EM Side-Channel Countermeasure for Switched-Capacitor DC–DC Converters Based on Amplitude Modulation

Ruzica Jevtic, *Senior Member, IEEE*, Marko Ylitolva, *Member, IEEE*, Clara Calonge, Martti Ojanen, Tero Santti, *Member, IEEE*, and Lauri Koskinen, *Member, IEEE*

***Abstract*— The security of IoT devices is becoming a major concern in industry. Noninvasive side-channel attacks pose a serious threat as they are capable of extracting secret information from distance while using low-cost equipment. In this article, we propose an efficient countermeasure technique against the electromagnetic (EM) side-channel attacks. The technique is applied to switched-capacitor (SC) dc–dc converters and is based on amplitude modulation of the load signal by the converter capacitance that acts as a carrier. We verify the proposed technique by using a reliable evaluation metric that predicts the correlation between the encryption secret key and the attacker's measured signal. The results show that the proposed technique can achieve cross correlation coefficients as low as 0.2, disabling the attacker from extracting the sensitive information. In addition, test vector leakage assessment (TVLA) ρ-test indicates that the number of leaky points for advanced encryption standard (AES) execution drops from 62 for unprotected circuit to zero for the circuit secured by the proposed technique. TVLA *t*-statistic is decreased by three orders of magnitude in the protected AES execution.**

***Index Terms*— Amplitude modulation (AM), security, side-channel attacks, switched-capacitor (SC) dc–dc converters.**

I. Introduction

NEW security threats are emerging as a consequence of the ever-increasing number of devices connected to the Internet. Each device acts as a network node in the Internet-of-Things (IoT) and needs to be available around the clock to provide information and control signals to the environment. While it is impossible to predict the exact consequences of the massive breakthrough of the IoT network, two key factors are evident: IoT nodes need to be energy-efficient and secure against hacking.

While there are a multitude of methods to hack devices, side-channel attacks can be the most cunning since conventional cryptographic methods, the basis of most security measures, inherently leak side-channel information. Most side-channel attacks are somewhat invasive and require access to the device. For example, power attacks usually require a small resistor to be inserted in the ground line of the device. By measuring the voltage over the resistance, the attacker can get the information on the current. The current depends on the data that are being processed and can indirectly provide the confidential information on the secret key.

Noninvasive side-channel attacks pose a serious threat to the security of cryptographic devices. The attacks cannot be detected and usually require only a simple low-cost equipment. This type of attacks relies on measuring electromagnetic (EM) radiation of the chip.

Recent studies show that the EM emanations differ from and provide more information than the leakage from other conventional side channels, such as timing and power [1]–[5]. EM attacks are based on the measurement of EM waves that are radiated from the device. Electrical and magnetic fields depend on the derivative of the voltage and current, so the leaked signal is fundamentally different from the leaked signal in power attacks. While power attacks rely on the absolute current value and the time moments that indicate when the current changes its value, the EM attacks depend on the current and voltage slope. In addition, EM attacks are completely contactless since it is not necessary to tamper with the device, and they can provide more information in spatial, temporal, and frequency domains [4], [5].

In this work, we focus on the EM leakage from the power supply signal since this is the strongest signal in the chip and thus, most easily attacked [3]. Power distribution network consists of voltage regulators that need to adapt the battery voltage to the power supply of the chip. The regulators are also used for dynamic voltage scaling to improve the energy efficiency of the IoT devices [6]–[8].

Inductive converters are efficient but have bulky inductive components off chip that increase the size of the chip and are therefore not suitable for small IoT nodes. Recent work has reported security techniques for fully integrated buck converters [9]. However, the wirebond inductances used in

Manuscript received September 3, 2020; revised November 24, 2020 and March 2, 2021; accepted March 27, 2021. Date of publication April 16, 2021; date of current version June 4, 2021. This research was funded by the Ministry of Science, Innovation and Universities of Spain, and the European Regional Development Fund of the European Commission, Grant No. RTI2018-095324-B-I00 and by the FitOptiVis Project funded by the ECSEL Joint Undertaking under Grant H2020-ECSEL-2017-2-783162. *(Corresponding author: Ruzica Jevtic.)*

Ruzica Jevtic and Clara Calonge are with Escuela Politecnica Superior, Universidad San Pablo-CEU, 28003 Madrid, Spain (e-mail: ruzica.jevtic@ceu.es; c.calonge@usp.ceu.es).

Marko Ylitolva is with the Department of Future Technologies, University of Turku, 20500 Turku, Finland, and also with CoreHW, 20100 Turku, Finland (e-mail: marko.ylitolva@corehw.com).

Martti Ojanen, Tero Santti, and Lauri Koskinen are with the Department of Future Technologies, University of Turku, 20500 Turku, Finland (e-mail: martti.ojanen@utu.fi; teansa@utu.fi; lauri.koskinen@utu.fi).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TVLSI.2021.3070687.

Digital Object Identifier 10.1109/TVLSI.2021.3070687

the converter can still leak critical information in form of EM emanations. The inductances act as a transmitting antenna due to the ac current that passes through them. They radiate EM waves that contain information on the switching frequency and duty cycle of the converter, both highly dependent on the load.

Linear regulators are implemented on-chip, but they are incapable of achieving high efficiency across a wide range of output voltages. Work in [10] reports improvement in side-channel resistance against power attacks, at the cost of deteriorating dynamic loop response, while work in [11] changes the reference voltage randomly in order to add additional noise to the leaked current signal.

In this work, we consider single-phase switched-capacitor (SC) voltage regulators, which can be fully integrated on-chip, do not have bulky inductive elements, and can be reconfigured to achieve multiple-output voltage levels without a significant loss in efficiency [6], [12]. They also have several tuning knobs to randomize the output voltage and decorrelate the chip activity from the physical leakages of the chip.

Several countermeasures against side-channel attacks applied to SC dc–dc converters have been reported in the literature [13]–[19]. However, they are either time-consuming as they optimize the design at the gate and/or layout level [17]–[19] or they are employed as protection from differential power attacks, rather than EM attacks [13]–[16]. In addition, most of the published techniques do not explore the causality of the leaked signal, as the work proposed here.

This work analyzes in detail the physical nature of the leaked EM signal. We prove that the signal obtained from capacitance values in time acts as a carrier in the amplitude modulation (AM) of the load signal. The resulting AM signal is leaked to the outside world in form of EM emanations. Based on this analysis, we propose to change the available capacitance in the converter in a deterministic manner during each conversion period. We change the capacitance value to create overlap in the load frequency spectrum, hence disabling the attacker from recovering the original load signal.

While the work in [16] is also based on the functionality of the switched-capacitor dc–dc converter, it focuses on the protection from the power attacks and masks the residual voltage on the capacitances from the power measured at the input. However, it is still likely that EM probe is able to detect the activity of the capacitances that are not connected to the input and reveal information on the load. In this work, we assume that the attacker has a complete information on the voltage over the flying capacitor via EM probe and propose a methodology that offers protection from EM side-channel attacks.

This article is organized as follows. Section II gives an overview on the implementation and functionality of the SC dc–dc converter. Section III describes the analysis of the leaked EM signal. In Section IV, the proposed security technique is described in detail. In Section V, we present the experimental results. Section VI studies the impact of the proposed technique on the power and area. Section VII concludes this article.

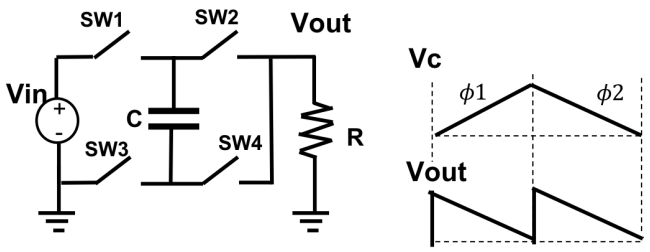

Fig. 1. Single-phase SC dc–dc converter operation: schematic with equivalent waveforms.

II. SC DC–DC Converter Specifications

Dynamic voltage scrambling is one of the side-channel countermeasures that randomly changes power supply voltage level in order to decorrelate the leaked signal from the processed data [13]–[16], [22]–[24]. This technique has low area and power overhead and has proved to be very effective against power attacks when applied to multiphase switched-capacitor dc–dc converters.

Since we consider single-phase switched-capacitor dc–dc converters, we adapt dynamic voltage scrambling to this type of converters by changing the value of the flying capacitor randomly. From here on, we call this technique random power scramble (RPS) technique.

In order to study the exact effects of this technique against EM attacks when applied to single-phase SC dc–dc converters, we start by examining the operation of the 2:1 step down converter shown in Fig. 1 [12]. The converter operates in two nonoverlapping phases $\phi 1$ and $\phi 2$. In phase $\phi 1$, SW1 and SW4 are turned on, and SW2 and SW3 are turned off, so the flying capacitor is connected between the input voltage and the output, and the capacitor is charging. In the second phase, $\phi 2$, SW2, and SW3 are turned on, and SW1 and SW4 are turned off, so the flying capacitor is connected between the output and the ground and is discharging. The equivalent waveforms on the capacitor and at the output are given in the same figure.

The ripple that appears at the output is usually suppressed by using a very large decoupling capacitance or interleaving the phases of the converter. In this work, we consider that the output voltage ripple specifications of the dc–dc converter are not so strict, as this have proved to increase the energy savings of the systems considerably [6], [8], [21]. Large voltage ripple would normally cause functional errors, but the adaptive error-protection technology presented in [8] can withstand this ripple. Also, the voltage ripple adds an element of entropy to the system both in the time and voltage domains. Two executions of the same load may differ in power and total execution time, depending on whether the supply voltage was mostly at the high or low end of the ripple during the execution. This entropy serves as additional security against side-channel attacks.

Switching from one switching phase to another ($\phi 1$ to $\phi 2$ or vice versa) in an SC dc–dc converter is controlled by the dc–dc switching clock [7]. This clock is the pulse frequency-modulated (PFM) signal and is generated by the controller shown in Fig. 2. The controller is event-driven and is composed of a comparator, flip-flop, and nonoverlapping circuit. The inputs to the comparator are the voltage generated

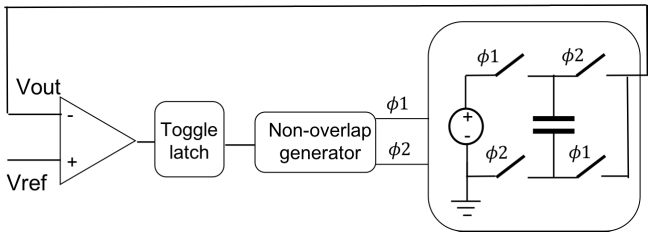

Fig. 2. Single-phase SC dc–dc converter control logic.

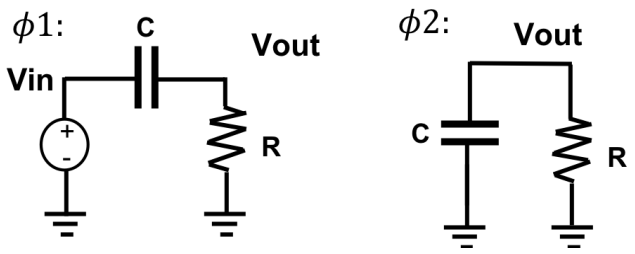

Fig. 3. SC dc–dc equivalent RC circuits.

by the SC converter and the reference voltage. Whenever the output voltage falls below the reference voltage, the converter switches to a different phase. The exact moment of the event is completely load-dependent as the load current determines the rate of charge and discharge of the flying capacitor. For example, more computationally intensive loads will lead to steeper slope of the output voltage and faster switching between the phases.

Consequently, changing the flying capacitor size will also affect both the voltage slope and the timing of the switching phases. Smaller flying capacitors discharge faster, resulting in shorter duration of the switching phase and steeper slope. In order to change the flying capacitor size, the SC dc–dc converter is partitioned into small unit cells. Each unit cell can be turned on or off independently of the rest. It is important to note that although intuitively, it seems that different voltage slope and change in the timing of the switching phases introduce entropy to the output voltage signal, it is not so clear how much impact these techniques will have on security.

In Section III, we analyze the RPS technique in detail and find that its effectiveness against EM side-channel attacks is limited for single-phase SC dc–dc converters. Then, we propose a new methodology to alternate the capacitance in order to achieve better circuit protection.

III. AM of the Load Signal

AM is based on the multiplication of the two signals in the time domain. When the modulated signal is analyzed in the frequency domain, its spectrum is obtained as a convolution of the frequency spectra of the two signals. AM signals are easier to analyze in the frequency domain, as they create specific spectral patterns.

In order to see how the change in flying capacitance affects the spectrum of the leaked signal, we first analyze the underlying physical mechanism of the circuit functionality.

In each switching phase, the circuit supplied by the SC dc–dc converter can be approximated by simple RC circuits shown in Fig. 3. The activity of the circuit is modeled as a time-variable resistance load, $R(t)$, and the flying capacitance is also modeled as time-variable capacitance value $C(t)$. By applying Kirchoff's law to the circuit in phase $\phi2$ for example, we obtain

$$-v_c = R(t)C(t)\frac{dv_c}{dt} \tag{1}$$

where v_c is the voltage over the flying capacitor. By rearranging the terms, the following equation is obtained:

$$R(t)C(t) = -\frac{1}{\frac{d(lnv_c)}{dt}}. \tag{2}$$

Similar equations are obtained for the circuit in phase $\phi1$.

It can be seen that the output voltage signal indirectly carries the information on the product of the load and the capacitance value. In other words, if the output voltage signal is postprocessed, first by applying natural logarithm to it, then taking the derivative of the result, and finally taking the reciprocal of the obtained derivative, we are able to obtain the product of the load and the capacitance value. Consequently, the output voltage, i.e., the leaked signal, contains full information on the load signal that is amplitude modulated by the changing capacitance acting as a carrier.

The load spectrum corresponds to the spectrum obtained when the cryptographic algorithm is executed. In this work, we consider the algorithms that are similar to advanced encryption standard (AES) algorithm as it is the most commonly used in the IoT devices.

AES algorithm is an iterative process, and in each iteration, a block of 128 bits is being processed [27]. The number and the type of operations that are executed in each iteration are always the same, but they are executed with different data. As an iterative, periodic process, we can assume that the AES spectrum is a baseband signal, having frequency components up to some maximum frequency fmax.

For the sake of clarity, we represent the spectrum of the load signal as in Fig. 4(a). As seen before, the resulting spectrum of the leaked signal corresponds to convolution of the load signal spectrum and the flying capacitance spectrum. If the flying capacitance spectrum were an ideal sinusoidal signal at frequency fs, the spectrum of the leaked signal would be represented as in Fig. 4(b).

In order to prevent the attacker from retrieving the load spectrum, we need to create overlap of the load spectrum in the leaked signal. If the flying capacitance spectrum were a sum of sinusoidal signals, separated by each other by less than fmax, it would result in the spectrum shown in Fig. 4(c). This would be effective since the information on the load signal would be lost.

If the RPS technique is applied and the capacitance is changed randomly, the capacitance spectrum corresponds to the broadband noise spectrum. Ideally, this would perfectly mask the load signal as this signal would be modulated by the infinite sum of sinusoidal signals.

However, the capacitance value needs to be a positive number at all times, resulting in a very large zero-frequency component in its spectrum. After the convolution, the spectrum of the AM load has the original load spectrum in its initial

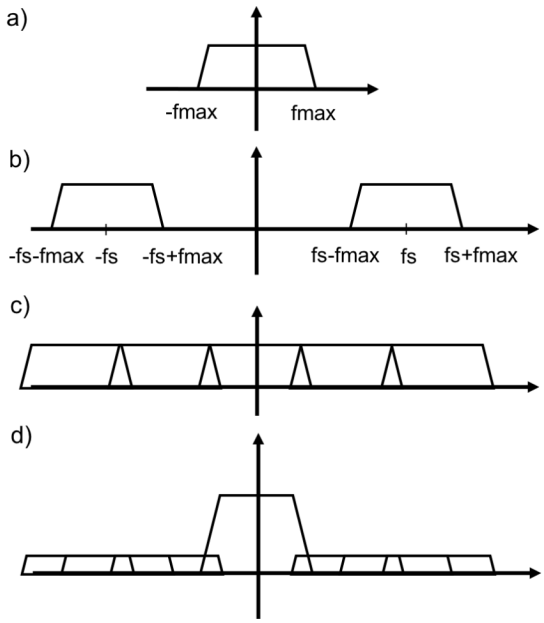

Fig. 4. (a) Load signal spectrum. (b) Load signal modulated by an ideal sinusoidal signal. (c) Load signal modulated by the sum of sinusoidal signals resulting in spectra overlapping. (d) Load signal modulated by the broadband noise with large zero-frequency component.

position due to the zero-frequency component [see Fig. 4(d)] and can be retrieved simply by applying a low-pass filter. This spectrum located in the initial position would be hardly affected by the other spectrum replicas since the value of the zero-frequency component is much bigger than the amplitudes of the rest of the sine components.

The effect explained here is more obvious for load spectra with dominant low frequencies. Load spectra that have dominant high frequencies are more affected by the replicas around the rest of the sine components, resulting in larger load signal distortion. However, we expect that the large zero-frequency component of the carrier signal will limit the circuit protection that can be achieved by applying random power scrambling regardless of the load spectrum features.

Based on this analysis and considering realistic conditions for the flying capacitance values, we propose to change the capacitance value in a deterministic fashion, as explained in Section IV. We call the proposed technique: AM technique.

It is important to note that we analyze the output voltage even though the leaked signal is an electromagnetic wave that has electrical and magnetic field components. However, it is a well-known fact that there is one-on-one relationship between the electromagnetic wave and the voltage and current that are generating it [28]. This allows us to study the output voltage waveform as an equivalent form of EM emanations.

IV. AM Technique

To prevent the attacker from separating the load signal spectrum from the spectrum of the leaked signal, we modify the capacitance value with what essentially amounts to AM modulation (see Fig. 5).

The capacitance signal needs to fulfill the following conditions.

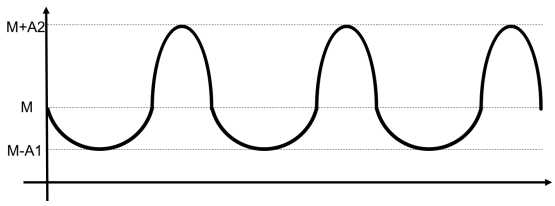

Fig. 5. Proposed flying capacitance signal.

1) At any point in time, capacitance value has to be a positive number.
2) The value that is assigned to the capacitance needs to be between the minimum capacitance value Capmin and the maximum capacitance value Capmax, both specified by the converter design.
3) The number of different capacitance values corresponds to the number of SC dc–dc unit cells.

Due to the AM modulation, the frequency spectrum of the load signal gets repeated around all carrier frequencies and is scaled according to the carrier amplitudes corresponding to these frequencies. Since the capacitance is acting as a carrier and the average value of the capacitance needs to be a positive number due to the first condition, the flying capacitance spectrum contains a zero-frequency component. As seen before, this component is dominant and responsible for the unchanged load spectrum located in its original position. In order to avoid this, we propose to generate the capacitance signal so that both the zero frequency and the next frequency value have similar values. When the load spectrum is repeated around the zero frequency and the next frequency, these two load spectra overlap and are summed together. The resulting overlap might be able to mask the load signal so that it cannot be retrieved through low-pass filtering. Unlike the spectrum generated by the RPS technique, the frequency component closest to the zero-frequency component needs to have an amplitude that is big enough to cause a significant impact when summed with the original spectrum.

With this in mind, we generate the capacitance signal in the following way. We generate a periodic signal where each period is obtained by concatenating half-periods of two sine functions. The sine functions are chosen since their Fourier transform is straightforward and enables us to see where the first nonzero-frequency component is situated in the signal spectrum. The first sine function, $s1$, has an amplitude $A1$ and frequency $f1$, and the second sine function, $s2$, has an amplitude $A2$ and frequency $f2$. We concatenate the half-periods of the two sine functions, as shown in Fig. 5. As can be seen, the negative half-period of $s1$ is concatenated to the positive half-period of $s2$. Since our goal is to have a signal with the lowest mean possible, the duration of the negative half-period of $s1$ needs to be larger than that of the positive half-period of $s2$. For the sake of simplicity, we choose the following relationship between the frequencies: $f2 = 2 * f1$.

In order to have better control of the signal parameters, we calculate the relationship of the two amplitudes so that the resulting signal has zero mean and obtain $A2 = 2 * A1$. Then, we add a constant M to the obtained signal so that the resulting signal lies in the range [Capmin Capmax] as specified

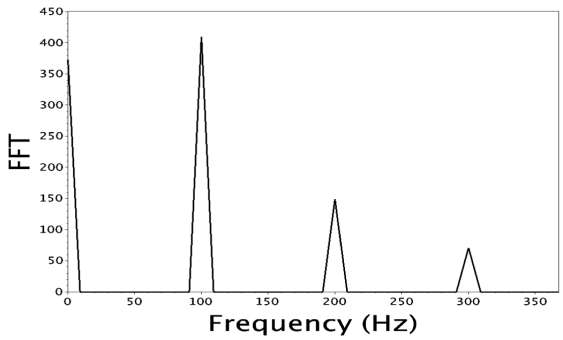

Fig. 6. Spectrum of the proposed flying capacitance signal.

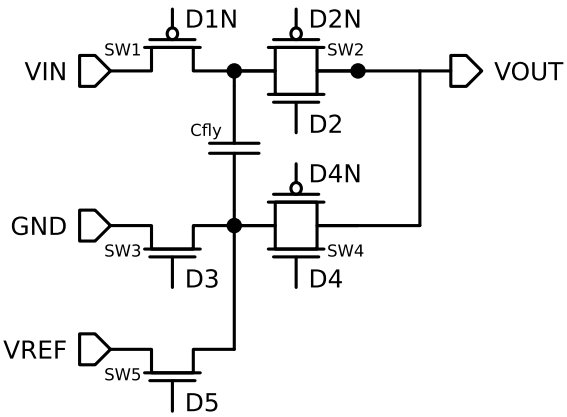

Fig. 7. SC dc–dc unit cell implementation.

by the second condition. The following equations need to be fulfilled:

$$\begin{aligned} M - A1 &= \text{Capmin} \\ M + A2 &= \text{Capmax} \\ A2 &= 2 * A1. \end{aligned} \tag{3}$$

Amplitudes of the two sine functions as well as the mean of the generated signal are then calculated as

$$\begin{aligned} M &= \frac{\text{Capmax} + 2 * \text{Capmin}}{3} \\ A1 &= \frac{\text{Capmax} - \text{Capmin}}{3} \\ A2 &= 2 * \frac{\text{Capmax} - \text{Capmin}}{3}. \end{aligned} \tag{4}$$

Fig. 6 shows an example of the generated signal spectrum for the following settings: $f1 = 75$ Hz, $f2 = 150$ Hz, $A1 = 313$ fF, $A2 = 626$ fF, and $M = 373$ fF. It can be seen that the first nonzero-frequency component has an amplitude that is comparable to the zero-frequency component, so the overlapping of the original spectrum with the shifted one is more effective. In addition, the position of the first nonzero-frequency component depends on the frequencies of the two sine signals and can be changed easily as to produce more effective overlapping in the resulting spectrum.

Since the generated flying capacitance signal is periodic and the number of unit cells fixed, there are a limited number of possible flying capacitance values. We choose the first flying capacitance value randomly out of possible values within one period of the generated signal. Instead of assigning always a value M as the first capacitance value (see Fig. 5), we might assign it any other value of the generated signal and start the signal generation from there. For example, if the first value is equal to $M - A1$ or $M + A2$, the flying capacitance signal is phase shifted by $\pi/3$ or $5\pi/6$, respectively. The analysis on the aliasing in the frequency domain is not affected by the signal phase shift, while it is ensured that two executions for the same load and the same moment in time have different flying capacitance values.

V. Security Evaluation

We design two sets of experiments. In the first set, we test the proposed technique for many different loads by calculating the correlation coefficient between the load signal and the leaked signal. The goal is to see whether critical information can be obtained by postprocessing the leaked signal. In the second set, we apply the test vector leakage assessment (TVLA) [25] to calculate the number of leaky points when the proposed technique is applied to the circuit. The goal is to see whether differential and correlation attacks would yield any significant information from the circuit. These attacks are the most common side-channel attacks and are based on measuring many side-channel traces for different input data for targeted algorithm. Afterward, a statistical test is employed to determine which secret key most probably caused the leakage.

A. Correlation Coefficient Comparison

In order to test the AM technique for many different loads and flying capacitance signals, we built our evaluation flow in Scilab in the following way.

First, we use Cadence to implement an SC dc–dc converter in 28-nm fully depleted silicon-on-insulator (FDSOI) CMOS. The converter consists of variable number of unit cells and the control circuitry that was described in Section II. We use the series–parallel topology for the SC dc–dc implementation. Each unit cell consists of five switches and a flying capacitor to achieve 1/2 ratio between the output and the input voltage, as shown in Fig. 7. Four switches S1–S4 are used for the normal operation mode of the converter when the converter is switching between phases $\phi1$ and $\phi2$. Switches S1 and S5 are used to connect the flying capacitor between 1 V and Vref when the unit cell is not used, ensuring that there is no additional strain over the switches when the cell is turned on.

We use a decoupling capacitance equal to 80 pF that is estimated to be the capacitance of the microprocessor supplied by the converter.

Then, we build a simulation flow in Scilab in order to accelerate the simulations for many different settings for the load and the flying capacitor. We describe the functionality of the dc–dc converter by using the following differential equations for the phase $\phi1$ (see Fig. 7):

$$\begin{aligned} V_{\text{in}} - R_{\text{sw1}} C_{\text{fly}} \frac{dV_c}{dt} - V_c - R_{\text{sw4}} C_{\text{fly}} \frac{dV_c}{dt} &= V_{\text{out}} \\ C_{\text{dec}} \frac{dV_{\text{out}}}{dt} &= C_{\text{fly}} \frac{dV_c}{dt} - \frac{V_{\text{out}}}{R_{\text{load}}} \end{aligned} \tag{5}$$

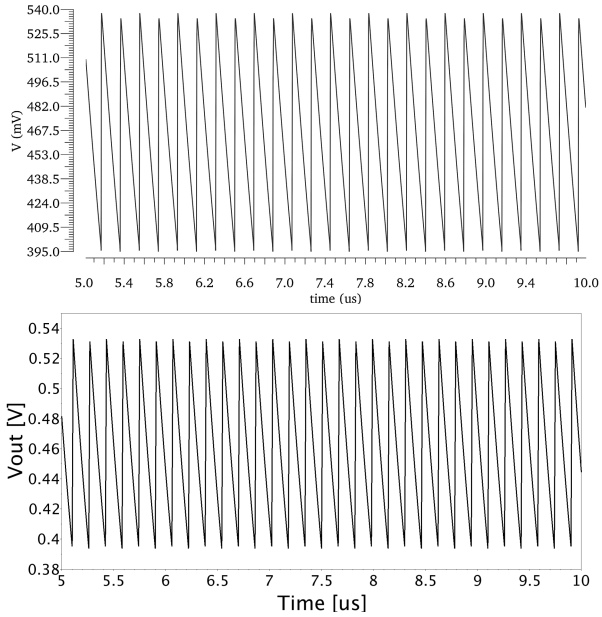

Fig. 8. Output voltage waveform from (a) Cadence simulation (top) and (b) Scilab simulation (bottom) for 300-Ω load.

and the following equations for the phase $\phi 2$:

$$R_{\text{sw2}}C_{\text{fly}}\frac{dV_c}{dt} + V_c + R_{sw3}C_{\text{fly}}\frac{dV_c}{dt} = V\text{out}$$
$$C_{\text{dec}}\frac{dV\text{out}}{dt} = -C_{\text{fly}}\frac{dV_c}{dt} - \frac{V\text{out}}{R_{\text{load}}} \quad (6)$$

where $R_{\text{sw}N}$ are the resistances of the switches ($N = 1, 2, 3, 4$), C_{fly} and C_{dec} are the values of the flying and decoupling capacitor, respectively, V_c is the voltage over the flying capacitor, and V_{in} and V_{out} are the input and output voltages, respectively. We confirm the veracity of the flow by comparing the Scilab simulation results to the results simulated in Cadence. Since the comparison is satisfactory (see Fig. 8), from here on, we use the flow built in Scilab to test the effectiveness of the proposed AM technique.

We start by verifying that (2) can be used to faithfully represent the functionality of the implemented SC dc–dc converter.

We use AES measured power traces available at [26] to generate the load that corresponds to the AES execution, and in addition, we design other types of loads to further explore the effectiveness of the proposed technique. The goal is to find out whether the proposed technique can offer better protection for different cryptographic algorithms. In order to simulate the load that corresponds to the execution of any cryptographic algorithm, we generate the load that fulfills the following conditions.

1) The load is generated as a periodic signal since most of cryptographic algorithms are iterative processes with the same number and type of operations that are executed in each iteration.
2) We generate different load patterns by changing the number of different load values in each iteration between four and 100 000.
3) The load current is changing between 50 and 500 μA, values that correspond to the minimum and maximum power consumption of the microprocessor presented in [20].

For each load, one load pattern is repeated over time in order to mimic the iterations in the cryptographic algorithms. The number of the different load values corresponds to the number of different operations that are executed and consume different powers. For example, AES algorithm has at least ten rounds. The number of rounds depends on the length of the secret key. In each round, there are four different actions that are carried out: Byte Substitution, Shift Rows, Mix Columns, and Key Addition [27]. Each of these actions consists of various different operations that are used to alter the data. For this reason, we choose to have at least four different load values that correspond to four different actions. Increasing the number of different load values corresponds to refining the number of different current values needed for each operation.

For each load pattern, we simulate the SC dc–dc converter with the corresponding load attached to its output voltage. We postprocess the output voltage signal by applying natural logarithm and applying derivative, as explained in Section III. We then take the reciprocal of the obtained derivative and multiply it with -1 in order to obtain the exact expression on the right-hand side of (2). In addition, we filter the resulting signal since the output voltage has discontinuity whenever there is a switch between the phases of the converter. When derivative is applied to the switch between the phases, it results in large peaks. These peaks can affect the cross correlation coefficient significantly, so we use a median filter to smooth out the postprocessed output voltage.

Finally, we compare the signals $R(t) * C(t)$ and the postprocessed output voltage, by calculating the cross correlation coeffient between them. We repeat the simulations for many different load patterns and different settings for the flying capacitor values. In all cases, the coefficient is very close to one, thus validating (2).

Fig. 9 shows an example for the waveforms of the output voltage, the postprocessed output voltage (i.e., the voltage after applying natural logarithm, derivative, and the negative reciprocal), filtered postprocessed output voltage, and the product of the load and the capacitance values. It can be seen that the filtered postprocessed output voltage is perfectly correlated with $R(t) * C(t)$ as expected from their correlation coefficient. Therefore, from here on, we calculate the cross correlation coefficient directly between the load $R(t)$ and $R(t) * C(t)$ for all the experiments designed to validate the effectiveness of the proposed side-channel countermeasures. The measured AES load has 16 000 traces [26]. For the rest of the loads, we generate 36 000 samples for the load signal, in order to make sure that the resulting coefficients are statistically correct.

We start by evaluating the RPS technique. We set the reference voltage to 0.4 V and randomly change the value of the flying capacitor between 60 pF and 1 nF. Scilab funtion grand(), used for pseudorandom number generation, assigns random values to the flying capacitor. To give an example of

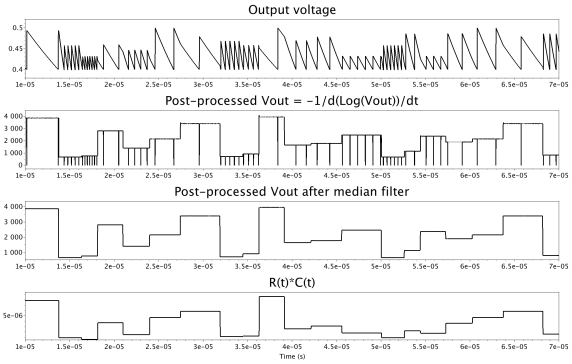

Fig. 9. Waveforms for output voltage, postprocessed output voltage, filtered postprocessed output voltage, and $R(t) * C(t)$.

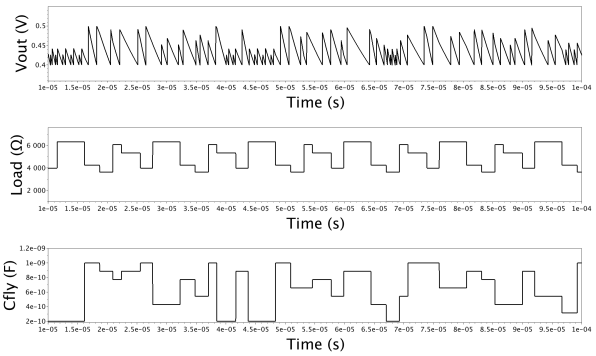

Fig. 10. Output voltage signal (top), load (middle), and flying capacitance (bottom).

the RPS waveforms, Fig. 10 shows the output voltage, the load that corresponds to the pattern six and the flying capacitor value. The pattern six refers to six different load values in each iteration. For each load pattern, we generate five different loads.

The cross correlation coefficients are calculated between the load signal $R(t)$ and the signal $R(t) * C(t)$ after it has been passed through a low-pass filter. The cross correlation coefficients for all load patterns are presented in Fig. 11. It can be seen that they are close to one for all generated loads. As mentioned before, this is due to the zero-frequency component of the flying capacitance. The spectra of the load, flying capacitor, and the product of the two are presented in Fig. 12 where this effect is visually represented. Due to the dominant zero-frequency component, random power scrambling is not appreciated in this figure. For this reason, this figure has been zoomed in and represented in Fig. 13. It can be seen that the leaked signal spectrum has additional noise due to the random power scrambling. However, this additional noise is too small to mask the original load spectrum.

For AES load, the coefficients drop to 0.6 measured power traces for AES execution have dominant high-frequency component since the current peaks occur on the rising clock edge when the flip-flops change their state. Hence, the high-frequency part of the original load spectrum will be affected more by the other load replicas, resulting in a lower coefficient between the load and the leaked signal.

We then evaluate the AM technique proposed in this article. The settings for the reference value, minimum and

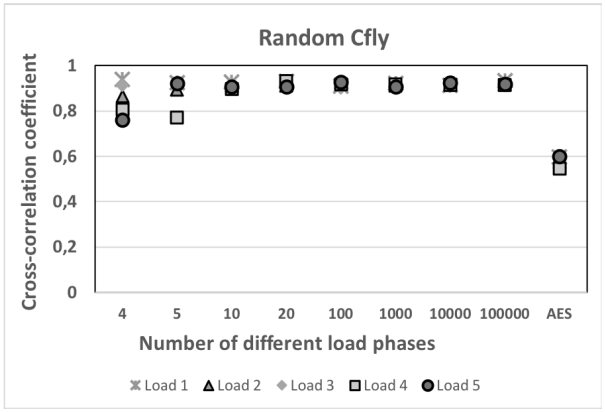

Fig. 11. Cross correlation coefficient for the RPS technique.

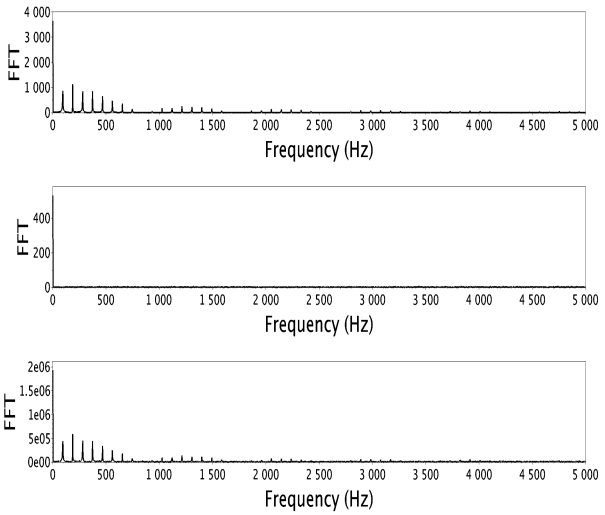

Fig. 12. Fast Fourier transformation (FFT) for load (top), flying capacitance (middle), and the convolution of the two (bottom) for the RPS technique.

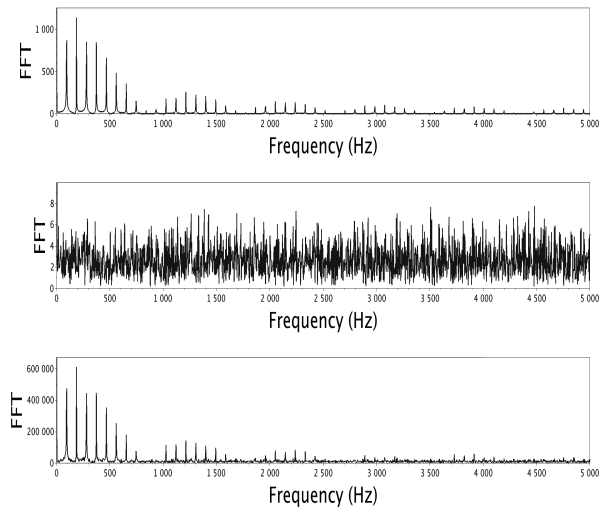

Fig. 13. Fig. 12 zoomed in.

maximum capacitance value, and the cross correlation computation method are the same as in the first case. The flying capacitance value is changed according to the signal generated, as explained in Section IV. We swipe the frequency of the generated signal (i.e., frequency $f1$ and consequently $f2$ of

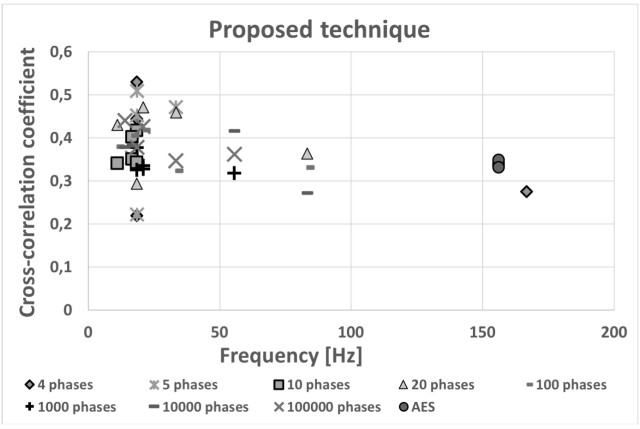

Fig. 14. Cross correlation coefficient for the AM technique.

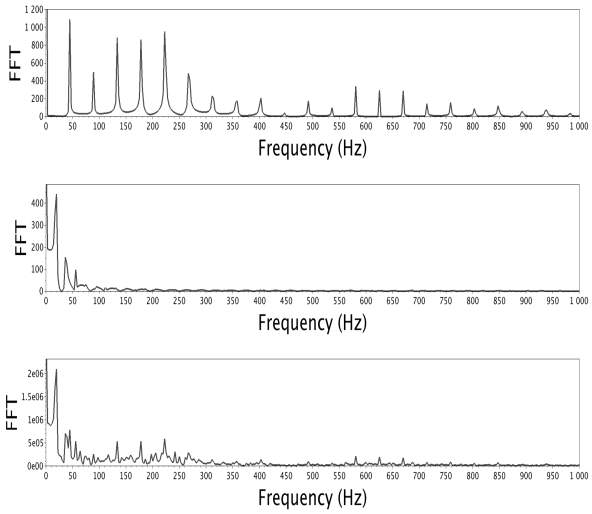

Fig. 15. FFT for load (top), flying capacitance (middle), and the convolution of the two (bottom) for the AM technique.

the generated signal presented in Fig. 5) in order to find the one that produces the lowest cross correlation coefficient.

The results are presented in Fig. 14. The number of phases in each load corresponds to the number of different load values. It can be seen that the proposed technique is extremely effective for some loads and is capable of lowering the cross correlation coefficient to 0.2. The cross correlation coefficient for the AES load is 0.35, showing over 40% reduction compared to the RPS technique. The maximum cross correlation coefficient was found to be 0.53.

In order to look at the effects of the applied technique in the frequency domain, we plot the spectra of the load, flying capacitor signal generated for that load, and the product of the two in Fig. 15. It can be seen that, unlike power scrambling, the AM technique results in the load spectra that is masked much better by the generated flying capacitance signal.

As a result, the proposed technique can not only improve the security of the existing cryptographic algorithm, but it can also be used to identify the cryptographic algorithms, which can be protected in a more efficient manner. The ones that achieve lower cross correlation coefficient are more attractive from the security standpoint.

So far, we have not considered the third condition for the capacitance value. The capacitance can have only discrete values that correspond to the number of SC dc–dc unit cells that are turned on at any given moment in time. We vary the number of unit cells between 2 and 25, while we keep the total flying capacitance equal to 1 nF and observe the change in the correlation coefficient. For the sake of clarity, we represent the results for the loads with four, six, eight, and ten different load values in Fig. 16. It can be seen that the number of the unit cells required for low cross correlation coefficient is fairly small in all cases. With only ten unit cells, the cross correlation coefficient is less than 5% different from the ideal nondiscretisized case for all loads. This is highly important for two reasons. First, should a design need a bigger unit cell (or equivalently smaller number of cells for the same total Cfly), in order to provide correct functionality during computationally intensive operations, there is a very small penalty to pay in cross correlation coefficient degradation. Second, the number of the unit cells stays limited by the minimum driver size during the design phase and is not affected by the added security, as explained next.

The drivers that are controlling the switches are usually composed of several inverter-based buffers that are used to transmit the switching clock to the switches. When the converter is divided into the unit cells, the flying capacitance in each cell is only a fraction of the total flying capacitance, and the switches are scaled together with the flying capacitor value. Smaller switches need smaller buffers to drive them. Once the driver is composed of just one minimum-sized inverter, there is no point in scaling down the unit cell further. Further scaling will only degrade the efficiency due to the higher switching loss [12].

As a result, it is important to note that the proposed technique does not imply additional constraint in determining the number of unit cells. For the converter used in this work, the minimum size unit cell has the flying capacitance of 60 pF that was previously determined by the minimum-sized driver buffer. Since the total flying capacitance is equal to 1 nF, the number of available unit cells is 17. From Fig. 16, it can be appreciated that the cross correlation coefficient for this number of unit cells is close to an ideal cross correlation coefficient for all tested loads.

B. TVLA: Correlation Test

Differential and correlation attacks, either power or EM, exploit the fact that different inputs to the cryptographic system produce different measurable characteristics [26]. In Section V-A, we proved that the proposed methodology lowers the correlation coefficient between the load signal and the leaked signal to 0.2. However, the leaked signal might still reveal secret information if it contains some recognizable pattern for a particular secret key, even though it is decorrelated from the load. TVLA is a technique based on signal statistics that is used to find points in the measured traces that could be leaking secret information.

TVLA provides two different metrics: t-test and ρ-test. While t-test has a very low sampling complexity and is a popular metric for security evaluation, ρ-test provides more

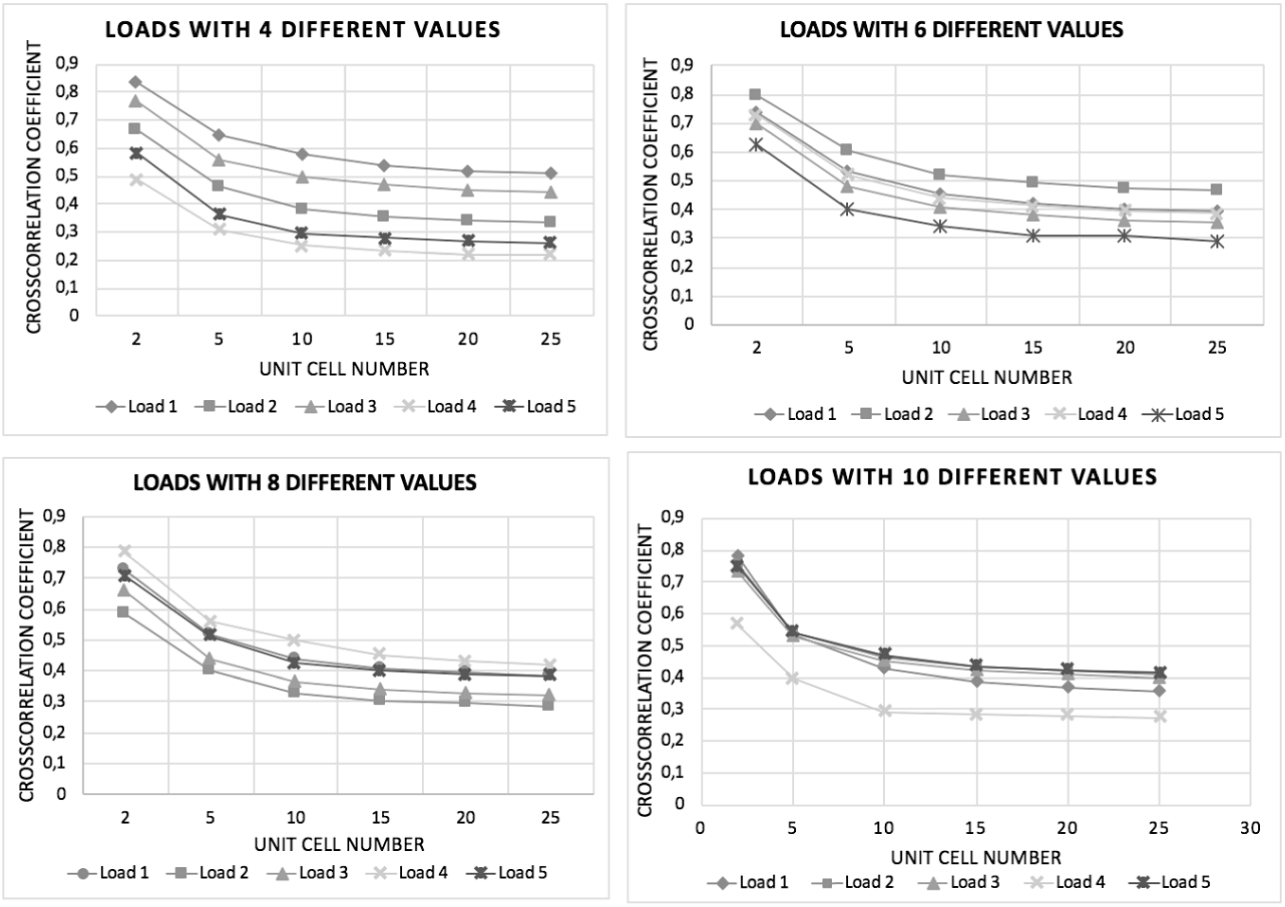

Fig. 16. Cross correlation coefficient for the presented technique for a different number of unit cells.

useful information over a long time window. Both tests are applied to the proposed methodology as follows.

The same steps that were used in [26] for ρ-test are applied here to the load computed from the measured power traces for AES algorithm execution also provided in [26].

First, the measured traces are divided into k sets, where each set has N/k traces. The values for N and k used in [26] are: $N = 2560$ and $k = 10$. Next, k different partitions are created. For each partition, one set out of ten is chosen to be a test set, and the rest of the sets belong to the profile set. Then, a model is applied to the profile set. For example, the model used in [26] is based on the first byte of the input plaintexts. All traces that are measured for the input plaintexts that have the same first byte are grouped together. Consequently, there will be 256 different groups inside each profile set since there are 256 different values for the first byte. Next, we take the average of all the traces belonging to each group leading to simplification of the profile set that now contains only 256 different traces. The correlation coefficient curve is now computed sample-wise between the simplified profile set and the test set. This procedure is repeated for each partition to overcome bias in the statistical test. Finally, the mean of the corresponding correlation coefficients is computed and the Fisher z-transformation is then applied to correlation coefficients. All time points with the corresponding correlation coefficient above 4.5 threshold, are considered to be leaky.

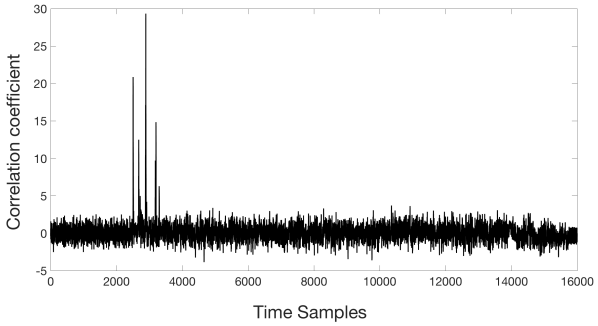

Fig. 17. Normalized correlation coefficients for unsecured AES execution.

First, we apply the ρ-test to the circuit where no security technique is applied. When we apply the test, the number of leaky points is 62, which is the same number reported in [26]. Fig. 17 shows the normalized correlation coefficients after the Fisher z-transformation. It can be seen that the leaky points (i.e., points above 4.5) correspond to the first round of the AES algorithm.

When the proposed AM technique for the same AES load is applied, the number of leaky points drops to zero (see Fig. 18). Consequently, the proposed technique not only lowers the correlation between the load and the leaked signal, but it

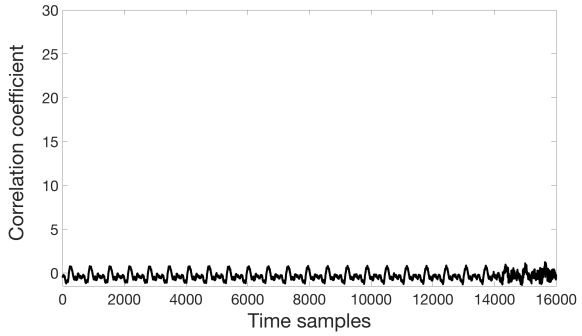

Fig. 18. Normalized correlation coefficients for secured AES execution.

is also extremely robust against differential and correlation attacks.

Next, we apply *t-test* in order to provide fair comparison of the proposed methodology with the other works proposed in the literature that use the same evaluation metric. For *t-test*, two data sets, one statistically random and another fixed with certain properties that allow it to be statistically distinguished from the random one, are chosen for a certain fixed key. *t*-Statistic is computed according to Welch's test and all points where the absolute value of *t*-Statistic is above 4.5 are considered to be leaky. We use the AES measured power traces provided in [26] and perform *t-test* for each time point. When no secured technique is applied, there are 9390 leaky points, the same number reported in [26]. When the AM technique is applied, the number of leaky points drops to only 3. Then, the RPS technique is applied using 8, 16, and 32 unit cells. The number of leaky points is 259, 203, and 156. It can be seen that the proposed AM technique achieves two orders of magnitude improvement in security over the RPS technique for single-phase switched-capacitor dc–dc converters.

VI. Overhead Analysis

In order to evaluate the power overhead and the converter efficiency when the AM technique is applied, we simulate the switched-capacitor dc–dc converter in Cadence. We generate a signal in Scilab that determines the number of unit cells that need to be turned on at any time. This signal is loaded to a memory. The values are read and fed into the thermomether decoder. Finally, the output of the thermomether decoder is distributed to the unit cells as an ON/OFF signal. We apply four different dynamic loads that were generated by Scilab. The number of the different phases in each load is 5, 10, 20, and 100.

Fig. 19 shows the waveforms of the load, output voltage when the AM technique is applied, and the flying capacitance signal. For the sake of clarity, the figure has been zoomed-in Fig. 20. It can be seen that around time equal to 148.5 μs, the converter is perfectly capable of tracking the large changes in the load even though the number of dc–dc unit cell used at that time is low.

Fig. 21 shows the efficiency of the converter without any security technique applied to it (marked as unsecured dc–dc converter) and with AM technique applied to it (marked as secured dc–dc converter). It can be seen that the AM technique lowers the efficiency by less than 10% for all loads.

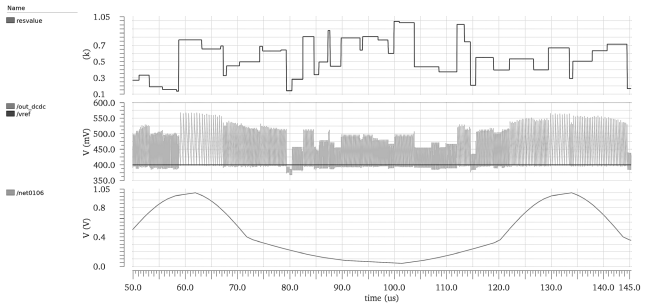

Fig. 19. Cadence waveforms for the load, output voltage, and flying capacitor.

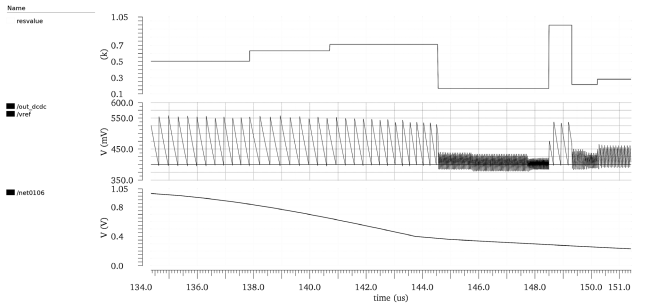

Fig. 20. Zoomed in view of Fig. 19.

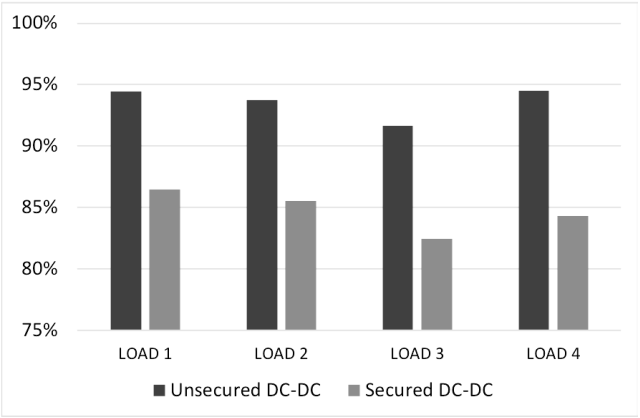

Fig. 21. Efficiency comparison between secured and unsecured dc–dc converters.

As mentioned before, the area overhead of the proposed technique when compared to the unsecured converter is only due to the control logic. Since the same technology (i.e., 28-nm FDSOI) and the same converter type (i.e., single-phase switched-capacitor converter) distributed as unit cells are used here and in [7], the area overhead for the AM technique can be estimated to be around 16%, similar to the area overhead reported there.

The performance of the converter is not affected since it is still perfectly capable of reacting fast to the load changes.

An overview of the comparison with state-of-the-art techniques is shown in Table I. In order to ensure fair comparison, the table lists previous works that use the same metric for security evaluation: *t*-test. Two numbers are reported for this statistic: the number of leaky points with the proposed technique and the number of leaky points of the unsecured design. In addition, power, area, and performance overheads are also listed for all techniques.

TABLE I
COMPARISON OF AM TECHNIQUE WITH EXISTING COUNTERMEASURES

Technique	AM	RPS	TVTF [16]	JSSC'18 [9]	ISSCC'19 [10]
Technology	28nm	28nm	65nm	130nm	130nm
Area	1.16X	1.16X	1.2X	2X	1.38X
Power	1.15X	1.15X	1.24X	2X	1.35X
Performance	No penalty	No penalty	No penalty	No penalty	1.1X
t-statistic	3/9390	203/9390	8.37/190.1	37.9/197.1	11.9/258
# of traces for t-test	2K	2K	7.5K	1M	>1M [1]
Attack type	EM	EM	Power	Power	Power and EM
Converter type	Single-phase SC	Single-phase SC	Multi-phase SC	Inductive Voltage Regulator	Digital-LDO

It can be seen that the proposed methodology achieves reduction in t-statistic is 99.93% while incurring no performance degradation and increasing power consumption by only 15% and area by 16%, compared to the unsecured design without voltage regulators. Consequently, an excellent tradeoff between the added security and converter power, area, and performance makes the proposed technique an attractive solution for protection from EM side-channel attacks.

VII. CONCLUSION

We have presented a novel technique for single-phase SC dc–dc converters to improve the security of the IoT devices against side-channel attacks. The technique relies on detailed physical mechanisms of the leaked signal and it is based on the AM of the load current by the flying capacitance that acts as a carrier. The capacitance is changed in a deterministic fashion in order to achieve overlapping of the load spectrum in the leaked signal spectrum. The results show that the technique can lower the cross correlation coefficient between the leaked signal and the load to below 0.2. The number of SC dc–dc unit cells that are needed to achieve low correlation coefficients is below the limit set by the design, resulting in no additional impact on the power density of the converter. When the statistical test based on TVLA is applied to the protected circuit, the number of leaky points is reduced to zero, indicating an excellent robustness against differential and correlation attacks. The presented methodology lowers the converter efficiency by less than 10% and has a minimal impact on the area and performance of the converter.

ACKNOWLEDGMENT

The authors would like to thank Prof. Mariano Garcia Otero from the Technical University of Madrid for his help on evaluation metric.

REFERENCES

[1] D. Agrawal *et al.*, "The EM side-channel(s): Attacks and assessment methodologies," in *Proc. CHES*, in Lecture Notes in Computer Science, vol. 2523, 2002, pp. 29–45.

[2] D. Das *et al.*, "Ground-up root-cause analysis guided low-overhead generic countermeasure for electro-magnetic side-channel attack," Criptology ePrint Arch., Tech. Rep. 2018/620, 2018, p. 620.

[3] R. Callan, A. Zajić, and M. Prvulovic, "FASE: Finding amplitude-modulated side-channel emanations," in *Proc. 42nd Annu. Int. Symp. Comput. Archit. (ISCA)*, Jun. 2015, pp. 592–603.

[1]The number of traces for t-test is not reported, but the number of traces used for correlation coefficient is over 1 million.

[4] L. Sauvage, S. Guilley, and Y. Mathieu, "Electromagnetic radiations of FPGAs: High spatial resolution cartography and attack on a cryptographic module," *ACM Trans. Comput. Logic*, vol. 2, no. 1, pp. 1–24, Aug. 2008, Art. no. 4.

[5] P. Maistri, S. Tiran, P. Maurine, I. Koren, and R. Leveugle, "Countermeasures against EM analysis for a secured FPGA-based AES implementation," in *Proc. Int. Conf. Reconfigurable Comput. FPGAs (ReConFig)*, Dec. 2013, pp. 1–6.

[6] R. Jevtic *et al.*, "Per-core DVFS for many-core processors in 28 nm FDSOI technology," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 23, no. 4, pp. 723–730, Apr. 2015.

[7] B. Zimmer *et al.*, "A RISC-V vector processor with simultaneous-switching switched-capacitor DC–DC converters in 28 nm FDSOI," *IEEE J. Solid-State Circuits*, vol. 51, no. 4, pp. 930–942, Apr. 2016.

[8] M. Turnquist *et al.*, "Fully integrated DC-DC converter and a 0.4V 32-bit CPU with timing-error prevention supplied from a prototype 1.55V Li-ion battery," in *Proc. Symp. VLSI Circuits (VLSI Circuits)*, Jun. 2015, pp. C320–C321.

[9] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering," *IEEE J. Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, Feb. 2019.

[10] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "25.3 A 128b AES engine with higher resistance to power and electromagnetic side-channel attacks enabled by a security-aware integrated all-digital low-dropout regulator," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2019, pp. 404–406.

[11] D. Kamel *et al*, "Towards securing low-power digital circuits with ultra-low-voltage Vdd randomizers," in *Proc. Int. Conf. Secur., Privacy, Appl. Cryptogr. Eng.*, 2016, pp. 233–248.

[12] H.-P. Le, S. R. Sanders, and E. Alon, "Design techniques for fully integrated switched-capacitor DC-DC converters," *IEEE J. Solid-State Circuits*, vol. 46, no. 9, pp. 2120–2131, Sep. 2011.

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

[15] R. Jevtic, M. Ylitolva, and L. Koskinen, "Reconfigurable switched capacitor DC-DC converter for improved security in IoT devices," in *Proc. 28th Int. Symp. Power Timing Modeling, Optim. Simulation (PATMOS)*, Jul. 2018.

[16] A. Ghosh, D. Das, and S. Sen, "Physical time-varying transfer functions as generic low-overhead power-SCA countermeasure," 2020, *arXiv:2003.07440*. [Online]. Available: http://arxiv.org/abs/2003.07440

[17] D. Das *et al.*, "27.3 EM and power SCA-resilient AES-256 in 65 nm CMOS through >350X current-domain signature attenuation," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2020, pp. 424–426.

[18] 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.

[19] C. Wang, Y. Cai, H. Wang, and Q. Zhou, "Electromagnetic equalizer: An active countermeasure against EM side-channel attack," in *Proc. Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2018, pp. 1–8.

[20] M. Hiienkari *et al.*, "A 3.15 pJ/cyc 32-bit RISC CPU with timing-error prevention and adaptive clocking in 28 nm CMOS," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Sep. 2014, pp. 1–4.

[21] F. U. Rahman *et al.*, "A unified clock and switched-capacitor-based power delivery architecture for variation tolerance in low-voltage SoC domains," *IEEE J. Solid-State Circuits*, vol. 54, no. 4, pp. 1173–1184, Apr. 2019.

[22] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *Proc. 20th Int. Conf. VLSI Design Held Jointly 6th Int. Conf. Embedded Syst. (VLSID)*, 2007, pp. 854–862.
[23] A. Krieg, J. Grinschgl, C. Steger, R. Weiss, and J. Haid, "A side channel attack countermeasure using system-on-chip power profile scrambling," in *Proc. IEEE 17th Int. On-Line Test. Symp.*, Jul. 2011, pp. 222–227.
[24] R. Korkikian *et al.*, "Practical instantaneous frequency analysis experiments," in *Proc. Int. Conf. E-Bus. Telecommun.*, 2013, pp. 17–34.
[25] F. Durvaux and F.-X. Standaert, "From improved leakage detection to the detection of points of interests in leakage traces," in *Advances in Cryptology EUROCRYPT* (Lecture Notes in Computer Science), vol. 9665, M. Fischlin and J. S. Coron, Eds. Berlin, Germany: Springer, May 2016, pp. 240–262.
[26] REASSURE Consortium, "Understanding leakage detection," in *Proc. Tutorial Co-Organized CARDIS*, Montpellier, France, Nov. 2018.
[27] *National Institute of Standards and Technology. Advanced Encryption Standard. Federal Information Processing*, Standard 197, 2001.
[28] D. J. Griffiths, *Introduction to Electrodynamics*, 4th ed. London, U.K.: Pearson, 2014.

Ruzica Jevtic (Senior Member, IEEE) received the B.S. degree in electrical engineering from the University of Belgrade, Belgrade, Serbia, in 2004, and the Ph.D. degree with European Ph.D. mention in electrical engineering from the Technical University of Madrid, Madrid, Spain, in 2009.

She was a Postdoctoral Fellow with the University of California at Berkeley, Berkeley, CA, USA, from 2011 to 2013, where she was engaged in low-power circuit design for energy-efficient microprocessors. She is currently an Assistant Professor with University San Pablo-CEU, Madrid. Her research interests include security and power management for digital circuits.

Dr. Jevtic was a recipient of the Marie Curie International Outgoing Fellowship and the Marie Curie Industry-Academia Partnerships and Pathways Fellowship.

Marko Ylitolva (Member, IEEE) received the B.Sc. degree in electronics and the M.Sc. degree in system electronics from the Faculty of Science and Engineering, University of Turku, Turku, Finland, in 2018.

He was a Research Assistant and a Project Researcher with the University of Turku from 2012 to 2019. He was involved in design of ultralow-power analog circuits. His research interests include energy-efficient energy converters and security against side-channel attacks in microprocessors for IoT devices. He is currently working at CoreHW, Turku, Finland, as an Analog IC Design Engineer.

Clara Calonge received the B.S. degree in computer science and the B.S. degree in communications from University San Pablo-CEU, Madrid, Spain, in 2019. She is currently pursuing the master's degree with the Technical University of Madrid, Madrid.

She has worked as an Intern in 2019 on Smart Cities Project in infrastructure company Ferrovial, Madrid. She has worked in Airbus Spain, Madrid, in 2020. Her research interests include security, big data, and computer networks.

Martti Ojanen received the M.Sc. degree in applied electronics from the Tampere University of Technology, Tampere, Finland, in 1993.

Afterward, he worked at Nokia, Finland, as a hardware (HW) and an IC Senior Design Engineer. He was a leading Designer for Nokias power management unit (PMU) application specific integrated circuits (ASICs) section, with four granted patents. From 2008, he worked as a Project Leader at STEricsson, Finland, on the improvement of PMU's intellectual properties (IPs) through miniaturization and cost, targeting top-level smartphone manufacturers as end-costumers (big volumes linked with reliability, high production yields, scalability, and end-products quality). In 2020, he joined the Faculty of Science and Technology, University of Turku, as a Senior Researcher, for modern edge computing approach with ASICs to enable advanced accelerators and sophisticated power management features.

Tero Santti (Member, IEEE) received the M.Sc. degree in electronics and information technology and the D.Sc. (Tech.) degree in microelectronics (computer systems) from the University of Turku, Turku, Finland, in 2002 and 2008, respectively.

He is currently a Senior Research Fellow with the University of Turku. Besides academia, he has been working in the industry and is a Co-Owner of a space technology company. His research interests include low-power electronics, digital imaging, field-programmable gate array (FPGA) prototyping, and space applications.

Lauri Koskinen (Member, IEEE) is the Chief Technology Officer (CTO) of Minima Processor and an Adjunct Professor with the University of Turku, Turku, Finland. He received a Fulbright Finland grant in the IC/Electronics field for a one-year postdoctoral visit to the UC Berkeley Wireless Research Center. He brings broad design expertise to Minima ranging from ultralow-power aspects of deep submicrometer transistors, up to the high-level realization of various systems (microcontrollers, deep learning, wireless biomedical sensors, audio, and video coders). He has authored or coauthored more than 50 articles in international conferences and journals.