a random amount of time is eventually delivered to the power grid, there is no additional power overhead.

References

[1] Y. K. Ramadass, A. A. Fayed, and A. P. Chandrakasan, "A fully-integrated switched-capacitor step-down dc–dc converter with digital capacitance modulation in 45 nm CMOS," *IEEE J. Solid-State Circuits*, vol. 45, no. 12, pp. 2557–2565, Dec. 2010.

[2] 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.

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

[4] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks Revealing the Secrets of Smart Cards (Advances in Information Security)*. New York, NY, USA: Springer, 2007.

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

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

[7] B. Kopf and D. Basin, "An information-theoretic model for adaptive side-channel attacks," in *Proc. CCS*, Oct. 2007, pp. 286–296.

[8] H. Maghrebi, S. Guilley, J. L. Danger, and F. Flament, "Entropy-based power attack," in *Proc. IEEE Int. Symp. HOST*, Jun. 2010, pp. 1–6.

[9] B. Köpf and G. Smith, "Vulnerability bounds and leakage resilience of blinded cryptography under timing attacks," in *Proc. IEEE CSF*, Jul. 2010, pp. 44–56.

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

[11] H. Jeon, "Fully integrated on-chip switched capacitor DC–DC converters for battery-powered mixed-signal SoCs," Ph.D. dissertation, Dept. Electr. Comput. Eng., Northeastern Univ., Boston, MA, USA, Oct. 2012.

[12] M. D. Seeman, "A design methodology for switched-capacitor DC–DC converters," Ph.D. dissertation, Electr. Eng. Comput. Sci., Univ. California Berkeley, Berkeley, CA, USA, May 2009.