IEEE Open Journal of
Circuits and Systems

Received 2 April 2023; revised 27 June 2023; accepted 2 August 2023. Date of publication 4 August 2023; date of current version 24 August 2023.

Digital Object Identifier 10.1109/OJCAS.2023.3302254

Physical Time-Varying Transfer Function as Generic Low-Overhead Power-SCA Countermeasure

ARCHISMAN GHOSH [1] (Graduate Student Member, IEEE), DEBAYAN DAS [2] (Member, IEEE), AND SHREYAS SEN [1] (Senior Member, IEEE)

[1]Purdue University, West Lafayette, IN 47907, USA
[2]Indian Institute of Science, Bengaluru 560012, India

This article was recommended by Associate Editor J. Viraraghavan.

CORRESPONDING AUTHOR: S. SEN (e-mail: shreyas@purdue.edu)

ABSTRACT Mathematically secure cryptographic algorithms leak significant side-channel information through their power supplies when implemented on a physical platform. These side-channel leakages can be exploited by an attacker to extract the secret key of an embedded device. The existing state-of-the-art countermeasures mainly focus on power balancing, gate-level masking, or signal-to-noise (SNR) reduction using noise injection and signature attenuation, all of which suffer either from the limitations of high power/area overheads, throughput degradation or are not synthesizable. In this article, we propose a generic low-overhead digital-friendly power SCA countermeasure utilizing a physical Time-Varying Transfer Function (TVTF) by randomly shuffling distributed switched capacitors to significantly obfuscate the traces in the time domain. We evaluate our proposed technique utilizing a MATLAB-based system-level simulation. Finally, we implement a 65nm CMOS prototype IC and evaluate our technique against power side-channel attacks (SCA). System-level simulation results of the TVTF-AES show $\sim 5000\times$ minimum traces to disclosure (MTD) improvement over the unprotected implementation with $\sim 1.25\times$ power and $\sim 1.2\times$ area overheads, and without any performance degradation. SCA evaluation with the prototype IC shows $3.4M$ MTD which is $500\times$ greater than the unprotected solution.

INDEX TERMS Power side-channel attack, low-overhead countermeasure, physical obfuscation, time-varying transfer function, synthesizable, generic.

I. INTRODUCTION

IN TODAY'S data-driven Internet-connected (IoT) world, security, and confidentiality of communication and computing are of utmost importance. To address these needs, various cryptographic algorithms have been proposed to date, which are computationally secure. However, as these algorithms are implemented on a physical substrate, it leaks critical 'side-channel' information in the form of power consumption [1], [2], electromagnetic (EM) emanation [3], [4], cache hits/misses [5], [6], and so on. These side-channel leakages can be exploited by attackers to extract the secret key from a cryptographic device. In this article, we focus on the power SCA attack on an AES engine.

A power analysis attack is one of the most common side-channel attacks on embedded systems. The time-complexity of breaking an AES-256 engine is reduced from 2^{256} for a brute-force attack to 2^{13} for a power SCA attack, as the key search space reduces to $2^8 = 256$ possibilities for each of the 16 key bytes. Power SCA is performed by measuring the power consumption of a target device during the encryption phase. Every captured trace is synchronized with a chosen plaintext (PT) or a known ciphertext (CT). The attacker can either feed chosen PTs to the target device or record the output CT while capturing the power traces. Once the traces are collected, a differential/correlational power analysis (DPA/CPA) attack [1], [2] is performed using a hamming weight (HW) or a hamming distance (HD) model. The HW leakage model considers the number of ones on the data bus during a switching activity, while HD model takes into account the number of bits switching from one state to the next. HW models are useful for software crypto implementations on various microcontrollers, while HD models are typically used for attacks on hardware crypto implementations where the operations are

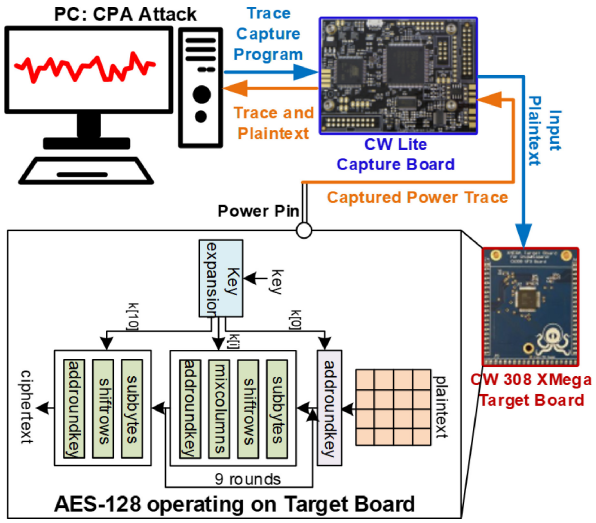

FIGURE 1. An example Power SCA attack setup using Chipwhisperer on an 8-bit Atmega microcontroller running AES-128 encryption.

highly parallelized and the same register is updated each clock cycle to store the updated state.

Fig. 1 shows an example of the power SCA attack set-up using the Chipwhisperer platform [7]. Traces are collected from an unprotected software AES-128 engine running on an 8-bit Atmega microcontroller for varying chosen input plaintexts which has been provided by Chipwhisperer board to the microcontroller. The traces from the Xmega target board is transferred to the PC, where a CPA attack is performed to extract the secret 128-bit key. It should be noted that the proposed solution is a generic countermeasure and can be used in any ASIC or fabricated CPU (or microcontroller) platform irrespective of the encryption algorithm. However, we choose to use software AES-128 on an XMEGA 8-bit microcontroller and HW-based CPA for initial exploration of theory as CPA attack on the software AES-128 shows a low initial MTD ($\sim 20-200$). Low MTD allows us to explore different countermeasures with reduced time for the collection of traces, as compared to a hardware implementation which would have a higher initial MTD 1000 for FPGA and $2000-10K$ in ASIC. The key metric to evaluate a countermeasure is to analyze the increase in MTD compared to the unprotected implementation. In summary, we analyze a fully-synthesizable time-domain obfuscation-based countermeasure utilizing multi-phase switched capacitors to achieve $\sim 5000\times$ increase in system level simulations and $500\times$ increase in ASIC implementation. We also analyze the reason behind the reduced efficacy of ASIC implementation in this paper.

First, we build a mathematical model for the countermeasure circuit. The traces collected from devices under attack is fed to the model. Finally, modified traces from the model are used for power side-channel analysis. As the proposed countermeasure is generic, it can be implemented across any generic processor or cryptographic core.

In this work, we focus on one particular key byte (13^{th} byte, as it required the minimum number of traces to break for the unprotected implementation) to demonstrate the resiliency of our proposed countermeasure.

A. MOTIVATION

Although power analysis attacks have been known for more than two decades, the threat of power SCA is increasing with the growth of miniaturized and resource-constrained IoT devices. For example, an 8/16-bit microcontroller consumes very low power but it has a high signal-to-noise ratio (SNR) making them more vulnerable to SCA attacks compared to the 64-bit processors (more 'algorithmic noise'). For side-channel analysis, attack models are built byte-wise or nibble-wise. Hence it is more prone to correlate to bytes being attacked for 8-bit/16-bit architectures. Hence, the development of a low-overhead countermeasure is extremely critical to protect these embedded devices against power SCA attacks.

In addition to the low-overhead requirements, a countermeasure can be easily incorporated into a product if it is generic and synthesizable. Generic countermeasures are preferred from an industry standpoint as it helps to maintain the legacy of the existing crypto algorithms and can be used as a wrapper without any modification to the crypto core. Synthesizable countermeasures help in scalability across different technology nodes and do not require manual efforts, aiding non-recurring engineering costs. These are important factors for an industry to adopt a particular countermeasure. All of these reasons have motivated the design of the proposed technique.

This article demonstrates a time-varying transfer function-based low-overhead physical countermeasure utilizing switched capacitors to reduce the information content of the leakage from the crypto engine. Using time-varying transfer functions (TVTF) by efficient randomization of physical resources in the form of switched capacitors, the traces are significantly obfuscated, without any performance degradation. This is a low-overhead circuit-level generic countermeasure and can be extended to any other crypto algorithm. Moreover, the circuit is entirely digital and can be synthesized, aiding technology scaling. Note that switches are implemented using power gates which are technology scalable in most libraries. Capacitors are utilized by DCAP cells and placed using an industry-standard place & routing tool (Cadence Innovus).

B. CONTRIBUTIONS

The specific contributions of this work are:

- *Proposal of physical time-domain obfuscation based countermeasure:* This paper proposes physical time-varying transfer functions (TVTF) to obfuscate the information leakage due to the crypto operations in the power traces. TVTF is achieved by efficient randomization of distributed switching capacitors. This

countermeasure is different from clock randomization-based countermeasures such as DVFS (Dynamic Voltage Frequency Scaling). Traces can be easily distinguishable from the trace as clock edge shifts in DVFS, making DVFS more prone to attacks, unlike TVTF.

- *Design space exploration for synthesizable countermeasure:* With the proposed technique, we mathematically and experimentally demonstrate the effect of multiple capacitors charging from the supply or driving the AES core at a given phase, revealing that randomly choosing a single capacitor each for charging/driving AES is the best choice to achieve the maximum protection against power SCA. Moreover, the proposed countermeasure is generic and digital-friendly allowing scalability across different technologies as it can be implemented without any analog components unlike other switched capacitor-based countermeasures [8].
- *Simulation-based study as proof-of-concept:* System-level simulation shows that the power SCA immunity is enhanced by $\sim 5000\times$ compared to the unprotected implementation with only 20%, 25% area and power overheads respectively, and without any performance degradation.
- *Mathematical explanation of claim:* The paper proposes a solution and represents a mathematical explanation for it. All the components are assumed to be ideal to validate the immunity provided by our countermeasure with respect to the unprotected implementation. Practically, system noise would exist which will make the SNR of the power signatures even lower enhancing the MTD.
- *65nm TSMC IC for demonstrating the technique:* Finally, we demonstrate the technique in silicon by fabricating it using TSMC 65nm technology node. it is observed that IC implementation achieves $500\times$ improvement in MTD instead of $5000\times$ improvement indicated by system-level simulations. We discuss in detail the shortcomings and the room for improvement of the ASIC implementation in this article.

C. PAPER ORGANIZATION

The remainder of the paper is organized as follows. Section II discusses the existing state-of-the-art in detail, along with the analysis of previously proposed switched capacitor-based countermeasures. In Section III, the theoretical background and analysis of the proposed TVTF countermeasure are presented. Section IV discusses more experiments and shows a mathematical formulation to evaluate the efficacy of the proposed TVTF-based multi-phase switched capacitor technique. Next, Section V presents the implementation results, followed by Section VI which analyses the tuning knobs for MTD improvement. We present a prototype IC fabricated based on the concept in Section VII. Finally, Section VIII concludes the paper.

II. BACKGROUND AND RELATED WORKS

A. BRIEF ABOUT POWER SIDE CHANNEL ATTACKS

Mathematically secured cryptographic algorithms when implemented in silicon or in software leaks critical information in terms of the power side channel. Traditional power side channel attack setup is shown in Fig. 1. First, traces are collected for different plaintexts and the same key. Ciphertext is anyway publicly available. Based on that, a hamming distance/hamming weight model can be built for all possible key bytes. Finally, we correlate the model with respect to traces and guess the correct key byte based on the highest correlation. It is observed that after some traces actual key byte is revealed. The minimum number of encryptions to reveal the correct key byte is called Minimum Traces to Disclosure (MTD). Clearly, it is a security metric and indicates how long an encryption engine is safe against this type of attack.

However, attack algorithms and models are getting improved day by day. Hence, a leakage analysis is required to determine the possibility of meaningful leakage which can be exploited by future algorithms. Test vector leakage assessment (TVLA) is one of the most trusted leakage assessment algorithms [9]. $t-value$ is calculated using Welch's t-test on a fixed and random set of side-channel traces. It is calculated by the equation (1).

$$t = \frac{\mu_r - \mu_f}{\sqrt{\frac{\sigma_r^2}{n_r} + \frac{\sigma_f^2}{n_f}}} \tag{1}$$

where, n_r, n_f are the number of random and fixed traces respectively. Mean and the standard deviation is presented by μ_r and σ_r for a random set of traces respectively. μ_f and σ_f signify the mean and standard deviation of the fixed set of traces. A $|t| - value$ of 4.5 or less indicates that traces do not have any data-dependent leakage.

B. STATE-OF-THE-ART POWER SCA COUNTERMEASURES

The state-of-the-art hardware countermeasure for power SCA resistance can be broadly classified into three categories - logical, architectural, and physical. The first category of logical countermeasures focuses on designing SCA-resistant logic styles to equalize the power in each cycle of the clock. This includes dual-rail precharge (DRP) logic style [12] and logic-level hiding like the sense amplifier-based logic (SABL) [13], both of which require custom library cell design, and also incurs a large area overhead. Other logic-level hiding techniques like the wave dynamic differential logic (WDDL) [14], [15], and bridge boost logic (BBL) [16] also fall under this category, however, they are based on single rail standard cell libraries. WDDL was the first power SCA-resistant circuit validated in silicon with an MTD of 21K, incurring a $3\times$ area, $4\times$ power, overheads as well as $4\times$ performance degradation. Logic level masking at the gate level includes masked dual-rail pre-charge logic [17], [18], which can be built using the standard library cells, however,

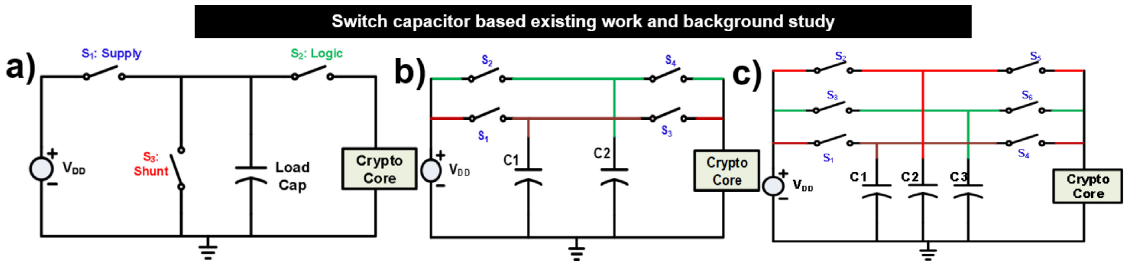

FIGURE 2. a) Switched Capacitor Current Equalizer Countermeasure proposed in [8], [10]. It has 3 phases of operations: 1. charging the load capacitor 2. charging the crypto core from the load capacitor 3. resetting the load capacitor voltage value to a predefined voltage value. b) 2-phase switch capacitor without current equalizer solution. Switching activity is explained in Table 1. A similar solution is proposed in [11]. c) Multiple capacitor-based circuits. Switching is mentioned at Table 1.

it suffers from the high area and power overheads. Different types of adiabatic logic-based countermeasures have been proposed [19], which require different logic families deviating from the standard CMOS implementation, and incur higher overheads. Recently, Thapliyal et al. [19] showed an MTD improvement of 10× with ∼ 90% power and area overheads using adiabatic logic.

The second category belongs to architectural countermeasures, which utilize time or amplitude distortions to hide the leakage. Random insertion of dummy operations, shuffling of operations, clock randomization, and random order execution fall in this category of architecture-level hiding. These shuffling techniques involving randomizing the order of instructions are limited by the number of instructions that can be shuffled depending on each algorithm and do not provide high protection [20]. Clock randomization-based countermeasures including dynamic voltage and frequency scaling (DVFS) has been shown to be defeated by observing the clock edges at the supply [21]. Masking schemes at the architecture level include boolean masking, masking multipliers, and random pre-charge. All these countermeasures are typically algorithm and architecture-specific and hence are not generic as it requires modifications in the algorithm itself.

The final category of power SCA protection is the physical countermeasure. The most well-known scheme in this category is noise injection. However, noise insertion suffers from the extremely high area and power overheads [22], [23]. Other techniques in this category are based on supply isolation. Low-dropout (LDO) regulators have been shown to provide power SCA resilience [24]. However, it has also been shown that an ideal series LDO implementation is inherently insecure [23], [25]. Buck-converter-based integrated voltage regulators (IVRs) suffer from area overhead due to embedded passives [26]. An on-chip signal suppression-based countermeasure has been proposed in [27]. Cell-level voltage randomization has been proposed recently [28], but it required a custom cell library and can not be easily scaled over different technology nodes. Moreover, it only improved the SCA security by ∼ 10× with the high area and power overheads. Recently, Das et al. [23], [25] proposed signature attenuation to enhance the minimum traces to disclosure (MTD) significantly. Although signature suppression is an efficient SNR reduction technique, it utilizes mixed-signal

TABLE 1. Switching pattern for the 2-phase switched capacitor without reset.

Time instance	Connected to V_{DD}	Connected to AES
t_{2n}	C1	C2
t_{2n+1}	C2	C1

circuits (high output impedance current source biased in saturation), which are not easily scalable across different technology nodes. Another physical-level countermeasure proposed by Tokunaga et al. utilizes a switched capacitor technique to isolate the AES engine from the power supply [8], [10]. This is a novel circuit-level technique as it improves the MTD significantly (> 2500×), but suffers from performance degradation. We will look into the operation of this circuit in the following sub-section. In another work, further improvements have been discussed [29] to reduce cross-talk, which is claimed to be more immune to SCA attacks.

C. SWITCHED CAPACITOR CURRENT EQUALIZER COUNTERMEASURE

The idea behind the switched capacitor current equalizer is to isolate the AES engine from the supply using a charging capacitor [8]. This countermeasure, as shown in Fig. 2(a) has three phases of operations. In the first phase, switch S_1 is closed and the load capacitor is charged. In the second phase of operation, switch S_2 is closed and the capacitor is connected to the crypto core, with complete isolation from the supply. In the third phase of this circuit (switch S_3 closed), the load capacitor is discharged (reset) to a fixed voltage so that the residual charge is not passed to the supply in the next phase (first phase: S_1 closed). To accommodate these three phases of operation, three identical switched capacitor modules are utilized providing uninterrupted AES operations. While this countermeasure provides high protection guarantees, it suffers from a 2× throughput degradation. Iso-performance would require using high values of capacitances, leading to > 2× area penalty. It needs to be noted that the third phase (reset) of operation is extremely important so that the discharged capacitor (connected to AES in the second phase) is not directly connected to the power supply.

Limitations of the Reset Phase: The reset phase of the countermeasure involves a bias voltage which renders it non-synthesizable and would not scale across different

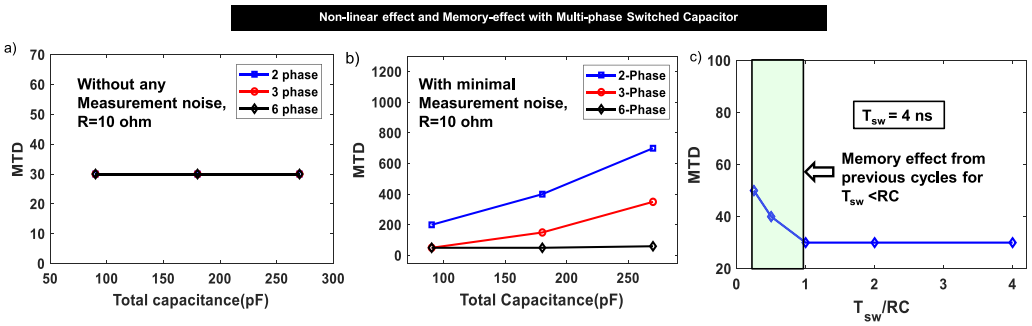

FIGURE 3. (a, b): Effect of residue voltage addition for a multi-phase capacitor with and without measurement noise. Measurement noise is added to emulate the original noise present in the captured traces, to see the effect of signature attenuation due to the capacitor. MTD is reduced when the number of phases is increased in the case of the deterministic algorithm. The trend is different from the final pseudo-random algorithm which is discussed later. (c): Memory effect (shown for baseline 2-phase circuit) helps in cases of very high time constant (RC) or at higher switching frequencies. At our chosen RC (in the flat region, $C = 200pF$, $R = 10\Omega$), MTD is not increased. Also in the zone where the memory effect is useful, increasing the switching frequency will increase power overheads, while high R and C choices will increase the area overhead.

technologies. Also, every time resetting switch capacitors to a predefined voltage value increases voltage swing across the capacitor, which increments power overhead. Hence, we will leverage the switched capacitor-based technique without the reset phase.

D. EVALUATION OF SWITCHED CAPACITOR PROTECTION WITHOUT RESET

To make the switched capacitor current equalizer circuit synthesizable, we need to get rid of the third phase of operation, where the capacitors are getting reset to a fixed bias (analog) voltage. The modified circuit shown in Fig. 2(b) consists of two phases with two load capacitors. In the first phase (t0), the capacitor (C1) is connected to the AES core, while the other capacitor (C2) is connected to the supply for charging. In the alternate phase (t1), C2 drives the crypto engine while C1 is charged from the supply. The residual voltage on a capacitor after it has been connected to AES is given by,

$$V_{res} = V_{DD} - \frac{1}{C}\int_{t_n}^{t_n+T} i_{AES}dt \tag{2}$$

where i_{AES}, T and C are the AES current, switching period and capacitance of each unit capacitor respectively. Hence, the supply current as a function of time is given as,

$$i_{sup}(t) = \frac{V_{DD} - V_{res}}{R}e^{-\frac{t}{RC}} \tag{3}$$

where R is the ON resistance of the switch. From eqn. (3), it is clear that the entire residue (integrated voltage) gets connected to the supply thereby leaking through the power supply. Similar approach has been taken in [11]. In this work, capacitors have been included in packaging instead of IC, which makes it vulnerable to invasive attack. The isolation just changes the traces in a deterministic manner which means in the case of CPA, the correlation point will change, however, it will still correlate. We observe a very small improvement in MTD ($< 10\times$) with the 2-phase switched capacitor without reset compared to an unprotected implementation (initial MTD $\sim$ 20) since this circuit does not achieve any supply isolation. Attenuation due to capacitors slightly increases MTD.

TABLE 2. Switching pattern for the 3-phase switched capacitor.

Time instance	Connected to V_{DD}		Connected to AES
t_{6n}	C1	C2	C3
t_{6n+1}			C1
t_{6n+2}	C1	C3	C2
t_{6n+3}			C3
t_{6n+4}	C2	C3	C1
t_{6n+5}			C2

Next, we study the effect of multiple phases of the switched capacitors without reset and examine if the addition of multiple phases which causes the non-linear transformation to power trace has any significant role in providing SCA protection.

E. MULTI-PHASE SWITCHED CAPACITOR IMPLEMENTATION

Here, we explore the effects of nonlinearity (NL) and memory by charging multiple capacitors together in a phase, while another capacitor drives the AES engine in that phase. Fig. 2(c) shows a three-phase switched capacitor circuit without any reset phase. Note that we refer to this circuit as three-phase because of the three capacitors (N = 3) which connect to the AES one at a time. Table 2 shows the switching activity for the three capacitors. This strategy can be extended to a larger number of distributed switching capacitors which we explore in the later part of the paper.

1) EFFECT OF NON-LINEARITY DUE TO MULTI-CAP CHARGING

Integration is a non-linear operation. Using a capacitor integrates current trace over a specified time to introduce non-linearity. Fig. 3(a) shows that the effect of just introducing non-linearity does not enhance the MTD. Hence, any influence on the MTD due to this strategy is solely due to the signature attenuation as the voltage fluctuation across the AES gets suppressed by the load capacitor and part of it gets reflected through the ON switch during the charging phase. To observe this effect of signature attenuation, we inject a small amount of noise calculated from the initial SNR (20dB) of the captured traces. With the peak AES current of $3mA$,

SNR of 20dB implies that the measurement noise present in the signal is $0.3mA$. Emulating this measurement noise, we observe the effect of signature attenuation with the increase in total capacitance as shown in Fig. 3(b). Now, the 2-phase (2 unit capacitors) switched capacitor implementation shows higher MTD than the 3-6-phase implementations as the unit capacitance becomes higher (total capacitance is constant for iso-area overhead).

2) EFFECT OF MEMORY ON MTD

Next, we analyze the memory effect of the distributed switched capacitor architecture on MTD. After a capacitor has been connected to the AES engine, it has been discharged up to a certain voltage. Now if we do not allow it to charge back completely, i.e., if the switching period is much lower than the RC time constant ($T_{sw} < RC$, R being the ON resistance of the switch and C is the unit capacitance of the 2-phase switched capacitor), then the effect of previous samples can be spread across multiple next cycles, leading to power trace distortion. However, as seen from Fig. 3(c), this obfuscation due to the memory effect is rather small and only increases the MTD slightly. Also, to leverage this small benefit would mean that the switching frequency (f_{sw}) is increased leading to a trade-off with the power overhead. Another way to satisfy the condition is to increase either capacitor size or decrease device size (hence increasing the impedance of the switches.) But, increasing capacitance increases area overhead. Decreasing device size beyond a point (length of the device according to different technology) is impossible and MTD does not increase much to the resistance of switches operating in the linear region as shown in Fig. 3(c). *Hence, partial charging is not an efficient technique to enhance MTD as information is still being leaked despite some distortion in the power trace.*

From these observations, we can conclude that multi-phase switched capacitor if used in a deterministic way does not produce significant distortion of the power traces and can be broken easily. We aim to achieve high-power SCA protection with low capacitances (low area overhead) and utilize physical time-based obfuscation techniques. It should be noted that for the rest of this work, we do not consider the effect of measurement noise unless mentioned otherwise, as we focus on evaluating the efficacy of physical time-domain obfuscation, rather than the effect of signature attenuation. This work utilizes the multi-phase distributed switched capacitor technique with physical time-domain pseudo-random obfuscation of the traces and demonstrates high SCA immunity with low area and power overheads and without any performance degradation.

III. MULTI-PHASE SWITCHED CAPACITOR WITH PHYSICAL TIME-VARYING TRANSFER FUNCTION

In the previous sections, it is shown that multi-phase capacitors in itself do not provide sufficient immunity to protect against power SCA attacks. Without the reset phase, the residual voltage of the capacitors leaks to the power supply and can be broken within a small MTD. Now, if these multi-phase switching capacitors can be randomized such that they connect to the power supply at different points in time, the information content can be reduced significantly due to time-domain obfuscation of traces.

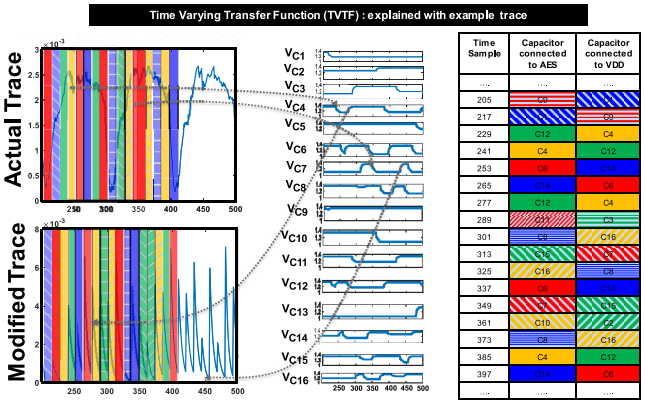

FIGURE 4. An example of TVTF-based randomization within a single cycle. AES trace is integrated and shuffled utilizing Algorithm 1 providing significant obfuscation in the modified power traces.

Algorithm 1 Obfuscation Algorithm for TVTF

Input: *n number of capacitors*
Output: *Continuous selection of 1 random capacitor to charge AES, 1 discharged capacitors to be charged*
1: Pre-charge the capacitors.
2: Divide them into 2 distinct arrays.
3: **while** *Encryption is not done* **do**
  3.1:Pick randomly one cap from 'to_be_charged' array and connect it to VDD.
  3.2: Pick randomly one cap from 'to_supply_AES' array and connect it to the AES.
  3.3: After *dt* time, put those 2 capacitors back in alternative arrays.
end

Fig. 4 shows a pictorial representation of the concept. Obfuscated power traces will be available to the attacker. We implement a pseudo-random algorithm to determine the capacitor that is being charged at a time and also the one which drives the AES. This allows physical shuffling of the distributed load capacitors and obfuscates the traces across different time samples. It is important to note that this is different from algorithmic shuffling which has been introduced in multiple works of literature. This work is done at the VDD level with a switched capacitor. Hence this technique is generic and easily applicable to any other crypto-algorithm. Algorithm 1 presents the physical TVTF technique for the randomized shuffling of the capacitors, by choosing only 1 capacitor (out of n total capacitors - $n-phase$ switched capacitor implementation) to drive the AES and another to be charged from the supply at a particular time. Each clock cycle is divided into n different phases and two capacitors are chosen by the algorithm, one for charging and the other drives the AES engine.

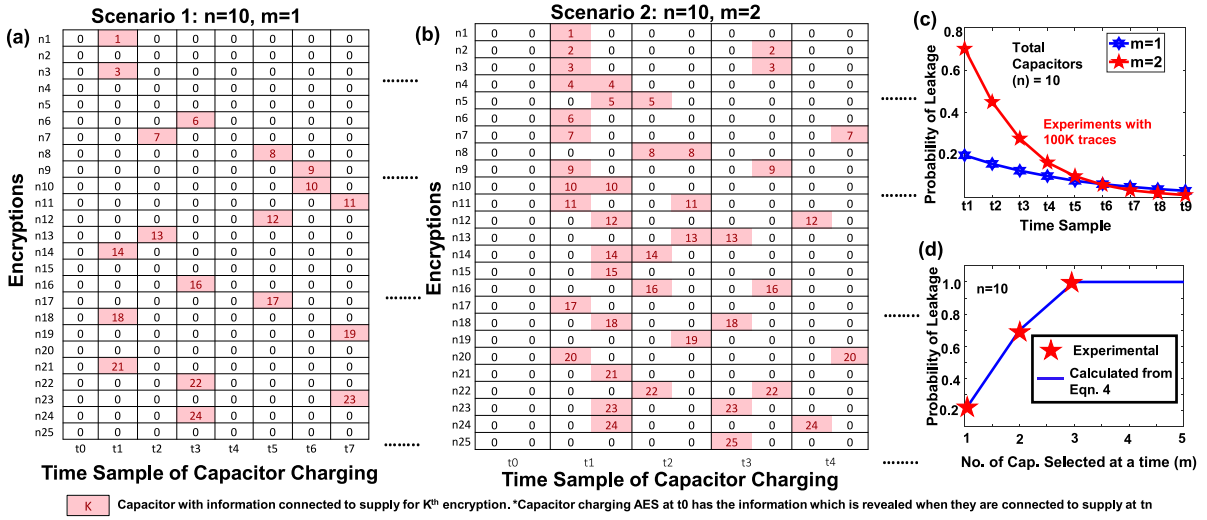

FIGURE 5. (a) An example of 7 time samples of 25 different encryptions when single capacitor (m=1) charges AES at $t0$ time (we assume that information leakage exists at $t0$). Maximum number of occurrences of capacitor with leakage component exists in $t1$ time sample. (b) An example of 4 time samples of 25 encryptions when m = 2. We see higher number of occurrences (thus higher probability of leakage in this case). The experiment is done with 100K traces to get the statistical phenomenon in support of theory explained in the manuscript. (c) With total capacitors (n) = 10 and m=1, maximum leakage probability $P_{leak} = 0.2$ which is $\frac{2}{n}$. While m = 2, leakage probability is much higher (0.7) at maximum leakage point ($t1$). (d) Theoretical and experimental probability of leakage with respect to capacitor selection at a time (m). Both show choosing more number of capacitors leads to more information leakage.

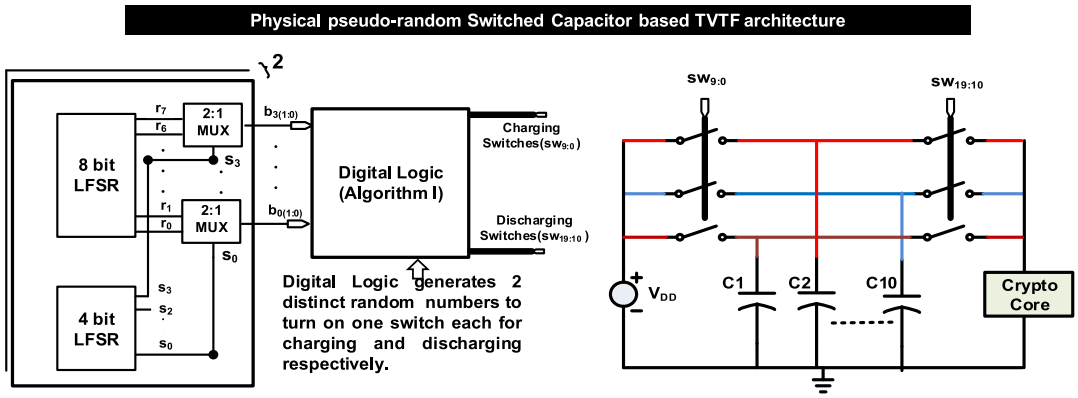

FIGURE 6. Architecture of the multi-phase switched capacitor-based TVTF.

The algorithm is implemented by incorporating linear feedback shift registers (LFSR) as shown in Fig. 6. For the 10-phase TVTF switched capacitor implementation, we utilize 2-level stochastic LFSRs to obtain a high periodicity of $2^8 - 1 = 255$. A 4-bit LFSR is used to stochastically subsample the 8-bit LFSR to produce a 4-bit output. The digital logic of Algorithm I takes two random numbers generated by both the LFSRs and ensures two numbers are different so that a capacitor cannot be connected to the supply and AES at the same time. Hence, AES can never be connected to supply directly. This block also decodes the logic to turn on one switch for both the charging and discharging switches.

This strategy of physical time-varying transfer function-based shuffling obfuscates the signal drastically and reduces the information content as shown in Fig. 4. Once a capacitor has charged AES at leakage point ($t0$) as shown in Fig. 5(a), it is transferred into a different pool of capacitors ('to_be_charged') following the Algorithm 1. From this pool, one of the capacitors can be chosen at $t1$ time with a probability of $\frac{1}{\frac{n}{2}} = \frac{2}{n}$. This probability reduces with time as shown in Fig. 5(c). Fig. 5(a) shows a graphical representation for the same. We take n=10 and m=1 for this example. Assuming $t0$ as the leakage point (for unprotected crypto core), the capacitor charging AES at that point has the leakage component. When this capacitor connects to the supply node for charging (say, at time tn), it will reveal the leakage through the power supply. This leakage component accumulated over a particular time sample (say, tn) would show correlation with the correct key. Even with just 25 encryptions, we see a high probability of occurrence of the capacitor with leakage component at the $t1$ time sample. But, $t3$ has higher leakage component than $t2$ due to randomness in a smaller set however has a monotonic decreasing

trend when we experiment with larger set (Fig. 5(c)). We continue this simulation with 100K encryptions and we observe that probability of leakage (i.e., maximum probability of occurrence of a capacitor with leakage component), P_{leak} converges to $2/n = 0.2$ as shown in Fig. 5(c). **Now, MTD will depend on the pattern of repetition of the shuffled capacitors and thus we employ 2-stage LFSRs (Fig. 6) to leverage a higher level of randomness.** It should be noted that the power consumption of an LFSR is much lower compared to the AES itself. Hence, it is very difficult for an attacker to retrieve the initial seed of the LFSR from the power traces. The seed can be programmed using TRNG to avoid dependency from LFSR [30]. Also, it should be noted that True Random Number Generators (TRNGs) are quite common in modern-day microcontrollers, which can be utilized as a source of randomization to avoid any type of post-processing. These on-chip TRNGs do not have much area overhead and can be enabled when security is extremely necessary even at the cost of energy overhead [31], [32]. In this section, we have discussed the proposed TVTF approach by choosing a single capacitor each for the charging and discharging phases respectively out of the n-capacitor array. In the next section, we will evaluate the effect of choosing multiple capacitors (m) each for the charging and discharging phases.

IV. EVALUATION OF TVTF WITH MULTIPLE SWITCHED CAP APPROACH

This section analyzes the effect of choosing multiple capacitors for charging and discharging at each phase of operation. We assume n is the total number of capacitors and m number of capacitors will be chosen to charge AES and similarly m of them will be connected to the supply node (VDD) at a time. All of the capacitors that charge AES at $t0$ contain the leakage component. As most of them are connected to the supply node in the immediate time sample $t1$ (as shown in Fig. 5(b, c)), they will have the maximum information/leakage. It is important to note that though each capacitor will have leakage components, the leakage will be partly suppressed due to the inherent attenuation from the capacitors. However, for this calculation, we only analyze the benefit of capacitor shuffling. As m number of capacitors are connected to AES at $t0$ leakage point, the probability of leakage = probability of maximum occurrence of such a capacitor at a point (which we observe is $t1$)

$$
\begin{aligned}
&= P_{leak} = P(C_{\text{leak }1} \cup C_{\text{leak }2} \cup \ldots \cup C_{\text{leak }m}) \\
&= P(C_{\text{leak }1}) + P(C_{\text{leak }2}) + \ldots + P(C_{\text{leak }m}) \\
&\quad - P(C_{\text{leak }1} \cap C_{\text{leak }2}) - P(C_{\text{leak }1} \cap C_{\text{leak }3}) \ldots \\
&\quad + P(C_{\text{leak }1} \cap C_{\text{leak }2} \cap C_{\text{leak }3}) \ldots \\
&= mP\big(C_{\text{leak }1)}\big) - {}^{m}C_2 P(C_{\text{leak }1} \cap C_{\text{leak }2}) \\
&\quad + {}^{m}C_3 P(C_{\text{leak }1} \cap C_{\text{leak }2} \cap C_{\text{leak }3}) - \ldots\ldots
\end{aligned}
$$

[All capacitor selection is uniformly random]

$$
\begin{aligned}
&= mP\big(C_{\text{leak }1)}\big) - {}^{m}C_2 P(C_{\text{leak }2}) P(C_{\text{leak }1} | C_{\text{leak }2}) \\
&\quad + {}^{m}C_3 P(C_{\text{leak }3}) P(C_{\text{leak }1} \cap C_{\text{leak }2} | C_{\text{leak }3}) - \ldots\ldots
\end{aligned}
$$

[Following Bayes' Therem]

$$
\begin{aligned}
&= m \cdot \frac{2m}{n} - {}^{m}C_2 \cdot \frac{2m}{n} \cdot {}^{m-1}C_1 \cdot \frac{1}{\frac{n}{2} - 1} \\
&\quad + {}^{m}C_3 \cdot \frac{2m}{n} \cdot {}^{m-1}C_2 \cdot \frac{1}{{}^{\frac{n}{2}-1}C_2} \cdots \\
&= \sum_{i=1}^{m} (-1)^{i+1} \frac{{}^{m}C_i}{{}^{n-1}C_{i-1}} \cdot {}^{m-1}C_{i-1} \cdot \frac{2m}{n} \cdots
\end{aligned} \tag{4}
$$

A simple example of n=10 and m=2 is demonstrated in Fig. 5 (b). Here, 2 capacitors are used to charge AES at $t0$ which is the information leakage point for unprotected. The probability of occurrences of any capacitor with leakage component at t1 (P_{leak}) is high, which we calculate as 0.7 using the Eqn. (4). We experiment with 100K traces and see the probability of leakage converge to 0.7 (Fig. 5(d)), which validates our theory. It should be noted that increasing n will produce more obfuscation leading to an increase in MTD. Eqn. (4) is plotted in Fig. 5(d). We conclude from Fig. 5(d) that for $m > 1$ probability of information leakage is more. Hence, with an n-phase switched capacitor array, choosing a single capacitor is the best possible TVTF strategy for physical time-domain obfuscation, as it reduces the information leakage by the maximum amount. In general, as shown by theory and experiment selecting m capacitors at a time increases leakage probability under the assumption that the security is achieved solely by the time domain obfuscation and not due to the attenuation provided by the capacitors. Hence, $m = 1$ is chosen for the proposed TVTF countermeasure.

V. RESULTS: DESIGN SPACE EXPLORATION

Power traces for simulation have been collected from an 8-bit Atmel microcontroller running AES-128 encryption, using the Chipwhisperer platform for design space exploration. The clock frequency of the software AES is 125MHz and has a peak current of $3mA$ (average current $\sim 1mA$). A CPA attack performed on this unprotected AES-128 showed an MTD of ~ 20 traces.

A. CHOICE OF SWITCH ON RESISTANCE & UNIT CAPACITANCE

As discussed earlier, to minimize the area overhead, a total capacitance of 200pF is chosen. Now we need to determine the optimal value of the unit capacitors such that there is no performance degradation of the crypto engine. Fig. 7(a) shows the effect of the switch ON resistance (R) and the choice of the unit capacitor (C) on the voltage droop across the AES core. Tolerating a maximum voltage drop of 0.1V,a minimum unit capacitance of 20pF can be supported with $R = 10\Omega$. This also implies that the maximum limit to our number of phases/capacitors (n) becomes 10.

B. EFFECT OF INCREASING THE NUMBER OF PHASES

Figure 7(b) shows that increasing the number of unit capacitors, and hence the phases of operation in a clock cycle

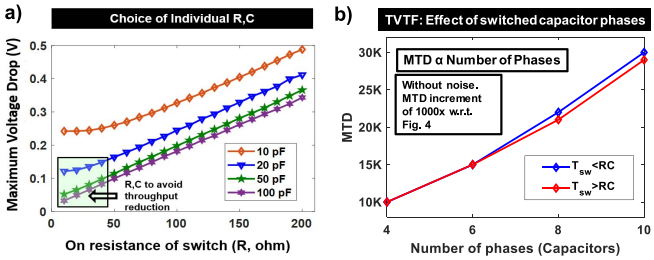

FIGURE 7. a) The choice of the switch ON resistance (R) and the unit capacitance (C) is shown. For our TVTF-based switched capacitor circuit implementation, switch resistance (R) is chosen as 10Ω and individual unit capacitors are chosen to be 20pF to avoid any performance degradation (voltage droop < 100*mV*). b) MTD increases as the number of phases (unit capacitors) is increased. The memory effect for $T_{sw} < RC$ is quite small and does not justify the associated power overhead trade-off. Hence, the proposed TVTF circuit operates in the region of $T_{sw} > RC$.

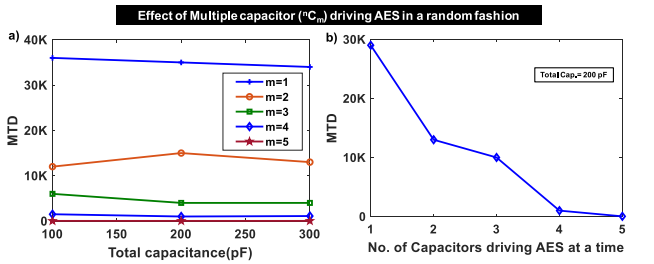

FIGURE 8. a) Effect of the choice of number of capacitors (m) at a time from a pool of 10 capacitors (n = 10) on MTD. Increasing m does not enhance MTD as the probability of information leakage increases. b) Effect of multiple capacitors for a fixed total cap (200pF) shows that the MTD is maximum when a single capacitor (m=1) is chosen by the TVTF algorithm, each for the charging and discharging. The decreasing trend with respect to *m* supports the mathematical justification in Section IV that choosing single capacitor is a better randomization technique than choosing multiple capacitors.

increase the MTD significantly. Also, Figure 7(b) shows that the effect of memory due to the previous time cycles ($T_{sw} < RC$) has a negligible effect on MTD. More phases (or capacitors) lead to a higher MTD. But, increasing the number of phases has a trade-off with power consumption (due to higher switching frequencies) and performance (due to larger voltage drop). Hence we choose 10 as the number of optimal phases.

C. EFFECT OF CHOOSING MULTIPLE CAPACITORS WITH TVTF

As discussed in Section IV, the next set of results is obtained by choosing multiple capacitors from an array of 10 capacitors. MTD reduces with the increase of the number of capacitors(m) chosen at a time. This finding is counter-intuitive, which is consistent with our analysis in Section IV. We see that for $n = 10, m = 1$ gives the maximum MTD, as seen from Fig. 8. As any of m capacitors will have the leakage component (distributed equally among all the capacitors), information will be leaked when m>1 more causing significant MTD reduction as shown in Fig. 8(b). $m > 3$ will surely have leakage component at $t1$ as shown in Fig. 5(d). $m = 3$ or $m = 4$ has some selection of non-leaky capacitor as well unlike $m = 5$. Hence, MTD is much lower for $m = 5$.

TABLE 3. MTD improvement by tuning periodicity of PRNG (number of capacitors and total capacitance are fixed).

Periodicity	MTD
$2^3 - 1$	700
$2^{16} - 1$	66000
$2^{32} - 1$	92000

Finally, Fig. 9(a) shows the MTD plots with respect to the number of traces analyzed for the proposed solution. For the TVTF based switched capacitor with 10 evenly distributed capacitors (n = 10, m = 1), we achieve an MTD of $\sim 30K$ traces (Fig. 9(a)).

D. EFFECT OF PERIODICITY OF PRNG

PRNG is the backbone of TVTF architecture. It has been observed with the increase in periodicity, MTD has increased significantly. This observation is tabulated in Table 3. Note that, change in periodicity inversely affects the probability of getting the same trace at the same time point, which increases MTD. Next, we study the effects of uneven distribution of unit capacitors to achieve higher levels of randomization.

E. EFFECT OF UNEQUAL CAPACITORS

Further randomization can be achieved with unequal capacitance values while maintaining a fixed total capacitance of 200pF. With this, MTD can be further enhanced (Fig. 9(b, c)). This is because according to equation 2 as the voltage residue value depends on individual capacitance. Hence the presence of different capacitors further distorts the signal and increases protection by $\sim 3\times$ and increases the MTD to ~96K traces ($\sim 5000\times$) with iso-area overhead. Voltage sample at n^{th} time sample will be obfuscated according to the proposed algorithm and will be available at different time samples for a different cycle as shown in Fig. 10 according to the Algorithm 1. From equation (2), we see capacitance value can further distort voltage trace as it is the co-efficient of the current integration term. Hence, introducing different capacitance values leads to MTD increment. To analyze the standalone effect of the spread vector due to uneven capacitance value, we take a sample signal. We scale the signal according to the effect of the vector due to the spread of the capacitance value and correlate it with our initial signal. We observe the change in correlation coefficient as shown in Fig. 9(b). Note that 20% in capacitance value spread gives a significant improvement in MTD (~5000x as shown in Fig. 9c). We can leverage this constraint to reduce the correlation value even more which will increase the MTD number significantly. Increasing the spread of the capacitance value reduces the minimum capacitance value increasing maximum droop. It can adversely affect the efficiency of the circuit. To be on the safer side, average capacitance has to be increased thereby increasing the area overhead.

F. TEST VECTOR LEAKAGE ASSESSMENT

Surely, attacking using CPA is an indication but does not completely declare extra security. Different types of power

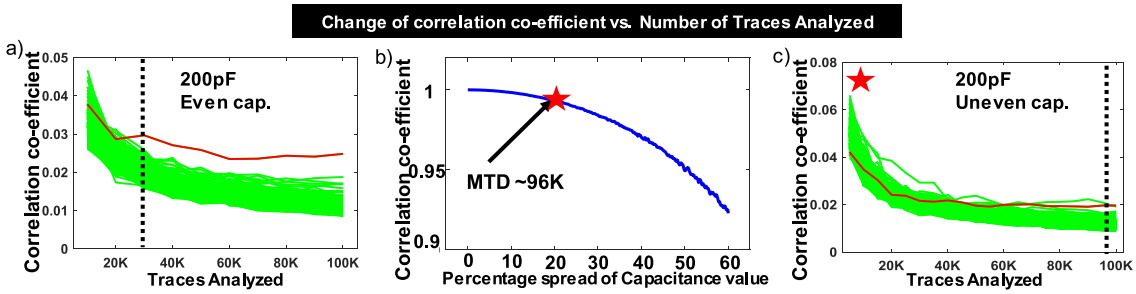

FIGURE 9. a) MTD plot for the TVTF-based switched capacitor technique shows an MTD ~ 30*K* (1500× improvement) with equally distributed unit capacitors (20pF each) across 10 phases. b) Correlation coefficient reduced with different capacitance values. The increase in percentage spread in capacitance provides a reduction in the correlation coefficient. c) With unequal capacitance ranging from 16pF-24pF with a total capacitance of 200pF produces protection up to MTD ~ 96*K* traces.

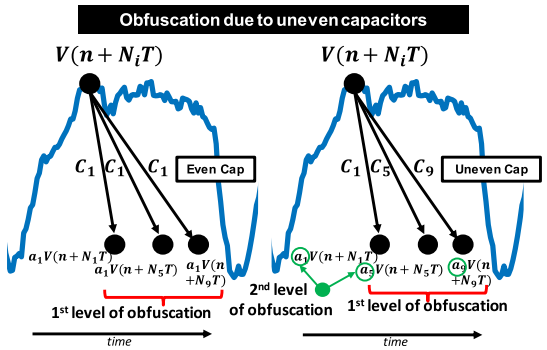

FIGURE 10. Effect of unequal unit capacitors: As the voltage residue depends on the capacitance value of each capacitor (equation (2)), introducing unevenness in capacitance adds an extra level of randomization.

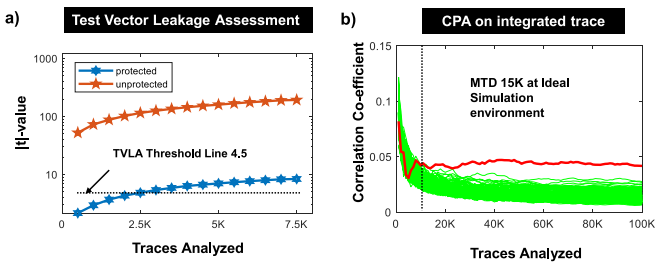

FIGURE 11. a) Test vector leakage assessment of TVTF-AES implementation using system-level simulation. b) Correlational power attack on integrated trace shows an improvement over the conventional CPA attack. In the ideal simulation set-up, MTD is 15K for the protected implementation.

analysis attacks have been introduced and research is going on for further improvement on attack models and algorithms. Hence, it is important to calculate the amount of meaningful leakage by an encryption engine. We use the TVLA score for such analysis. AES with TVTF crosses the threshold of 4.5 after 2.5K traces while unprotected has a much higher value (11.5) even with a few traces. We observe a maximum $t-value$ of 8.37 in the protected AES version against 190.1 of the unprotected version after 7.5K traces. The trend has been shown in Fig. 11(a). However, it should be noted that TVLA scores should not be compared as a security metric rather it can be used as order of security [33]. This is valid for our measurement as well. TVLA result is explored for the software serial implementation. Unprotected has a distinctive mean for fixed traces from random traces. This implies TVLA score is excessively high for unprotected and the correct key can be retrieved. We can retrieve the correct key with just 20 traces. For the protected implementation, we utilize TVLA for security evaluation of the proposed TVTF countermeasure during the design space exploration phase in simulation (Fig. 11(a) in the revised article). We observe that TVLA score is much lower and it only crosses the threshold of 4.5 after 2.5K traces. It should be noted that due to algorithmic noise, a parallel hardware architecture will perform much better in terms of side-channel security. Considering this intuition, initial TVLA results provide us the confidence to explore the design methodology further with the TVTF hardware design. In brief, we use TVLA results to evaluate if it is relatively secure and further explore the design space instead of a direct comparison.

G. IMMUNITY AGAINST CORRELATIONAL POWER ANALYSIS ON SLIDING WINDOW-BASED INTEGRATED TRACE

To do a complete security analysis, we explore different ways of post-processing techniques for attack which can be used in addition to standard CPA. Using integrated traces is one of them. As we are shuffling in time domain, leakage is still present. It is harder for attacker to retrieve the correct key as leakage points are not aligned. Hence, it is intuitive to sum up/integrate over a larger time to exploit the leakage point. We call this time frame as window and utilize the concept of sliding window-based attack here to evaluate if our design can be exploited in a lower number of traces [34]. However, it is observed that the correct key is not retrieved with 15K number of traces primarily due to the presence of very few leakage points that are obfuscated in time. Hence, when we integrate it, noise gets amplified causing SNR to be low as shown in Fig. 11(b). Traditional CPA assumes a single leakage point and expects it to be correlated with the attack model. Crypto algorithms (especially in software implementations) might have multiple leakage points which are usually located near each other [34]. To test the immunity of our countermeasure, traces are integrated with a sliding window and it was attacked using CPA. The proposed countermeasure has an MTD of 15K in the ideal simulation as

TABLE 4. Overhead comparison of time-varying transfer function (TVTF) with the existing state-of-the-art countermeasures.

Parameters	This Work	TCAS-I'18 [23]	JSSC '06 [14]	ISSCC '09 [8]	ISSCC '17 [26]	ISSCC '19 [24]
Technology	65nm	130nm	180nm	130nm	130nm	130nm
Technique used	TVTF	ASNI	WDDL	Sw. Capacitor	IVR	Digital LDO
Power	1.24x	1.68x	4x	2.66x	2x	1.35x
Area	1.2x	1.6x	3x	1.25x	2x	1.38x[1]
Performance Degradation	0	0	4x	2x	0	1.1x
MTD	∼5000x(>1M)	1000x	30x	2500x	100x	4210x
Comments	Digital-friendly	Mixed-signal	Mixed-signal	Mixed-signal	Mixed-signal	Digital-friendly

[1]Large metal-insulator-metal (MIM) load capacitor (1.9nF) not considered in the area overheads.

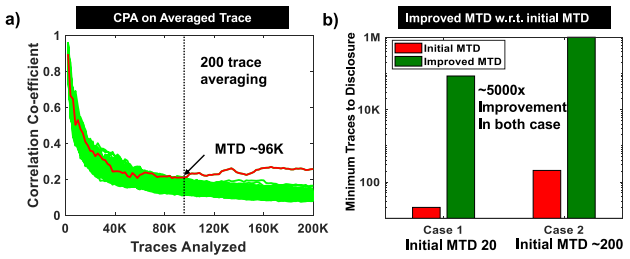

FIGURE 12. a) Correlational power attack on the averaged traces. 480 averaged traces are required to break the countermeasure with an average of 200. b) Effect of initial MTD on the SCA resilience: case 1) Initial MTD ∼ 20 and Improved MTD ∼ 96K. case 2) Initial MTD ∼ 210 and Improved MTD >1M.

shown in Fig. 11(b). One important point to note is this attack algorithm can only work better if multiple correlation points are nearby. This attack technique will not necessarily be better in other types of implementation where only one correlation point exists.

H. IMMUNITY AGAINST AVERAGED TRACE-BASED CPA

Averaging multiple traces for the same plaintext/keys would cause a reduction of noise. It is a common technique [33], [35] to reduce measurement noise and can provide a cleaner power trace for the attack. The same intuition is used here. Reference [33] has shown an improvement in terms of leakage analysis too. MTD should be verified even with averaged traces to gain confidence in the countermeasure. The proposed TVTF has been tested against 200× averaged traces. Fig. 12(a) shows an MTD of 96K with averaged trace which implies our countermeasure works well against CPA on averaged traces too.

I. AREA AND POWER OVERHEAD

Power overhead depends on 3 components.

1. Power lost while charging the capacitors and have been given by, $P_l = 0.5 \times f_{switching} \times unit\_capacitance \times (\delta V)^2 = 0.125\ mW$, where δV is the maximum voltage drop.

2. Another component is the switching power, $P_{switching} = f_{switching} \times C_{gate\_cap} \times V_{DD}^2 = 50\ uW$, where C_{gate_cap} is the gate capacitance of switch.

3. Pseudo-random number generator (PRNG) is another cause of power overhead. For a 10-bit LFSR, the power overhead is given by $P_{PRNG} = P_{LFSR} \times 2 + P_{logic} = 150\mu W$. Final power overhead, $P_{ov} = P_l + P_{PRNG} + P_{switching} = 325\mu W$. PRNG power is calculated from the synthesis report using the design compiler after mapping the design to 65nm TSMC CMOS technology. The power overhead can be given as, $\frac{P_{AES}+P_{ov}}{P_{AES}} = \frac{0.325+1.32}{1.32} = 1.24\times$.

Similarly, the area overhead will have 3 components - area due to capacitors (A_{cap}), area of PRNG (A_{PRNG}) and area of the PMOS switch (A_{sw}). Hence, area overhead is given as, $A_{ov} = A_{cap} + A_{PRNG} + A_{sw} = 0.03\ mm^2$. Area of AES in 65nm TSMC CMOS technology is $\sim 0.15\ mm^2$. Hence, the relative area overhead $= \frac{A_{ov}+A_{AES}}{A_{AES}} = \frac{0.15+0.03}{0.15} = 1.2\times$.

J. REMARKS

Table 4 compares this work with existing solutions. WDDL [14] suffers from high overheads and performance degradation. Switch capacitor current equalizer circuit by Tokunaga and Blaauw [8] also suffers from performance degradation and is a mixed-signal circuit. IVR [26] based countermeasure does not increase MTD to a large number. On a different note, Digital LDO-based countermeasure [24] has a higher area overhead with capacitors. The proposed countermeasure has an area overhead of 4% without the capacitors.

Power overhead linearly increases with higher switching frequency. At a switching frequency of 1.25GHz, the power consumption becomes $325\mu W$. Again from Fig. 10, it is evident that the increasing number of phases per clock cycle of AES increases MTD, hence providing more immunity. Clearly, we can infer from these two trends that the number of phases can be used as a tuning knob to optimize between MTD and power efficiency.

Fig. 12(b) shows that protected MTD increases with improved initial MTD. It is observed that MTD reaches >1M where initial MTD is 210 and unprotected trace is collected from hardware AES implemented on an Artix FPGA. This observation leads to the conclusion that being a physical circuit-level countermeasure, TVTF can be used as a wrapper both for hardware as well as software implementations of AES. The primary reason for choosing the software AES was to deal with low initial MTD values which help in the faster analysis of the proposed countermeasure. This method is completely generic and can be used on top of any encryption engine, unlike algorithmic shuffling. We further evaluate the countermeasure in a custom ASIC.

Note that this paper mainly focuses on power side-channel attacks. Though EM side channel attack is also a threat to consider, it is beyond the scope of this work. But, this

solution can be extended to EM Side channel attacks too. Analysis has been shown in [36] that low-level metal layers radiate a very less amount of leakage from the IC. Hence capacitors shuffling logic as well as AES charging logic can be implemented using a low-level metal layer before it routes to highly radiating metal layers for charging supply capacitors. EM probe will detect shuffled traces in this solution which is already immune to side-channel attacks.

VI. TUNING KNOB TO ENHANCE THE RESISTANCE OF THE PROPOSED COUNTERMEASURE

This section summarizes the key factors that allow increasing the immunity of the proposed countermeasure even more at the cost of area or power overhead.

- *Number of Phases:* Number of phases is one of the most important parameters to increase MTD. The number of phases implies an increase in randomization within a given time window. Hence, the probability of getting the same traces at a particular point reduces further which helps to increase MTD. Fig. 7(b) shows the trend. Note that increasing the number of phases requires a higher switching frequency producing higher power overhead.
- *Effect of uneven capacitors:* Residue trace depends on the capacitance value of capacitors as discussed previously. Changing the capacitance of each capacitor and making it slightly uneven for each other further distorts the trace thus reducing the information.
- *Periodicity of PRNG:* Periodicity of PRNG implies repetitive patterns in capacitor connection to VDD and AES. Hence increment in periodicity increases random shuffling and helps in MTD increment.

VII. MEASUREMENTS FROM 65NM CMOS IC

To further evaluate the concept, we have taped out a 65nm TSMC CMOS IC with the TVTF concept. Though the countermeasure technique is generic and can be extended to any of the encryption engines, we chose AES-256 as the test encryption engine. Parallel AES-256 is implemented which calculates a complete encryption in 14 cycles [30]. TVTF is used as a countermeasure. The detailed IC implementation and evaluation have been already presented in the authors' previous work [30], [37] and beyond the scope of this paper. However, [30] presents a proof-of-concept of the theory discussed here and presents a practical implementation. Interested readers are requested to read [30].

IC micrograph is presented in Fig. 13(a). Unprotected and TVTF circuits are shown in the micrograph. AES is operated at 0.8V and 10MHz frequency when it consumes 151uW power. We use the HD attack model because of hardware implementation and chose hamming distance between the 13^{th} and 14^{th} cycle for the attack as shown in Fig. 13(b). Note that, each cycle of operation is clearly visible from unprotected traces. However, cycles for operation are not clearly visible for TVTF as shown in Fig. 13(c). We perform correlational power attacks (CPA) on both unprotected and protected implementation. The unprotected correct key byte

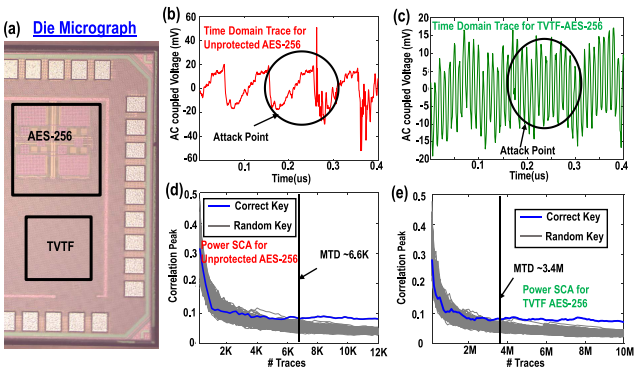

FIGURE 13. (a) Die Micrograph of 65nm CMOS IC. The IC has parallel AES-256 implementation both unprotected and protected using TVTF [30]. (b) Last 4 cycles of time-domain power trace of unprotected implementation. (c) Power trace of TVTF-AES256 for the same region as (b). (d) CPA on unprotected reveals the correct key within 6.6K traces. (e) CPA on TVTF AES256 reveals the correct key in 3.4M traces which is 500× better than unprotected implementation.

is revealed within 6.6K traces. However, the correct key is not revealed until 3.4M traces for TVTF AES-256 which is 500× greater than unprotected implementation.

Future improvement for IC Implementation: The IC implementation serves as proof of the concept presented here. Interestingly, it achieves 500× improvement which is 10× less as expected by theory. Note that, this switch cap-based solution needs switches that have been implemented using transmission gates (TG). To make sure, it can provide the perfect amount of current with a very small time constant, the W/L ratio has been increased leading to an increase in leakage current. Due to static leakage, the correct key comes out quicker than expected. A theoretical evaluation of static leakage-based attack is presented in [38]. In our future work, different types of low-leakage switches will be explored to fit into this solution.

VIII. CONCLUSION

A power side-channel attack is a prominent attack on encryption ICs. This works proposes TVTF: a physical Time-Varying Transfer Function countermeasure to significantly obfuscate the power traces in the time domain utilizing multi-phase switched capacitors. Previously, shuffling-based architectural countermeasures have been proposed that randomize the order of instructions, but there are a limited number of instructions that can be shuffled and are specific to a particular algorithm and architecture. DVFS-based countermeasures based on clock randomization were shown to be broken previously by observing the clock edges at the power supply since it preserves the order of the instructions. This paper demonstrates the efficacy of TVTF against SCA attacks as well as with TVLA. TVTF performs efficient randomization of the switched capacitors to obfuscate the traces. Commercial micro-controllers have in-built TRNGs which can be used as seed generator/randomization units to further enhance security in actual production.

Overall, the proposed TVTF-based switched capacitor countermeasure provides a generic, low-overhead (1.2× area,

1.25× power overhead), and digital solution. The capacitors can be synthesized using DCAP cells available in digital libraries, the rest of the countermeasure is completely digital which makes it scalable across different technologies. Finally, it achieves a power SCA protection of ∼5000× (∼500× in measurement) compared to the unprotected implementation without any performance degradation. As a future work, low leakage switches will be used to improve the performance of SCA resilience in measurement.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. CRYPTO*, Aug. 1999, pp. 388–397.

[2] E. Brier, C. Clavier, and F. Olivier, "Optimal statistical power analysis," in *Proc. IACR Cryptol*, 2003, p. 152.

[3] J.-J. Quisquater and D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards," in *Proc. Smart Card Program. Secur.*, 2001, pp. 200–210.

[4] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Proc. CHES*, May 2001, pp. 251–261.

[5] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems," in *Proc. CRYPTO*, Aug. 1996, pp. 104–113.

[6] D. Brumley and D. Boneh, "Remote timing attacks are practical," in *Proc. USENIX Securi. Symp. (SSYM)*, Berkeley, CA, USA, 2003, p. 1.

[7] C. O'Flynn and Z. Chen, "ChipWhisperer: An open-source platform for hardware embedded security research," in *Proc. COSADE*, 2014, pp. 243–260.

[8] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *Proc. ISSCC*, Feb. 2009, pp. 64–65.

[9] D. Basu Roy, S. Bhasin, S. Patranabis, D. Mukhopadhyay, and S. Guilley, "What lies ahead: Extending TVLA testing methodology towards success rate," in *Proc. IACR Cryptol.*, 2016, p. 1152.

[10] 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.

[11] A. Shamir, "Protecting smart cards from passive power analysis with detached power supplies," in *Proc. CHES*, 2000, pp. 7–17.

[12] J.-L. Danger, S. Guilley, S. Bhasin, and M. Nassar, "Overview of dual rail with precharge logic styles to thwart implementation-level attacks on hardware cryptoprocessors," in *Proc. 3rd ICSCS*, Nov. 2009, pp. 1–8.

[13] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. ESSIRC*, Sep. 2002, pp. 403–406.

[14] D. D. Hwang et al., "AES-based security coprocessor IC in 0.18-μm CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.

[15] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. DATE*, vol. 1, 2004, pp. 246–251.

[16] S. Lu, Z. Zhang, and M. C. Papaefthymiou, "1.32GHz high-throughput charge-recovery AES core with resistance to DPA attacks," in *Proc. VLSI*, Jun. 2015, p. 246.

[17] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in *Proc. CHES 2005*, pp. 172–186.

[18] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style MDPL on a prototype chip," in *Proc. CHES*, Sep. 2007, pp. 81–94.

[19] H. Thapliyal, T. S. S. Varun, and S. D. Kumar, "Adiabatic computing based low-power and DPA-resistant lightweight cryptography for IoT devices," in *Proc. ISVLSI*, 2017, pp. 621–626.

[20] N. Veyrat-Charvillon, M. Medwed, S. Kerckhof, and F.-X. Standaert, "Shuffling against side-channel attacks: A comprehensive study with cautionary note," in *Proc. ASIACRYPT*, 2012, pp. 740–757.

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

[22] T. Güneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *Proc. CHES*, Sep. 2011, pp. 33–48.

[23] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 10, pp. 3300–3311, Oct. 2018.

[24] 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 *Proc. ISSCC*, Feb. 2019.

[25] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," in *Proc. HOST*, May 2017, pp. 62–67.

[26] M. Kar et al., "8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," in *Proc. ISSCC*, 2017, pp. 142–143.

[27] G. B. Ratanpal, R. D. Williams, and T. N. Blalock, "An on-chip signal suppression countermeasure to power analysis attacks," *IEEE Trans. Depend. Secure Comput.*, vol. 1, no. 3, pp. 179–189, Jul.-Sep. 2004.

[28] F. Zhang, B. Yang, B. Yang, Y. Zhang, S. Bhasin, and K. Ren, "Fluctuating power logic: SCA protection by *v_{DD}* randomization at the cell-level," in *Proc. AsianHOST*, 2019, pp. 1–6.

[29] A. Moradi and F.-X. Standaert, "Moments-correlating dpa," in *Proc. ACM Workshop Theory Implement. Secur.*, 2016, pp. 5–15.

[30] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "SynSTELLAR: An EM/power SCA-resilient AES-256 with synthesis-friendly signature attenuation," *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, Jan. 2022.

[31] Q. Tang, B. Kim, Y. Lao, K. K. Parhi, and C. H. Kim, "True random number generator circuits based on single- and multi-phase beat frequency detection," in *Proc. IEEE Custom Integr. Circuits Conf.*, 2014, pp. 1–4.

[32] K. Yang, D. Blaauw, and D. Sylvester, "An all-digital edge racing true random number generator robust against PVT variations," *IEEE J. Solid-State Circuits*, vol. 51, no. 4, pp. 1022–1031, Apr. 2016.

[33] F.-X. Standaert, "How (not) to use Welch's t-test in side-channel security evaluations," in *Proc. CARDIS*, Montpellier, France, 2018, pp. 65–79.

[34] D. Fledel and A. Wool, "Sliding-window correlation attacks against encryption devices with an unstable clock," in *Proc. IACR Cryptol*, 2018, pp. 193–215.

[35] A. Ghosh, D.-H. Seo, D. Das, S. Ghosh, and S. Sen, "A digital cascoded signature attenuation countermeasure with intelligent malicious voltage drop attack detector for EM/power SCA resilient parallel AES-256," in *Proc. CICC*, 2022, pp. 1–2.

[36] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis," in *Proc. HOST*, 2019, pp. 11–20.

[37] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "36.2 an EM/power SCA-resilient AES-256 with synthesizable signature attenuation using digital-friendly current source and RO-bleed-based integrated local feedback and global switched-mode control," in *Proc. ISSCC*, 2021, pp. 499–501.

[38] T. Moos, A. Moradi, and B. Richter, "Static power side-channel analysis—An investigation of measurement factors," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 2, pp. 376–389, Feb. 2020.