Syn-STELLAR: An EM/Power SCA-Resilient AES-256 With Synthesis-Friendly Signature Attenuation

Archisman Ghosh, Debayan Das, *Student Member, IEEE*, Josef Danial, *Student Member, IEEE*, Vivek De, *Fellow, IEEE*, Santosh Ghosh, and Shreyas Sen, *Senior Member, IEEE*

***Abstract*— Mathematically secure cryptographic algorithms leak meaningful side-channel information in the form of correlated power and electromagnetic (EM) signals, leading to physical side-channel analysis (SCA) attacks. Circuit-level countermeasures against power/EM SCA include a current equalizer, IVR, non-linear LDOs, enhancing protection up to 10M traces, and current-domain signature attenuation (CDSA), and randomized NL-LDO cascaded with arithmetic countermeasures achieved protection up to >1B. This work embraces the concept of analog CDSA but makes it easily scalable over technology nodes with digital-friendly current sources, digital control loop, and digital bleed path to increase the MTD from 10M to 250M (25× improvement, using a single digital countermeasure). Ring oscillator (RO) used as the bleed path to bypass encryption-dependent leakage acts as local negative feedback (LNFB). Besides, based on RO oscillation frequency, AES node voltage can be tuned at startup, PVT, or frequency variation. Thus, RO acts as integrated LNFB and global feedback for the digital signature attenuation circuit (DSAC). Another circuit technique, namely, the time-varying transfer function (TVTF), removes the requirement of dc bias in the current-domain equalizer (best switch capacitor-based countermeasure till date) to make it digital and utilizes switch cap-based circuit for time-domain obfuscation to achieve enhanced security. This work, namely, Syn-STELLAR: SYNthesis-friendly Signature aTtenuation Embedded crypto with Low-Level metAl Routing, combines both DSAC and TVTF techniques to achieve an MTD > 1.25B for both EM and power SCA, which is 25% higher than the existing state of the art. The 65-nm CMOS test chip contains unprotected and both the protected (DSAC and DSAC-TVTF) parallel AES-256 implementation. This implementation is the first synthesis-friendly countermeasure, which converges two analog-type strong protections (signature attenuation and switched cap current equalizer) in a digital-friendly solution and achieves >1.25B MTD with power and area overheads comparable to previous circuit-level countermeasures.**

***Index Terms*— AES-256, correlational power analysis, electromagnetic (EM) leakage, generic countermeasure, hardware security, side-channel attacks, synthesizable signature attenuation, test vector leakage analysis (TVLA).**

Manuscript received May 21, 2021; revised August 6, 2021; accepted September 5, 2021. Date of publication October 1, 2021; date of current version December 29, 2021. This article was approved by Associate Editor Shidhartha Das. This work was supported in part by the National Science Foundation (NSF) under Grant CNS 17-19235 and Grant CNS 19-35573, and in part by Intel Corporation. *(Corresponding author: Archisman Ghosh.)*

Archisman Ghosh, Debayan Das, Josef Danial, and Shreyas Sen are with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA (e-mail: ghosh69@purdue.edu; shreyas@purdue.edu).

Vivek De and Santosh Ghosh are with Intel Labs, Hillsboro, OR 97124 USA.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JSSC.2021.3113335.

Digital Object Identifier 10.1109/JSSC.2021.3113335

I. Introduction

MATHEMATICALLY secure cryptographic algorithms leak critical side-channel information in the form of correlated power [1], electromagnetic (EM) [2], timing [3], cache hits/misses, and so on, leading to physical SCA attacks. Due to such SCA information leakage, mathematical complexity for successful attacks can be greatly reduced. For example, the time complexity of breaking the AES-256 encryption engine has been reduced to 2^{13} from 2^{256}. Power/EM side-channel attacks can be broadly classified into two categories: 1) non-profiled attack [1], [4] and 2) profiled attack [5], [6]. The profiled attack has two phases, namely, training and attack phases, and requires a prior experiment with the device in the training phase. Correlational power/EM side-channel attacks belong to the first category, and these are direct attacks on a single device running hardware/software crypto-algorithms. This work mainly deals with non-profiled power and EM side-channel attacks on the AES-256 encryption engine.

Recently, it is observed that the AES-256 key can be easily sniffed from a distance using a cheap EM probe from even a meter distance without knowing detailed circuit/PCB implementation [7]. Hence, EM side-channel attack is a significant threat to integrated circuits.

For power/EM side-channel attacks, the attacker needs to collect traces from the target device using an oscilloscope. Corresponding output ciphertexts are publicly available for each trace. These attacks work on small portions of the secret key, such as 1 byte at a time. For each key byte, a Hamming Distance (HD) model is built for all key guesses. HD values are then correlated with the collected traces. It is observed that, after multiple traces are analyzed, the correct key byte can be recovered through the correlational analysis.

Along with the advancements in SCA attacks, the side-channel countermeasure community has progressed a lot as well. From architectural and gate-level countermeasures, generic physical countermeasures have been introduced. Circuit-level countermeasures include current equalizer [8], [9], series LDO [10], IVR [11], and so on. These circuit-level countermeasures have enhanced the protection up to 10M minimum traces to disclosure (MTD). Recently,

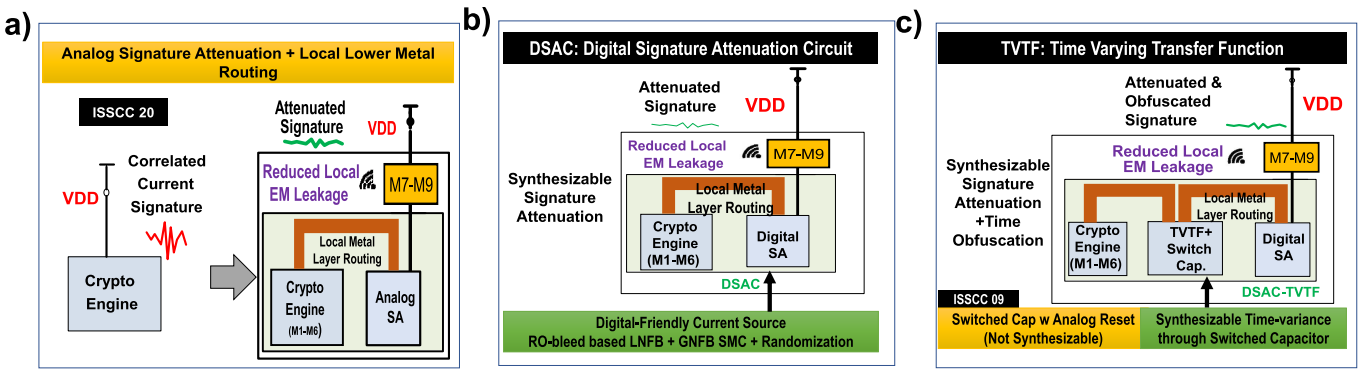


Fig. 1. Overview of the countermeasure techniques. (a) Analog signature attenuation. (b) DSAC: digital-friendly signature attenuation technique for side-channel security. (c) Switched cap-based TVTF used before signature attenuation for extra security.

current-domain signature attenuation (CDSA) technique is introduced in [12], [13]. This technique, for the first time, achieves >1B MTD. This is the only solution to date, which achieves >1B MTD with a single strategy. A progression of DSAC-TVTF design is presented in Fig. 1. Another solution [14], [15], which is a cascade of two solutions, namely, randomized digital LDO and arithmetic countermeasures, recently achieved similar security as well.

The fabricated 65-nm CMOS IC contains three configurations: 1) unprotected AES-256; 2) DSAC-AES-256; and 3) DSAC-TVTF-AES-256. It is observed that the unprotected implementation could be broken with just 7k traces using a correlational power attack (CPA). Also, 9k traces are required to break an unprotected AES-256 implementation using correlational EM Attack (CEMA). However, the DSAC-AES-256 key can be retrieved in 348M traces in CPA and 250M traces in CEMA. This is 25× better than the latest state of the art for a single digital countermeasure [10], [14]. TVTF is initiated to improve security. In the presence of both the countermeasures together, an MTD of 1.25B is achieved, which is the highest to date for an SCA-resilient AES-256 crypto-core.

The remainder of this article is organized as follows. Section II describes the existing works on power and EM side-channel attack countermeasures. A detailed conceptual discussion of digital signature attenuation circuit (DSAC) along with circuit architecture is presented in Section III. Section IV outlines the concept and implementation details of the time-varying transfer function (TVTF). The full system architecture is presented in Section V. Section VI describes the efficacy of the countermeasure against CPA, CEMA along with the test vector leakage analysis (TVLA), and the measurement setup. Section VII finally concludes this article.

II. Related Works

Power/EM SCA countermeasures can be classified into three broad categories. First two categories are **logic-level** countermeasures and **architectural** countermeasures that belong to design-specific countermeasures. The final category is **circuit-level** countermeasures, which is physical and more generic in nature.

A. Logic-Level and Architectural Countermeasures

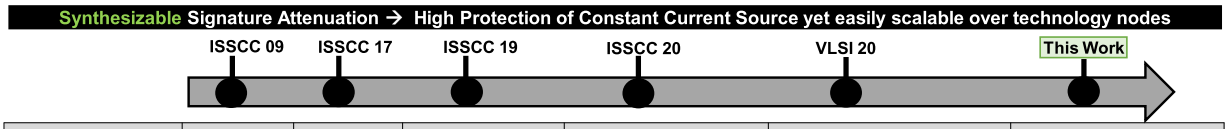
Logic-level countermeasures include sense amplifier-based logic (SABL) [16], dual-rail precharge circuit (DRPC) [17], wave dynamic differential logic (WDDL) [18], and gate-level masking [19], [20]. These countermeasures utilize the principle of power balancing for security. Both DRPC and SABL require equalizing gate-level power leading to a need for specific library cells' design, which requires manual engineering effort. WDDL is the first silicon validated protection technique that can be designed using single-rail standard cells. However, this solution suffers from a higher power, area, and performance overheads.

The second category is the architectural countermeasures. These countermeasures include distortion in the trace by insertion of dummy operations, shuffling of operations, arithmetic countermeasures, and so on. These are effective but cannot provide the highest level of security as there is a limited number of operations to be shuffled depending on architecture and algorithm [21]. Moreover, these solutions are very much architecture-specific and not generic to any crypto-engine.

B. Circuit-Level Countermeasures

Final category of countermeasures is called physical-/circuit-level countermeasures. Circuit-level countermeasures against power/EM SCA include current equalizer [8], [9], series LDO [22], and integrated voltage regulator (IVR) [11], which enhances protection up to 10M traces. Noise injection-based countermeasures reduce the SNR, helps improving security, and, however, suffers from a very high power overhead [23].

Switch capacitor-based current equalizer [8] achieves a high MTD by isolating the encryption engine from V_{DD} and bypass the key-dependent leakage by connecting periodically with an ac ground. This is a pioneering work among switch capacitor-based solutions and provides the highest MTD among silicon-verified switch capacitor-based countermeasures to date. However, one drawback of this solution is that it suffers from performance degradation. It is not easily scalable over technology nodes as dc bias (ac ground) and analog comparator are used. Our work utilizes a switch capacitor as temporary storage of charge and achieves time-domain obfuscation with help of switch capacitors. Hence, there is no



Technique		Switched Capacitor Current Equalizer	Integrated Buck Regulator	Digital LDO with Randomization	Current Domain Signature Attenuation	Digital NL-LDO with Randomization and Arithmetic Countermeasure	Digital Signature Attenuation with Time-Varying Transfer Function
MTD	**Single Strategy**	>10M	>0.1M	6.8M	**>1B**	**>10M** → 25x	**~250 M**
	Combined Strategy	-	-	-	-	**>1B**	**>1.25 B**
Strategy	Signature Attenuation	×	×	×	✓	×	✓
	Switched Cap.	✓	×	×	×	× Digital-friendly	✓
Synthesizable/Easily Scalable over Technology Nodes		No (Analog comparator+ Ref. Voltage)	No	Yes	No	Yes Digital-friendly	Yes
Capacitor Inductor		300pF None	3.2nF MIM 11.6nH(board)	1.9nF MIM None	150pF MOS None	- None	180pF (DSAC), 320pF (+TVTF) MOS None
Limitation		High Perf. Deg.(2x)	On board Inductor →Attackable	High MIM cap →EM leakage	**Analog Solution** →Higher Engineering Effort to scale	Higher overhead with LDO, Arithmetic countermeasures →Specific to algorithm	-

Fig. 2. State-of-the-art circuit-level countermeasures' timeline.

requirement for analog reset and comparator, which is making our solution digital. IVR [11] uses buck converter along with loop randomization for security. It suffers from high passives, including onboard inductors making it inherently vulnerable to attacks. Series LDOs are insecure as the instantaneous current drawn by the LDO circuit is equal to AES current [24]. Series LDOs with loop randomization provide better security and, however, use MiM capacitor, which can leak side-channel information by EM radiation [22].

Recently, CDSA was proposed, which, for the first time, achieved an MTD of >1B. CDSA [12], [13] uses cascode current source (CS) for signature attenuation and PMOS-based bleed path to bypass key-dependent leakage, voltage DACs for biasing the CS, and analog comparators for the switched-mode control (SMC) loop. However, most of these components are analog in nature and, hence, require manual effort to scale across technology nodes. This work brings the benefit of signature attenuation into the digital domain by introducing similar components in a digital-friendly manner.

Another countermeasure [14], [15] has recently achieved a similar level of security in silicon against different SCA attacks. This is a cascade of two countermeasures namely, non-linear LDO, and arithmetic countermeasure [14]. One countermeasure alone of these two provides medium security (∼10M MTD) against SCA. LDO has a higher power overhead, and it takes an almost similar area to an AES encryption engine. Moreover, the arithmetic countermeasure is very specific to the algorithm [14]. A timeline of the state of the art is presented in Fig. 2.

Our solution (Syn-STELLAR) addresses both problems. The goal of this work is to achieve a higher MTD with an all-digital solution and improve the state of the art for a single scalable countermeasure with comparable area/power overheads. It should be noted that, although just DSAC is not as effective as CDSA as a single countermeasure strategy, the DSAC achieves ∼250M MTD as a single countermeasure technique and >1.25B MTD in combination with TVTF against both power/EM SCA.

III. Digital Signature Attenuation Circuit: Concept and Circuit Design

CDSA technique [see Fig. 1(a)] has shown that the MTD is proportional to Attenuation^2 [25] and achieved very high SCA resilience through signature attenuation by utilizing a high impedance CS [12]. We leverage the similar strategy of signature attenuation. However, our CS design along with the other circuit components for both DSAC and TVTF is digital-friendly. Conceptual contribution, key design techniques, and components are discussed in more detail in the following.

A. Key Contributions

In general, reducing the signal-to-noise ratio (SNR) helps improve the MTD. However, the CDSA technique required cascode CS slices, PMOS bleed path, and voltage digital-to-analog converters (DACs) for bias voltage generation, which are inherently analog in nature and require manual re-design to scale across technology nodes. In this work, we resolve this constraint by making the digital-friendly signature attenuation circuit. This solution, for the first time, utilizes digital-friendly CSs to attenuate the critical signature and, hence, brings the benefit of analog signature attenuation in the digital domain to achieve higher SCA security. Parallelly, along with the DSAC, an intelligent TVTF is incorporated for enhanced security. A conceptual diagram is shown in Fig. 1(b) and (c). The key contributions of this article are summarized as follows.

1) **DSAC** is used to ensure CDSA using a digital-friendly circuit resulting in 25× MTD improvement over the existing state of the art for a single digital countermeasure.

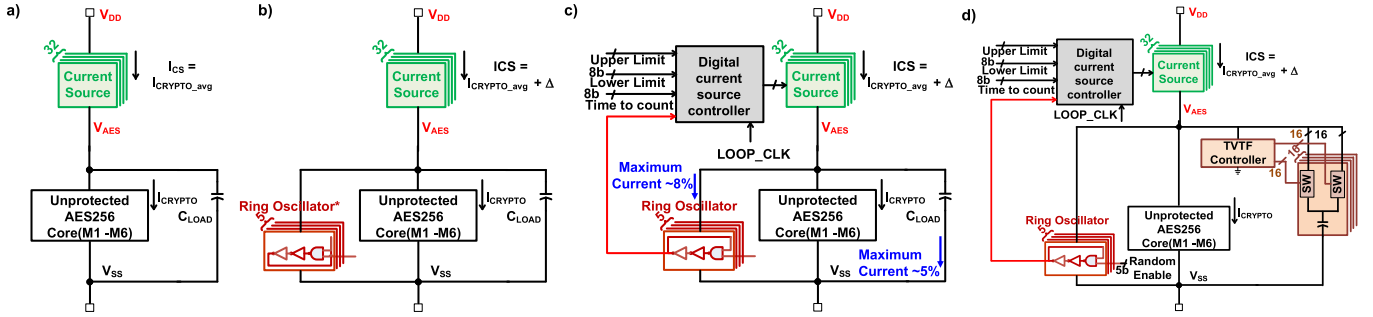


Fig. 3. (a)–(c) Build-up to the DSAC design and (d) DSAC with TVTF integrated. (a) Realization of digital CS. (b) RO-based LNFB used to bypass encryption dependent leakage. (c) Low-bandwidth digital global SMC loop used for PVT variation and coarse current change of AES-256. (d) Switch capacitor-based TVTF integrated with DSAC for enhanced security.

a) DSAC uses a high impedance **digital-friendly CS** to supply the average crypto-current and to attenuate the signature.
b) **Bleed path** is digitized by utilizing a **ring oscillator (RO)** instead of biased PMOS.
c) RO acts as a voltage-dependent current load. Hence, it has been used as **local negative feedback (LNFB)** to bypass the key-dependent leakage current.
d) Based on RO oscillation frequency, a low-bandwidth global CS controller tunes number of CS slices at startup or in case of coarse current variations due to changes in frequency or PVT corner. Hence, RO acts as an **input of global negative feedback** (GNFB) loop.

2) **TVTF** strategy improves the previous switch capacitor-based SCA countermeasure [8] toward a digital-friendly countermeasure. It incorporates the switch capacitor-based countermeasure without the analog reset phase of the current-domain equalizer circuit [8], [9], which provides the highest resilience for a switched cap-based solution to date. In our proposed TVTF, switched capacitors are utilized as temporary charge storage elements, and these charged capacitors are "physically" shuffled to provide time-domain obfuscation of the crypto-current signature before it passes through the DSAC, which then provides significant signature attenuation to achieve enhanced security. An intelligent lightweight digital controller circuit (TVTF controller) is designed for implementing the TVTF logic.
3) Finally, **Syn-STELLAR** utilizes **a combination of DSAC & TVTF** strategies to achieve an MTD of >1.25B, which improves overall countermeasure state of the art by 25%.

B. Circuit Architecture

Signature attenuation has been proven to be a powerful technique as a countermeasure. Based on instantaneous power consumption while encryption, correlated voltage fluctuations are visible at the V_{DD} node. Ideally, making those instantaneous current/power fluctuations invisible or fully constant can help in providing security [12]. Practically, it is impossible to make it fully constant to get complete security. A very high impedance CS between actual V_{DD} node and operational V_{DD} node (mentioned as V_{AES} hereafter) can attenuate the signature by a factor of Attenuation^2, which can help to enhance security, as shown in Fig. 3(a). This is the fundamental concept of Signature aTtenuation Embedded crypto with Low-Level metAl Routing (STELLAR)-based countermeasures, which remains the same for this article as CDSA. CDSA is able to attenuate the signature by 350× using a highly analog cascode CS. Our novelty of this work is implementing this countermeasure as a synthesis-friendly strategy against SCA and, hence, the name Syn-STELLAR.

While placing the CS within V_{DD} and V_{AES} node, it should be ensured that average crypto-current I_{CRYPTO_avg} constantly flows through the CS to drive the AES-256 encryption engine. This is required to make supply current independent of instantaneous crypto-current without any performance penalty.

Depending on the key byte, the current drawn by the encryption engine changes a little. This delta change of current should be bypassed to the ground (bleed path) to mask the key-dependent leakages. Current through the bleed path (I_{bleed}) should be a function of its supply voltage. RO satisfies this property; hence, it is used as the bypass path, as shown in Fig. 3(b). Another reason behind choosing an RO is that it can be easily synthesized using already available commercial tools. Multiple ROs are incorporated in this design, and they can be randomly turned on and off to inject noise at V_{AES} node, which further helps the countermeasure.

On the other hand, we can get an idea of V_{AES} node voltage by keeping track of RO frequency (by counting oscillation of RO in the time domain). Hence, RO frequency can be used as an input for the global feedback network. Based on the frequency of RO, a global SMC loop, namely, digital CS controller, decides to turn on or turn off CS slices to maintain the average current, as displayed in Fig. 3(c). Thus, the V_{AES} node voltage can be controlled. RO acts as an input to the GNFB and the LNFB, thereby combining the two loops together. It is observed that the excess quantization error current with respect to average current is very minimal. The maximum current through RO is ∼8%, while the maximum current through load capacitor (C_{LOAD}) is observed around 5%. Fig. 3(d) shows how the switch capacitor-based TVTF can be used instead of load capacitor. It is discussed in Section IV in detail.

C. Digital-Friendly Current Source

CS is the core of our countermeasure. CDSA used a cascode CS for signature attenuation, as shown in Fig. 4(a). Cascode

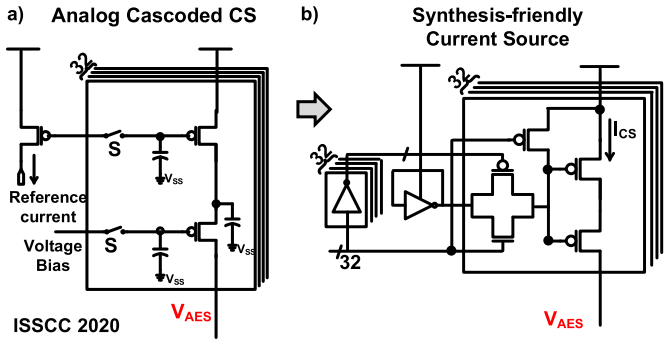


Fig. 4. (a) Cascoded CS used in CDSA [12]. (b) Digital-friendly CS.

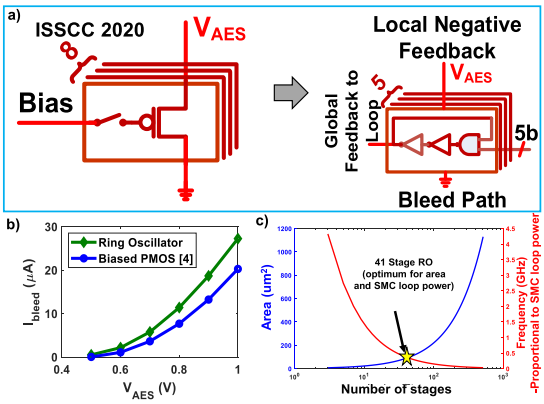


Fig. 5. (a) RO as LNFB. (b) Parametric Extracted (PEX) simulation shows similar behavior in biased PMOS and RO as bleed path. (c) 41-stage RO used for area/power optimization of SMC loop.

CS gives 10× more attenuation with respect to the simple CS stage. Attenuation is expressed by the following equation:

$$\text{Attenuation} = \frac{\text{SNR}_{\text{core with countermeasure}}}{\text{SNR}_{\text{unprotected}}}. \tag{1}$$

However, it is analog in nature as it includes voltage bias and reference current, which should be avoided to make it easily technology scalable. A synthesis-friendly CS is designed in this work. CS is realized using stacked PMOS, as shown in Fig. 4(b). V_{AES} node voltage can be controlled through global feedback.

A desirable voltage between 0 to V_{DD} is required to bias the stacked PMOS to realize the CS. Intermediate voltage is created by using a self-biased inverter, as shown in Fig. 4(b). A power-gate switch is used for connecting the bias voltage to the PMOS gate. Switching CS slices are controlled by the global SMC loop. Readers should note that the corresponding ISSCC manuscript has similar CS, which does not have to pull up PMOS to turn it off. That is a typo, which is corrected here.

One important point to note is attenuation is ∼41× just by using this digital CS circuit. However, unlike [12], attenuation is not the sole contributor of the defense mechanism. It is one of them. Randomized bleed path and TVTF (explained later) work together along with attenuation to increase security.

D. Ring Oscillator as Local Negative Feedback

RO is another important component of our Syn-STELLAR circuit. An LNFB is needed to bypass the key-dependent leakages. CDSA used a biased PMOS as negative feedback to bypass the encryption-dependent current variation. However, a key requirement of our Syn-STELLAR design is to make all the components digital while exploiting the signature attenuation feature for higher security. Hence, the requirement of analog biasing has been removed. Instead, RO is used for LNFB, as shown in Fig. 5(a). Parasitic extracted simulation results [see Fig. 5(b)] show that the RO draws a similar bleed current as a biased PMOS. When the V_{AES} node voltage increases or decreases, the current through bleed path I_{bleed} increases or decreases to as it follows the following equation:

$$\begin{aligned} \text{Consumed Power} &= I_{\text{bleed}} \times V_{\text{AES}} = f \times C \times V_{\text{AES}}^2 \\ &\Longrightarrow I_{\text{bleed}} \propto C \times V_{\text{AES}} \times f \;\&\; f \propto V_{\text{AES}} \\ &\Longrightarrow I_{\text{bleed}} \propto V_{\text{AES}}^2. \end{aligned} \tag{2}$$

The frequency of RO changes proportionately with respect to V_{AES}. As V_{AES} increases, the RO bypasses the extra CS current, which is more than the average AES current consumption. Fig. 6(a) (simulation) shows the effect of the RO bleed to maintain the V_{AES} within the desired range of the guardband. We observe that, without the bleed path, V_{AES} keeps increasing with time (as the CS current $I_{CS} = I_{\text{AES\_avg}} + \Delta$) due to the extra delta current (Δ), which is the quantization error (difference between CS current and actual current drawn by AES). Now, when the RO is enabled, as V_{AES} increases, the RO frequency increases proportionately. Hence, the extra current is bypassed through the RO, exhibiting LNFB and ensuring that the voltage stays within the guardband during the steady-state operation. The gain $[(\Delta I_{\text{bleed}})/(\Delta V_{\text{AES}})]$ can be controlled by tuning the number of parallel RO bleed that is turned on.

The change in current due to random bleed turn on creates a little bit fluctuation as power supply noise at V_{AES} node, as shown in Fig. 6(b). This helps in security. On another note, RO acts as LNFB. Hence, it has a direct contribution in bypassing the delta variance in current, which helps in security as well. As LNFB, it helps to keep V_{AES} node voltage at a stable point in steady state when the global feedback loop is disengaged. Power overhead/stability and randomization for the security can be traded off using this control knob (number of RO turned on).

E. Ring Oscillator as Global Negative Feedback

RO has another important feature that its output frequency is a reflection of its voltage. This property plays an important role in our Syn-STELLAR circuit. V_{AES} voltage can be estimated by counting the number of oscillations in a given period. GNFB is integrated to LNFB utilizing this property. When RO oscillation count goes beyond the predefined bound provided by the user, the SMC loop gets engaged, and CS slices are activated or deactivated as required. By controlling the number of CS slices, V_{AES} node voltage can be controlled.

It is clear that RO is one of the most important components of our design. The GNFB SMC loop works based on RO output. SMC loop uses an asynchronous counter to count RO frequency. If the RO frequency is too high, the SMC loop will end up being a power-hungry block. Hence, we require more

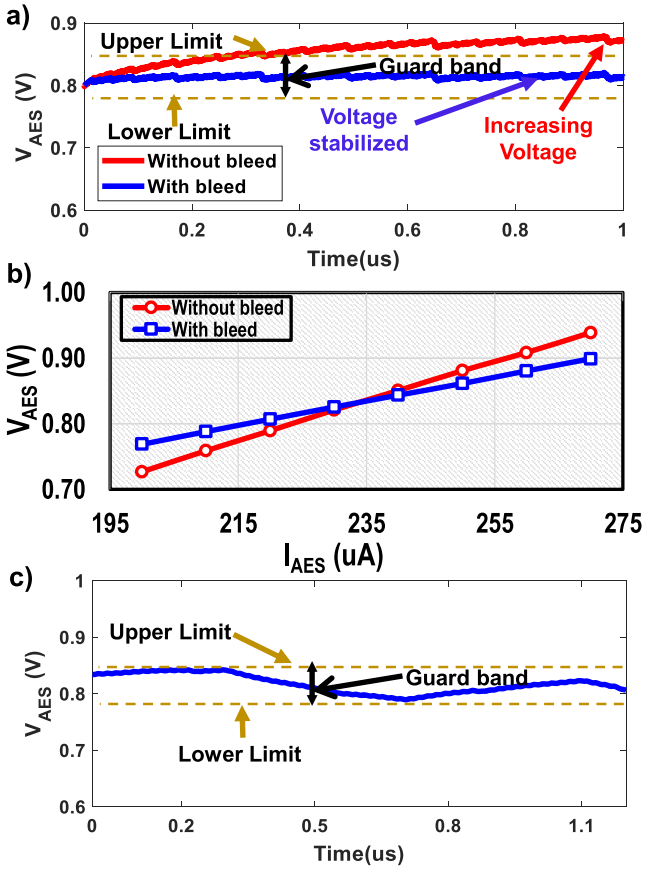


Fig. 6. (a) V_{AES} voltage with random bleed path enabled and disabled. (b) V_{AES} variation with injected I_{AES} using CS. (c) V_{AES} when random bleed enabled.

number of stages for the RO. However, an increasing number of stages a lot will lead to higher area overhead. Hence, an optimum point is required for minimal power and area overhead. Fig. 5(c) shows that 41 stages of RO are optimum from an overhead point of view for this technology and current loads, which is implemented in the test chip.

F. Ring Oscillator as Randomized Noise Source

RO is also used to serve as a noise injector. Noise can be injected at V_{AES} node by randomly activating or deactivating RO slices. This randomization process helps in countermeasure's overall performance against side-channel analysis (SCA). As we are randomizing the number of RO slices to be turned on in the bypass path, the total bleed current changes slightly, which makes the V_{AES} node voltage fluctuate. It should be noted that too much fluctuation might cause performance degradation, which should be avoided.

G. Current-Source Controller Loop

SMC is used as the GNFB for the countermeasure circuit, as shown in Fig. 7. An asynchronous counter counts the number of oscillations by RO for a fixed time period, which can be controlled through the scan. Although an optimized number of stages of RO is used for power/area optimization, a three-stage frequency divider circuit is further employed to reduce the operational frequency so that asynchronous counter

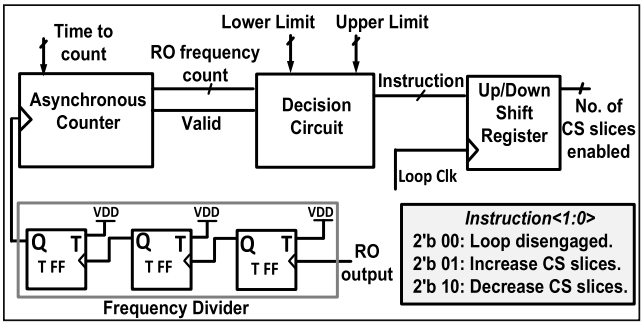


Fig. 7. Global switched-mode controller loop architecture.

consumes lesser power. Based on RO frequency count for a given time period, a decision circuit takes the decision to activate or deactivate CS slices. The lower limit and upper limit of count value provide a guard band across V_{AES} voltage to ensure that the SMC loop is turned off during the steady state. The decision circuit provides instructions to up/down shift register, which, in result, turns on or off the CS slices. SMC loop engages in two conditions.

1) At **startup**, to ensure saturation region of CS slices for high impedance isolation and stability; the SMC is engaged to turn on or off the required number of CS slices.
2) If, for some reason (for example, **process, voltage, or temperature (PVT) variation** or **change in operation frequency**), coarse change in current drawn by encryption engine is observed, the SMC turns on and adjusts the number of CS slices accordingly.

A sample waveform is presented in Fig. 8(a). Frequency divided RO output is counted by the asynchronous counter and can be seen in RO frequency count. If it is greater than the upper limit or less than the lower limit, the decision circuit will take the decision to reduce or increase the number of CS slices, respectively. It is observed from the waveform of Fig. 8(a) that the RO frequency count is greater than the upper limit. Hence, no. of CS is reduced until and unless it reaches within the predefined lower limit and upper limit value. SMC loop is active at the startup of the circuit, as shown in Fig. 8(b). SMC loop is engaged until and unless V_{AES} node voltage enters within a guard band of the lower limit and upper limit to ensure saturation region of PMOS so that it can act as CS. Once AES voltage comes to the desired range, the loop is disengaged.

It should be noted that the guard band plays an integral role in the security and efficiency of the encryption engine. Guard band consists of minimum and maximum voltage levels for the V_{AES} node. The minimum voltage level should not be decided as very low as it will hurt the efficiency. The maximum frequency of operation for the AES encryption core will be reduced as well in that case. The maximum voltage level of the guard band is very important for security purposes. Digital CS is realized by keeping stacked PMOS in the saturation region. The drain voltage of the PMOS should be controlled properly in order to maintain the PMOS in the saturation region. The maximum voltage level of the guard band determines V_{SD} of the PMOS and ensures the saturation region of PMOS in

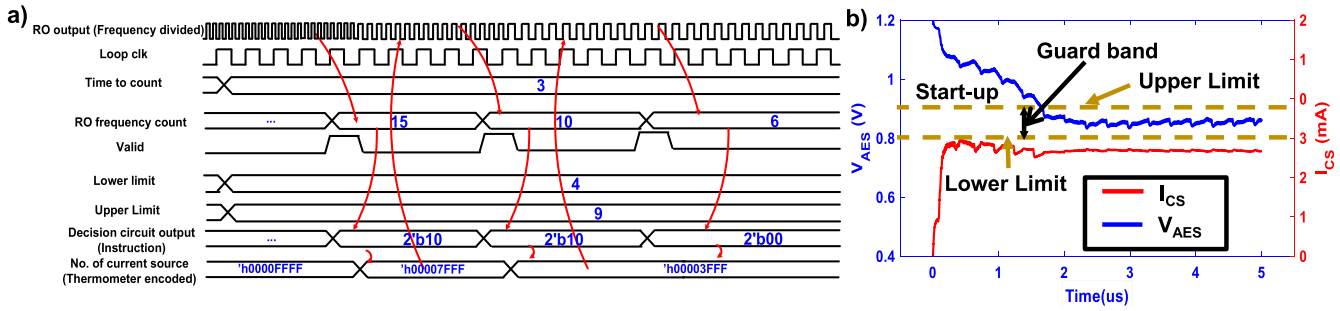


Fig. 8. SMC loop waveforms. (a) Waveform of the loop. (b) After startup, average current is adjusted by turning on CS slices to make sure that V_{AES} is within guard band.

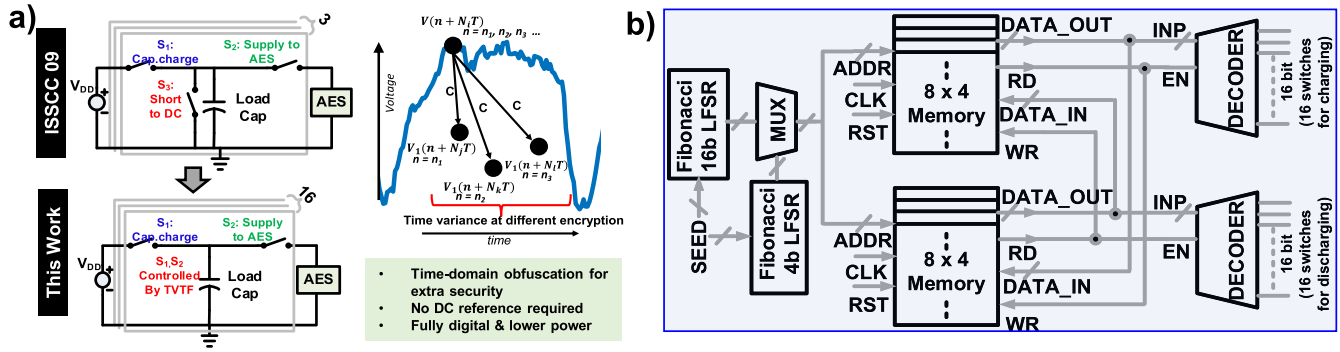


Fig. 9. (a) Switched capacitor-based TVTF. (b) Lightweight two-stage LFSR-based TVTF controller.

order to get higher attenuation. This is critical because we do not want the instantaneous voltage across the AES (V_{AES}) to be reflected to the supply current. Basically, it ensures that the SMC loop is turned off in the steady-state operation of the DSAC. This, along with the low-frequency operation of the SMC and the high impedance CS on top, makes sure that the correlated signature is not passed directly to the power supply pin.

IV. Time-Varying Transfer Function for Additional Security

Our second technique is switch capacitor-based TVTF. Switch capacitor-based countermeasure was initially proposed by Shamir *et al.* [26]. A different version has been implemented by Tokunaga *et al.* [8], [9]. A three-phase switch capacitor is used for this. A capacitor is getting charged at the first phase. It charges the AES encryption engine at the second phase. In the final phase, the encryption engine is connected to an ac ground to bypass the encryption-dependent leakages. Encryption-dependent leakages are the reason for side-channel leakage. While different plaintext is sent to the encryption engine, the instantaneous current drawn by the circuit changes a little, which is the source of the side-channel leakage. This can be called encryption-dependent leakage. In this way, higher MTD is achieved for this circuit. Three capacitors have been used for continuous operation. However, it has one drawback. It uses a current equalizer in the reset phase to bypass the key-dependent leakage. It is not easily scalable over technology nodes. This reset phase is removed in the presented solution (details discussed in Section IV-A).

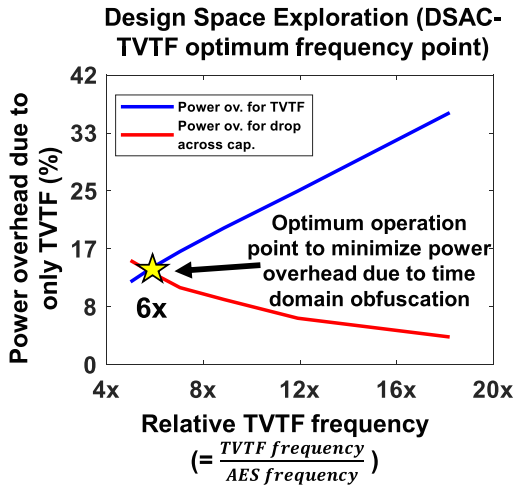


Fig. 10. Design space exploration for optimum TVTF frequency to reduce overhead. Frequency is calculated relatively with respect to the AES frequency. Power overhead is calculated only for TVTF as it is a theoretical evaluation for finding the optimal design point.

Moreover, the current equalizer-based countermeasure suffers from performance degradation.

A. Switched Capacitor-Based TVTF Design

Our primary goal for Syn-STELLAR design is to make it digital. Hence, we use switched capacitor-based circuits in a different manner. The 16∼20-pF unit capacitors, as shown in Fig. 9(a), are used. At one particular time sample, one capacitor is connected to V_{DD}. At that point of time, another capacitor charges the AES-256 encryption engine. Other

14 capacitors are at rest. At a different point of time, different capacitors are picked for charging AES and getting a charge from V_{DD} from the resting capacitor pool. This circuit has been used for creating time-domain obfuscation leading to extra security.

Traces are randomly shuffled in the time domain to create the variance. This is working as countermeasure. The right figure of Fig. 9(a) pictorially depicts the time variance. The waveform is voltage trace of one particular cycle of encryption operation. N_i^{th} sample of the trace is considered in the figure. After random obfuscation, N_i^{th} trace is located in different time sample in different iterations (i.e., N_j, N_k, N_l, and so on) of encryption. n generally implies number of iterations (n_i, n_2, n_3, and so on). Amplitude (V_1) is slightly different from unprotected voltage trace (V) as capacitors inherently add an integration of charge. Also, here, voltage traces have been collected by measuring voltage drop across 1-Ω resistors embedded in PCB. Basically, this drop implies current or power traces expressed in voltage terms.

One important tradeoff is taken while choosing the size of the capacitors. Design considerations are given as follows: area overhead should not be greater than ∼50%, and only MOS cap should be used as higher level MiM capacitors radiate and are vulnerable to EM side-channel attacks. Hence, ∼320 pF of MOS cap can be used to satisfy both criteria. A smaller number of unit capacitors will not be enough to create obfuscation, and hence, minimum 16 capacitors are used of ∼20 pF each. It should be noted that the effect of multiple numbers of capacitors on security is still under research. An increasing number of capacitors (keeping total capacitance constant) will lead to a reduction in capacitance, which will create high droop across the capacitors and will affect the efficiency of AES.

It should be noted that there is an important tradeoff if power overhead is considered. If the relative frequency of the TVTF circuit increases, power overhead increases too, as the power of the digital circuit is directly proportional to frequency. However, lower frequency causes high voltage droop, which causes higher power overhead. Hence, an optimum result is found from the simulation (presented in Fig. 10), and it is observed that 6× relative frequency with respect to AES is optimum from an overhead point of view. Hence, the TVTF is operated at 6× frequency. Switch capacitor-based TVTF creates time-domain obfuscation prior to the signature attenuation with DSAC; 16 switch capacitors and an intelligent TVTF controller have been used for this circuit realization, as shown in Fig. 3(d).

B. TVTF Controller

The TVTF controller is a very lightweight circuit. It has two small memories, two cascoded Fibonacci LFSRs for randomization, and two decoders, as shown in Fig. 9(b). The two memories keep track of the two sets of capacitors namely the charging capacitor set and discharging capacitor set. Capacitors are randomly selected for charging and discharging by randomly selecting addresses of the memories. After charging or discharging is done, capacitors swap places between the memories as the charged capacitor is ready to discharge and vice versa.

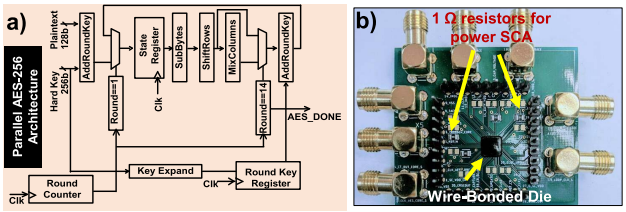


Fig. 11. (a) Parallel AES-256 architecture used as a crypto-engine in test-chip. (b) PCB photograph.

Two memories store tag number for capacitors. Each number signifies an identifier for each capacitance. Hence, any integer implying the tag will be fine. However, in our code, we were storing 1–8 in the "charging array" and 9–16 in the "discharging array." The only thing to consider here is that there should not be any repetition of tag as that will lead to malfunction of switch capacitor block.

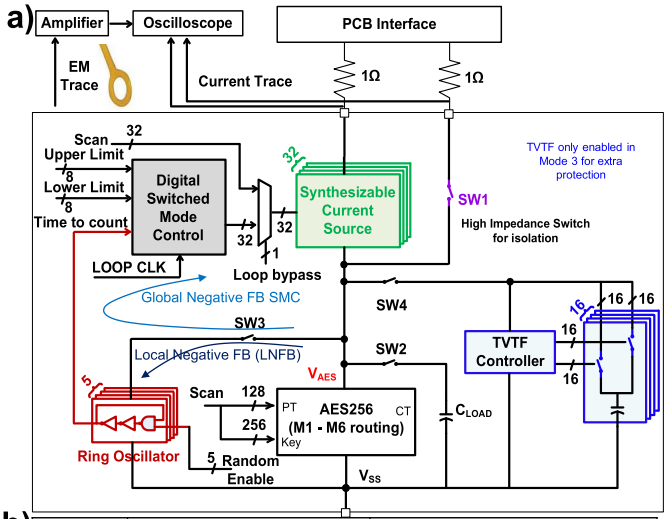
LFSRs can be a weak link and can potentially be broken by attackers. However, seeds of the LFSRs are provided from an outside true random number generator (TRNG). It should be noted that TRNGs can be used as the source of randomization. In this work, the focus is to check how obfuscation helps as a countermeasure under the assumptions that, if the process is effective, seed can be protected using TRNGs as they are easily available in modern-day SoCs. Moreover, obfuscated traces are further attenuated. Just by seeing the side-channel waveform, it is not possible to detect the obfuscation. Hence, the randomization unit is not vulnerable.

V. System Architecture

A parallel AES-256 is implemented as the encryption engine in the test chip. Architecture of AES engine is presented in Fig. 11(a). This implementation requires 14 cycles per encryption. The parallel architecture ensures high throughput. Fabricated PCB is shown in Fig. 11(b). Wire bonded die and 1-Ω register are clearly visible from the PCB photograph. Note that 1-Ω resistor is used for power SCA. System architecture is shown in Fig. 12(a). It has all three modes, namely, unprotected AES-256, DSAC-AES-256, and DSAC-TVTF-AES-256. Unprotected AES-256 is activated when switch 1 is ON and other switches are OFF. DSAC-AES-256, which is the single strategy used as a countermeasure, can be activated by turning off switches 1 and 4 and turning on switches 2 and 3. DSAC-TVTF-AES-256 is our final strategy. It can be activated by turning off switches 1 and 2 and turning on switches 3 and 4. Switching activity is tabulated in the table of Fig. 12(b).

It should be noted that Fig. 12(a) shows the detailed system architectures. Switches used here are different from switches used in the conceptual diagram in Fig. 9(a). The TVTF circuit presented in the conceptual diagram is implemented in the real circuit presented in Fig. 12(a). Switches are in-built in TVTF architecture, as shown in the blue shade of the system architecture.

One more important point to note is that all the measurements are done at 10 MHz. However, it is observed from load



Modes	Description	Configurability
Mode 1	Unprotected AES-256	SW 1 ON, SW2-4 OFF (see Fig. 11(a))
Mode 2	DSAC-AES256 (Single Strategy)	SW2-3 ON, SW1 & SW4 OFF (see Fig. 11(a))
Mode 3	DSAC-TVTF-AES256 (Combined Strategy)	SW1-2 OFF, SW3-4 ON (see Fig. 11(a))

Fig. 12. (a) Full system architecture. (b) Different mode of operations supported in the IC.

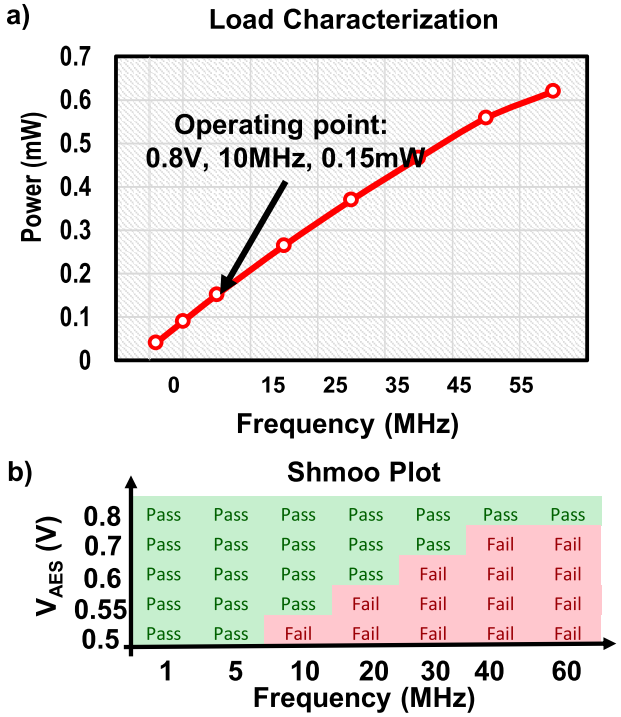


Fig. 13. (a) Load characterization of the encryption engine. (b) Shmoo plot explaining different maximum frequencies in different supply voltage levels.

characteristics presented in Fig. 13(a) that AES is operational at 60 MHz. Point of operation is 0.8 V at 10 MHz, which consumes ∼0.15-mW power. A Shmoo plot is presented with details of functionality check in different supply voltages and different frequencies in Fig. 13(b). It is observed that the encryption engine works perfectly at ∼5 MHz at a lower supply voltage of 0.5 V. However, it fails to work in higher frequency at those lower supply voltages. However, the test chip is fully functional at 60 MHz at 0.8 V. It should be noted that MTD is related to attenuation, and attenuation

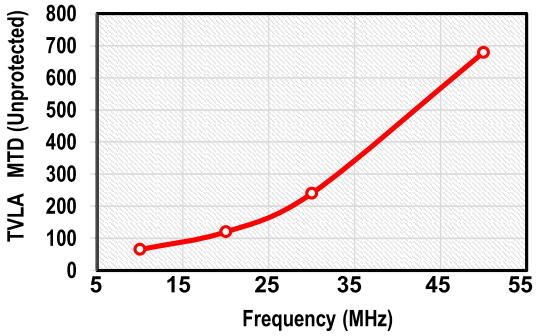


Fig. 14. TVLA MTD at different AES clock frequencies.

is proportional to output impedance [24], hence inversely proportional to frequency (Attenuation $\propto 1/(\omega RC)$, where ω is the frequency, R is the load impedance, and C is the parallel capacitors). Higher frequency inherently increases the MTD number of unprotected implementations. The encryption engine is operated at 10 MHz to avoid default attenuation at a higher frequency. For the sake of clarity, leakage analysis is conducted via TVLA test in different frequencies and presented in Fig. 14. It is observed that the power consumption of the encryption engine starts meaningful leakages after 700 traces for 50 MHz and 250 traces for 30 MHz while as low as 65 traces for 10 MHz. It is clear that a lower frequency of operation leads to higher leakages (hence, lower baseline MTD), which implies that baseline will be low and the efficacy of the countermeasure can be thoroughly checked in a limited measurement setup. It should be noted that, even at 10-MHz operational frequency, protected AES shows better results than existing SoAs.

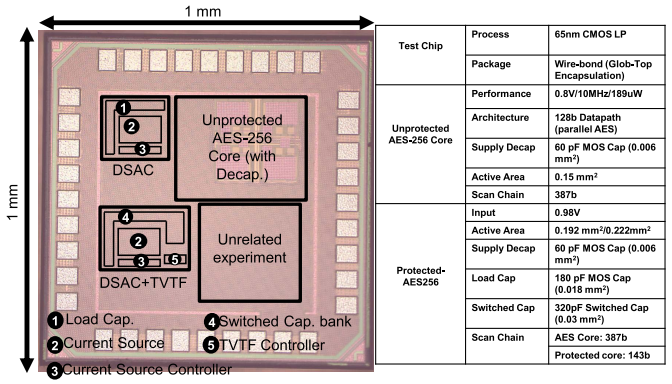
VI. Measurement Results: Efficacy of the Countermeasure

Die micrograph is shown in Fig. 15. All the key circuit components are visible from the die diagram. The details of chip implementation are summarized in Fig. 15. The chip is fabricated in a 65-nm CMOS process. The package was wire-bonded on the PCB with glob-top encapsulation. Unprotected AES implementation takes an active area of 0.15 mm^2. A scan chain-based interface is used for configuring and testing the chip; 60 pF of load capacitor is used as a decoupling capacitor.

A. Test Setup

The test chip has been attacked using CPA and CEMA both in the time domain and the frequency domain. First, the trace is collected in the time domain and transferred to the frequency domain by the fast Fourier transform (FFT). Then, CPA/CEMA is conducted by sweeping center frequency from 10 MHz to 1 GHz with a bandwidth of 10 MHz, as shown in Fig. 16(a). The time-domain attack is done by correlating time-domain traces with respected HD of all possible guesses of single keybyte at 13th and 14th rounds of AES-256 operation, as shown in Fig. 16(b).

Our test setup is presented in Fig. 16(c). Power traces have been collected by a 5-GS/s oscilloscope-based setup.



Test Chip	Process	65nm CMOS LP
	Package	Wire-bond (Glob-Top Encapsulation)
Unprotected AES-256 Core	Performance	0.8V/10MHz/189uW
	Architecture	128b Datapath (parallel AES)
	Supply Decap	60 pF MOS Cap (0.006 mm²)
	Active Area	0.15 mm²
	Scan Chain	387b
Protected-AES256	Input	0.98V
	Active Area	0.192 mm²/0.222mm²
	Supply Decap	60 pF MOS Cap (0.006 mm²)
	Load Cap	180 pF MOS Cap (0.018 mm²)
	Switched Cap	320pF Switched Cap (0.03 mm²)
	Scan Chain	AES Core: 387b
		Protected core: 143b

Fig. 15. Die micrograph of the system in 65-nm CMOS process and design summary.

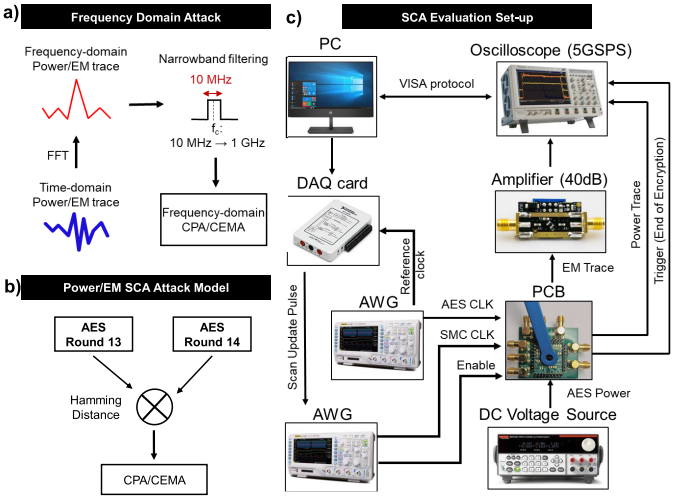


Fig. 16. (a) Frequency-domain attack model. (b) Time-domain correlational attack model. (c) Measurement setup for EM and power SCA attacks, including actual PCB photograph.

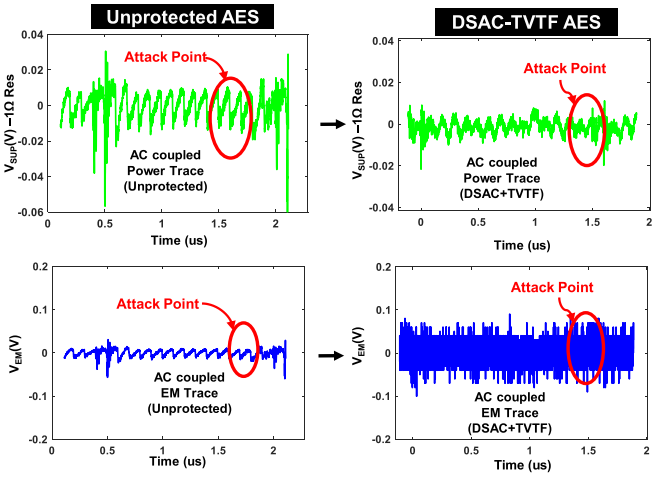


Fig. 17. Time-domain waveform from the measurement.

Collected traces by the oscilloscope are sent to a PC for further processing using VISA protocol. PC gives input to the chip by a DAQ card. Arbitrary wave generator (AWG) is used for clock and enable signal. The dc voltage source is used for powering up the circuit. A 10-mm H-probe is used for collecting EM

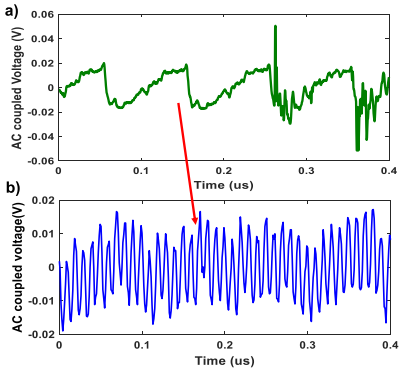


Fig. 18. (a) Unprotected power trace in the time domain. (b) TVTF power trace from the measurement.

traces. It is amplified by 40 dB amplified before being fed into an oscilloscope-based setup.

1000 trace averaging across 1.25M unique traces are taken for the experiment. Signature attenuation, bleed path randomization, and TVTF (switch capacitor-based obfuscation) are used as countermeasure techniques. Attackers will try to average out the inaccuracies and will increase the SNR to extract the key by averaging the traces. This rationale is considered behind choosing the attack method. However, it will be interesting to see how a different number of averaging helps in attacking this type of countermeasure, which will be done as part of future work.

B. Time-Domain Measurement Results

The time-domain power/EM waveform of unprotected AES and DSAC-TVTF-AES-256 is presented in Fig. 17. All the cycles of AES-256 operation are clearly visible in the case of both power and EM signatures for unprotected AES-256. However, for DSAC-TVTF, it is distorted, and the spike comes from the high-frequency operation of TVTF, which does not contain exact information to sniff the data. The attack is done in the last two cycles and shown in the red circle in the time-domain waveform of Fig. 17. Moreover, measured time-domain waveform for TVTF is presented in Fig. 18 confirming switching activity.

C. Measurement Consideration for EM Attack

We choose a 10-mm-diameter H-probe for our EM SCA evaluation. A thorough analysis is performed comparing it with smaller-sized EM probes. A set of measurements using the 10-mm H-probe, as shown in Fig. 19(a), is taken; 14 cycles of AES operation are clearly visible from the collected trace, as shown in Fig. 19(a). We have correlated collected EM trace with corresponding power trace for assurance. A correlation coefficient of 0.1069 is observed.

A similar analysis is performed using a 100-μm Langer probe too, as shown in Fig. 19(b). A 10 $\times$ 10 grid search is executed over the test chip based on TVLA analysis. Thus, the best leakage point is set. Even there, 14 cycles of the AES operation are not clearly visible Fig. 19(a). The correlation coefficient with respect to power trace is 0.0368, which is almost 3$\times$ lower than 10 mm H-probe numbers. Hence,

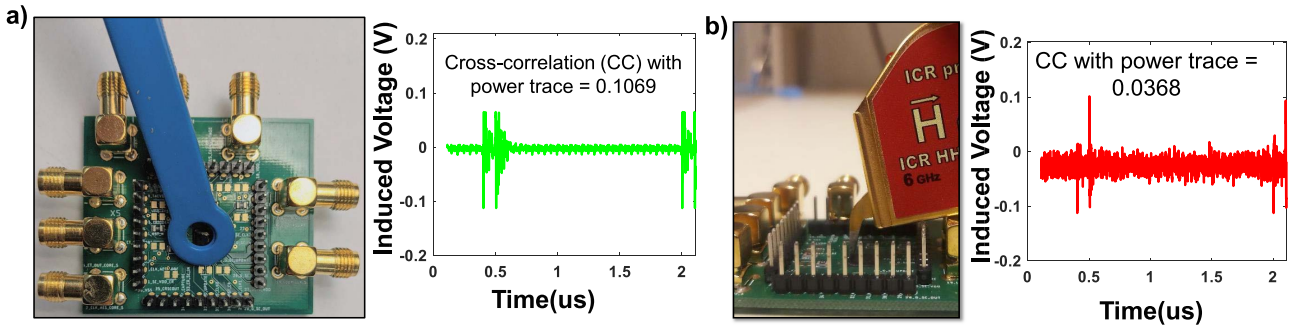


Fig. 19. (a) EM probe setup for 10-mm H-probe. Collected trace has higher correlation co-efficient (0.1069) with power trace hence used in actual attack setup. (b) EM probe setup with 100-μm Langer probe. It has much lower correlation co-efficient even in the best leakage point.

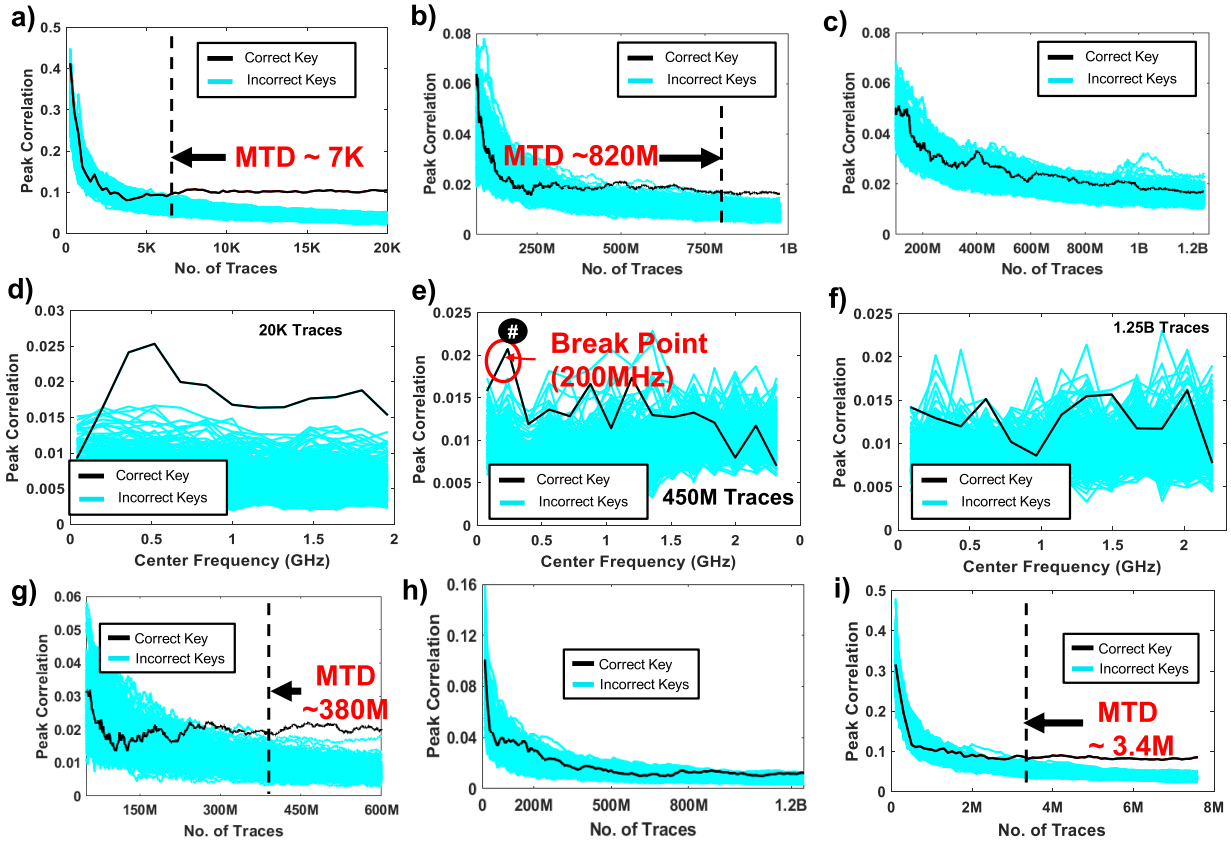


Fig. 20. Time-domain CPA on (a) unprotected, (b) DSAC-AES-256, and (c) DSAC-TVTF-AES-256. Frequency-domain CPA on (d) unprotected, (e) DSAC-AES-256, and (f) DSAC-TVTF-AES-256. (g) Frequency-domain CPA calculation at breakpoint (center frequency of 200 MHz). (h) Frequency-domain CPA at 600 MHz for DSAC-TVTF. (i) Time-domain CPA on standalone TVTF with 1000-trace averaging-based attack setup.

10-mm H-probe is chosen over a smaller probe for attack-related measurements. However, there might be multiple reasons behind the low correlation number using 100-μm Langer probe. Due to packaging, the 100-μm probe cannot reach enough close for a better attack. Also, there might be a possibility that it is not precisely placed for the attack. Further studies are being conducted and will be published in detail as part of future work.

D. EM and Power Side-Channel Analysis and Attacks

1) CPA Attacks: The CPA is conducted for all the modes available. Correct keybyte separates out within 7k traces for CPA in the time domain, as seen in Fig. 20(a). For DSAC-AES-256, the correct key comes out with 820M traces in the time domain, as shown in Fig. 20(b). This shows the effectiveness of the DSAC strategy as a countermeasure. Correct keybyte does not separate out until 1.25B traces in the case of our final strategy, as shown in Fig. 20(c). Frequency-domain attacks are shown in Fig. 20(d)–(f). Correct keybyte is clearly visible for unprotected within 20k traces. However, for DSAC-AES-256, the correct keybyte comes out within 450M traces at the center frequency of 200 MHz [see Fig. 20(e)]. Correct keybyte does not separate out even in frequency-domain CPA with 1.25B traces. Further analysis is performed to find out exact frequency-domain MTD for CPA against DSAC design. It is observed that the correct keybyte can be detected after ~380M traces at the center frequency of 200 MHz (breakpoint), as shown in Fig. 20(g).

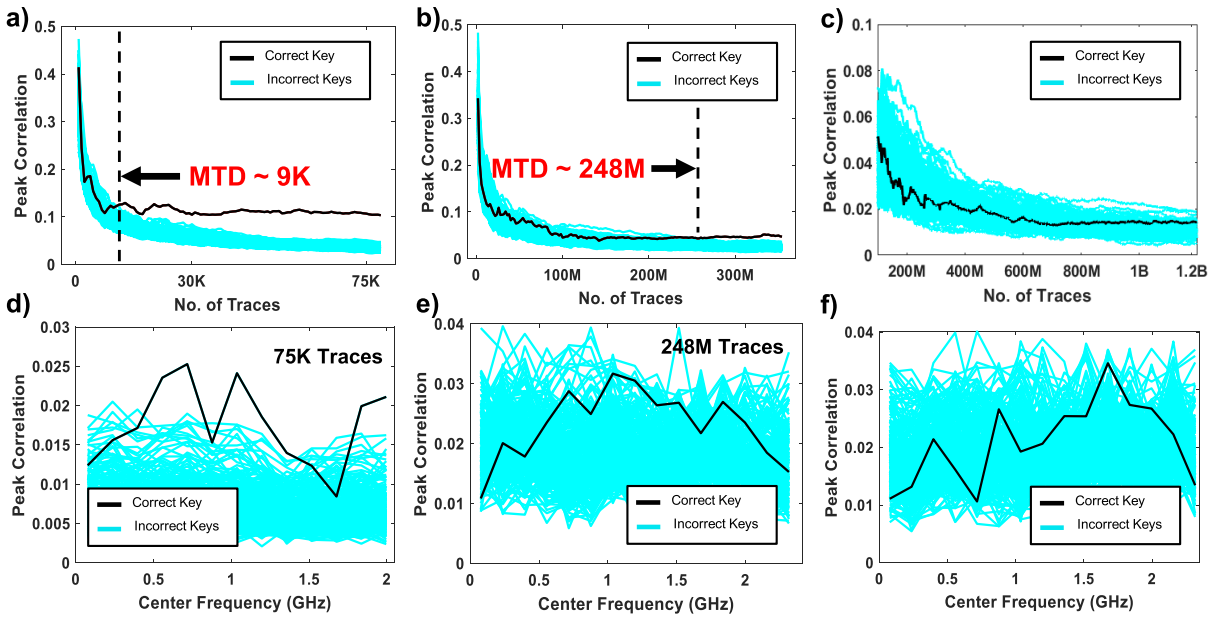
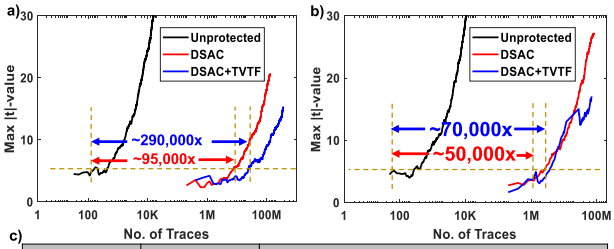


Fig. 21. Time-domain CEMA on (a) unprotected, (b) DSAC-AES-256, and (c) DSAC-TVTF-AES-256. Frequency-domain CEMA on (d) unprotected, (e) DSAC-AES-256, and (f) DSAC-TVTF-AES-256.

Fig. 20(h) shows the peak correlation value for different keybytes with respect to the number of traces at the 600-MHz center frequency for DSAC-TVTF-AES, as Fig. 20(f) shows a relatively higher correlation value for the correct option. It is observed that, even after 1.25B traces, the correct key did not come out. Furthermore, TVTF was enabled without any signature attenuation circuit. It is observed that the correct key comes out within 3.4M traces with 1000 averaging in case, as shown in Fig. 20(i).

2) CEMA Attacks: CEMA is conducted for all the modes available. Correct keybyte separates out within 9k traces for CEMA in the time domain, as seen in Fig. 21(a). For DSAC-AES-256, the correct key comes out with ∼248M traces in the time domain, as shown in Fig. 21(b). Correct keybyte does not separate out until 1.25B traces in the case of our final strategy, as shown in Fig. 21(c). Frequency-domain attacks are shown in Fig. 21(d)–(f). Correct keybyte is clearly visible for unprotected within 75k traces. Correct keybyte does not separate out even in frequency-domain CPA with 1.25B traces.

3) TVLA Results: TVLA tests have been conducted for extra assurance. Note that statistical $|t|$-value reveals the amount of meaningful leakage. A $|t|$-value of less than 4.5 implies the absence of meaningful leakage. Statistical $|t|$-test is done for all the modes of the circuit. A $|t|$-value of 4.5 is achieved in 95 000× more traces in the case of DSAC-AES-256 with respect to unprotected implementation in power SCA, as shown in Fig. 22(a). A $|t|$-value of 4.5 is achieved in ∼290 000× for DSAC-TVTF-AES-256 more traces with respect to unprotected implementation. This clearly indicates that countermeasures are SCA-resilient and provides very good security against power SCA. For EM SCA [as shown in Fig. 22(b)], a $|t|$-value of 4.5 is achieved in 50 000× traces for DSAC with respect to unprotected one and ∼70 000× for DSAC-TVTF-AES-256 with respect to unprotected AES.



c)

|t|-value	Attack Type	No. of Traces		
		Unprotected	DSAC	DSAC+TVTF
4.5	Power	65	6.2M	**19M**
	EM	46	2.3M	**3.3M**

Fig. 22. (a) Power TVLA comparison between all three modes. (b) EM TVLA comparison amongst all three modes. (c) Tabular comparison between the number of traces presented for $|t|$-value = 4.5 in different modes of the test chip.

Detailed leakage analysis is tabulated in Fig. 22(c). TVLA MTD is defined by minimum traces required to cross $|t|$-value of 4.5. Power leakage analysis is conducted for all the configurations. DSAC and DSAC-TVTF have TVLA MTDs of 6.2M and 19M, respectively, while unprotected implementation starts leaking from 65 traces. TVLA MTDs for DSAC and DSAC-TVTF are 2.3M and 3.3M, respectively, for EM side-channel leakage. It should be noted that unprotected implementation starts leaking from as low as 46 traces.

Some prior works have shown EM SCA MTD lesser than power SCA MTD [27]. This is because the EM SCA greatly depends on the position of the EM probe, and we can obtain a localized view compared to the global view for the power traces. Now, with the DSAC countermeasure, we have two types of attenuation: local and global. For the local attenuation, the EM traces are only suppressed by a smaller factor

TABLE I
COMPARISON WITH STATE OF THE ART

Parameter			This Work	JSSC'21 [15]	JSSC'20 [13]	JSSC'20 [23]	JSCC'18 [11]	JSSC '10 [9]
Countermeasure Technique			Digital Signature Attn (DSAC) +TVTF	NL-DLDO + Arithmetic Countermeasures	Current Domain Signature Attenuation	Digital LDO with randomization	Integrated Buck Regulator	Switched Capacitor Current Equalizer
Process			65nm CMOS	14nm CMOS	65nm CMOS	130nm CMOS	130nm CMOS	130nm CMOS
Crypto Algorithm			AES-256	AES-128	AES-256	AES-128	AES-128	AES-128
Standalone AES Power/Frequency			0.15mW@ 10MHz,0.8V	-	0.8mW @ 50MHz, 0.8V	10.9mW @ 80MHz, 0.84V	10.5mW @ 40MHz	33mW @ 100MHz
Design Overheads	Area		**28%(0.043mm^2)** & 52%(0.078mm^2)[d]	8%[c]	36.7%	36.9%[b]	1%[a]	33%
	Power		**33%(0.05mW)** [e] **&** 50%(0.0727mW)[d,e]	10%[c]	49.8%	32%	5%[a]	20%
	Perf.		**0%**	0.7%	0%	10.4%	3.33%	50%
SCA Analysis	Time/Freq Domain		**Time, Freq**	Time	Time, Freq	Time, Freq	Time, Freq	Time
	CPA MTD	Power	**390M & >1.25B(>178,000x)**	1B (>100,000x)	>1B (125,000x)	8M (4210x)	>100K (20x)	>10M (2500x)
		EM	**248M & >1.25B(>138,888x)**	1B (>100,000x)	>1B (>83,333x)	6.8M (136x)	-	-
	Attack Mode		**Power/EM**	Power/EM	Power/EM	Power/EM	Power	Power

[a]Does not include regulator area/power, [b]Does not include Cap area, [c]Does not include DLDO area/power. Area overhead >150% with DLDO (estimated), [d]Power overhead includes the dropout voltage across current source, the extra bleed current drawn, SMC loop and TVTF power. Area overhead includes all the extra components without unprotected and calculated with respect to unprotected AES-256, [e]Power overhead = power with countermeasure – power for standalone AES at same frequency.

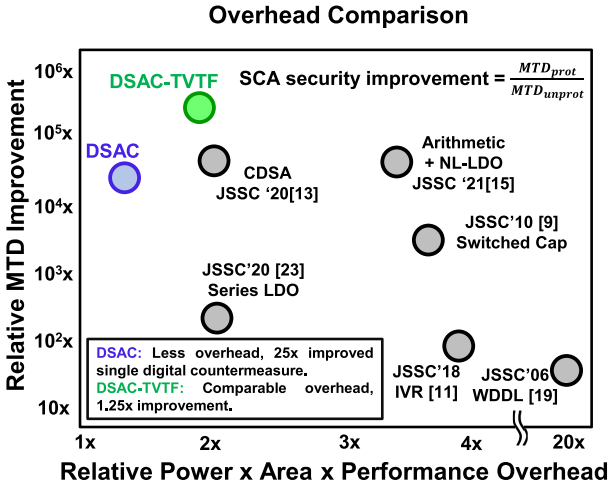


Fig. 23. Overhead comparison with the previous works.

(∼5×, due to the lower metal routing) compared to the global attenuation (∼41×), which is primarily through digital signature attenuation. Hence, although the power signature is completely suppressed by the global attenuation, the EM signature has both the components of which the local leakage can only be suppressed by a smaller factor. This analysis is shown in detail in a prior work [25], where the power signature is suppressed by a factor of 200×, but the EM signature is suppressed by a factor of 150×. A high metal layer for routing or higher level MiM capacitors is not used. However, inherently, EM leakage is more as defense techniques are different for different SCA. However, it is observed with the presence of extra security (TVTF); both the countermeasures achieve 1.25B MTD.

E. Comparison With State of the Art

This solution has reached 1.25B MTD, which is 25% greater than the existing state of the art. This is 178 000× greater than an unprotected solution in the case of CPA. Also, the MTD number is 138 888× greater than the unprotected counterpart in the case of CEMA. In modern IoT devices, where overhead is a concern and medium security is required, DSAC-AES-256 solution can be enabled, which is a lower overhead but effective solution. A brief comparison with respect to the existing state of the art is presented in Table I. Power consumption at 10-MHz frequency is tabulated in Table I. It is observed that DSAC consumes ∼0.2 mW, which is 33% greater than unprotected implementation, and DSAC-TVTF takes ∼50% greater average power (0.227 mW) with respect to unprotected implementation. DSAC and DSAC-TVTF take 0.19- and 0.238-mm^2 silicon areas in the test chip, respectively, which is 28% and 52% greater than unprotected implementation. It should be noted that other implementations are fabricated in different technology nodes, such as 14 or 130 nm. Overhead might change when we change the technology nodes. Fig. 23 describes a pictorial depiction of relative MTD improvement with respect to relative power, area, and performance overhead. We define the x-axis as the multiplication of all the relative overheads. Syn-STELLAR using DSAC-TVTF improves the overall countermeasure state of the art by 25% with a comparable overhead and single strategy digital countermeasure by 25× with less overhead using only DSAC.

VII. CONCLUSION

Syn-STELLAR provides power and EM side-channel attack immunity using DSAC along with TVTF. It advances two different types of physical and generic countermeasures

(attenuation-based and switch capacitor-based) that are proven to be best among the silicon verified implementations by making them digital-friendly and combines them together to achieve >1.25B MTD for the first time against both correlational power and EM side-channel attack, which is 25% greater than the existing state of the art. Only DSAC strategy gives high security too (25× improvement over state of the art for a single digital-friendly solution) and can be used as a countermeasure for IoT devices due to its lightweight implementation. These solutions are scalable over technology nodes barring the capacitors. DSAC and TVTF are digital in nature barring the capacitors. Some standard cell libraries have power gates, which can be used as switches or CS. Most of the circuits can be easily designed with standard digital APR flow. The same hardware description language (HDL) code can be used, a tool that automatically takes care of scaled technology nodes. Hence, it does not require much manual design effort to scale down when the technology node changes. Moreover, it can be placed on top of an encryption engine. It is clear that no design change is required for this portable feature in case of higher order implementation or different encryption engines. Syn-STELLAR does not have any performance degradation, and being a generic solution, it can be used over any encryption engine as a wrapper around it.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO'99* (Lecture Notes in Computer Science), vol. 1666, M. Wiener, Ed. Berlin, Germany: Springer, Aug. 1999, pp. 388–397.

[2] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs," in *Proc. CT-RSA*. Tel Aviv, Israel: Tel Aviv Univ., 2016.

[3] C. Paul Kocher, "Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems," in *Advances in Cryptology—CRYPTO'96* (Lecture Notes in Computer Science), vol. 1109, N. Koblitz, Ed. Berlin, Germany: Springer, Aug. 1996, pp. 104–113.

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

[5] D. Das, A. Golder, J. Danial, S. Ghosh, A. Raychowdhury, and S. Sen, "X-DeepSCA: Cross-device deep learning side channel attack," in *Proc. 56th ACM/IEEE Design Automat. Conf. (DAC)*, Jun. 2019, pp. 1–6.

[6] A. Golder, D. Das, J. Danial, S. Ghosh, S. Sen, and A. Raychowdhury, "Practical approaches toward deep-learning-based cross-device power side-channel attack," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2720–2733, Dec. 2019.

[7] *TEMPEST Attacks Against AES*, Fox-IT, Fremont, CA, USA, 2015.

[8] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2009, pp. 64–65.

[9] 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.

[10] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "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] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," *IEEE J. Solid-State Circuits*, vol. 53, no. 8, pp. 2399–2414, Aug. 2018.

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

[13] D. Das *et al.*, "EM and power SCA-resilient AES-256 through >350× current-domain signature attenuation and local lower metal routing," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, Jan. 2020.

[14] R. Kumar *et al.*, "A SCA-resistant AES engine in 14 nm CMOS with time/frequency-domain leakage suppression using non-linear digital LDO cascaded with arithmetic countermeasures," in *Proc. IEEE Symp. VLSI Circuits*, Jun. 2020, pp. 1–2.

[15] R. Kumar *et al.*, "A time-/frequency-domain side-channel attack resistant AES-128 and RSA-4K crypto-processor in 14-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 56, no. 4, pp. 1141–1151, Apr. 2021.

[16] 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. Eur. Solid-State Circuits*, Sep. 2002, pp. 403–406.

[17] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Cryptographic Hardware and Embedded Systems—CHES 2006* (Lecture Notes in Computer Science). Berlin, Germany: Springer, Oct. 2006, pp. 232–241.

[18] 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.

[19] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style MDPL on a prototype chip," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science). Berlin, Germany: Springer, Sep. 2007, pp. 81–94.

[20] A. Poschmann, A. Moradi, K. Khoo, C.-W. Lim, H. Wang, and S. Ling, "Side-channel resistant crypto for less than 2,300 GE," *J. Cryptol.*, vol. 24, no. 2, pp. 322–345, Apr. 2011.

[21] B. Yu, X. Li, C. Chen, Y. Sun, L. Wu, and X. Zhang, "An AES chip with DPA resistance using hardware-based random order execution," *J. Semicond.*, vol. 33, no. 6, Jun. 2012, Art. no. 065009.

[22] A. Singh *et al.*, "Enhanced power and electromagnetic SCA resistance of encryption engines via a security-aware integrated all-digital LDO," *IEEE J. Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, Feb. 2020.

[23] 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. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2017, pp. 62–67.

[24] 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.

[25] 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. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2019, pp. 11–20.

[26] A. Shamir, "Protecting smart cards from power analysis with detachable power supplies," Patent U.S. 6507913 B1, Jan. 14, 2003.

[27] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side—Channel(s)," in *Proc. 4th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*. Berlin, Germany: Springer-Verlag, 2002, pp. 29–45.

Archisman Ghosh received the bachelor's degree in electronics and telecommunication engineering from Jadavpur University, Kolkata, India, in 2017. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Purdue University, West Lafayette, IN, USA, working with Prof. Shreyas Sen.

He was a Digital Design Verification Engineer with Samsung Semiconductor India R&D (SSIR), Bengaluru, India. His research interests include mixed-signal IC design and hardware security.

Mr. Ghosh, during his Ph.D., has been awarded the ECE Fellowship for academic excellence during 2019–2020. He has been serving as a Primary Reviewer for multiple reputed journals and conferences, including IEEE International Conference on VLSI Design (VLSID) and *Wireless Personal Communication* (WPC) (Springer).

Debayan Das (Student Member, IEEE) received the bachelor's degree in electronics and telecommunication engineering from Jadavpur University, Kolkata, India, in 2015. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Purdue University, West Lafayette, IN, USA, working with Prof. Shreyas Sen.

Prior to joining the Ph.D. degree, he worked as an analog design engineer at a startup based in India. He has interned with the Security Research Lab, Intel Labs, Hillsboro, OR, USA, over the summers of 2018 and 2020. He has authored/coauthored more than 30 peer-reviewed conferences and journals, including two book chapters and one U.S. patent. His research interests include mixed-signal IC design and hardware security.

Mr. Das was a recipient of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST) Best Student Paper Awards in 2017 and 2019 and the 3rd Best Poster Award in the IEEE HOST 2018. In 2019, one of his papers was recognized as a Top Pick in Hardware & Embedded Security published over the span of the last six years. During his Ph.D. degree, he has been awarded the ECE Fellowship from 2016 to 2018 and the Bilsland Dissertation Fellowship during the final year (2020–2021) for his outstanding overall achievements. He has been serving as a Primary Reviewer for multiple reputed journals and conferences, including IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS (TCAS-I), IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS (TCAD), *ACM Transactions on Design Automation of Electronic Systems* (TODAES), IEEE ACCESS, *IEEE Internet of Things Journal* (IoTJ), IEEE Engineering in Medicine and Biology Society (EMBC), and ACM Design Automation Conference (DAC).

Josef Danial (Student Member, IEEE) received the B.Sc. degree in computer engineering from Purdue University, West Lafayette, IN, USA, in 2018, where he is currently pursuing the master's degree with the SPARC Lab, as a Graduate Research Assistant.

He has two years of industry experience in automotive (Fiat Chrysler Automobiles, Auburn Hills, MI, USA) and IoT (Cisco Jasper, Santa Clara, CA, USA) companies. His research interests include machine learning, hardware security, and computer vision.

Vivek De (Fellow, IEEE) received the B.Tech. degree from IIT Madras, Chennai, India, in 1985, the M.S. degree from Duke University, Durham, NC, USA, in 1986, and the Ph.D. degree from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 1991, all in electrical engineering.

He is currently an Intel Fellow and the Director of Circuit Technology Research with Intel Labs, Hillsboro, OR, USA. He is responsible for providing strategic technical directions for long-term research in future circuit technologies and leading energy efficiency research across the hardware stack. He has 327 publications in refereed international conferences and journals with a citation H-index of 83 and 236 patents issued with 27 more patents filed (pending).

Dr. De received the Intel Achievement Award for his contributions to an integrated voltage regulator technology. He was a recipient of the 2019 IEEE Circuits and System Society (CASS) Charles A. Desoer Technical Achievement Award for "pioneering contributions to leading-edge performance and energy-efficient microprocessors & many-core system-on-chip (SoC) designs" and the 2020 IEEE Solid-State Circuits Society (SSCS) Industry Impact Award for "seminal impact and distinctive contributions to the field of solid-state circuits and the integrated circuits industry." He received the Best Paper Award at the 1996 IEEE International ASIC Conference and nominations for Best Paper Awards at the 2007 IEEEACM Design Automation Conference (DAC) and 2008 IEEE/ACM International Conference on ComputerAided Design (ICCAD). He also coauthored a paper nominated for the Best Student Paper Award at the 2017 IEEE International Electron Devices Meeting (IEDM). One of his publications was recognized in the 2013 IEEE/ACM Design Automation Conference (DAC) as one of the "Top 10 Cited Papers in 50 Years of DAC." Another one of his publications received the "Most Frequently Cited Paper Award" in the IEEE Symposium on VLSI Circuits at its 30th Anniversary in 2017. He was recognized as a Prolific Contributor to the IEEE International Solid-State Circuits Conference (ISSCC) at its 60th Anniversary in 2013 and a Top 10 Contributor to the IEEE Symposium on VLSI Circuits at its 30th Anniversary in 2017. He received the Outstanding Evening Session Award at the 2018 International Solid-State Circuits Conference (ISSCC). He received the 2017 Distinguished Alumnus Award from IIT Madras. He has served as an IEEE/EDS Distinguished Lecturer in 2011 and an IEEE/SSCS Distinguished Lecturer from 2017 to 2018. He is also an IEEE/CASS Distinguished Lecturer for the term 2020–2022.

Santosh Ghosh received the Ph.D. degree from IIT Kharagpur, Kharagpur, India, in 2011.

He completed his post-doctoral studies from the Computer Security and Industrial Cryptography Group (COSIC), KU Leuven, Leuven, Belgium, in the area of cryptographic hardware and side-channel attacks. He is currently a Research Scientist with Intel Labs, Hillsboro, OR, USA. He has coauthored about 65 research publications in refereed international conferences and journals with a citation H-index of 21 and 20 issued with other 51 more patents filed (pending). The primary focus of his research includes: 1) design and implement cryptographic hardware microarchitecture and RTL with the aggressive area, latency, and throughput constraints; multiple of them are already being deployed in high-volume Intel products; 2) investigate and develop timing, power, and EM side-channel countermeasures; and 3) collaborate with academic partners and provide cryptography and security guidance to Intel business units.

Shreyas Sen (Senior Member, IEEE) received the Ph.D. degree in ECE from Georgia Tech, Atlanta, GA, USA, in 2011.

He has over five years of industry research experience in Intel Labs, Hillsboro, OR, USA, Qualcomm, Austin, TX, USA, and Rambus, Los Altos, CA, USA. He is currently an Elmore Associate Professor of ECE & BME, Purdue University, West Lafayette, IN, USA. He is the inventor of the Electro-Quasistatic Human Body Communication (EQS-HBC), or Body as a Wire Technology, for which, he was a recipient of the MIT Technology Review top-ten Indian Inventor Worldwide under 35 (MIT TR35 India) Award. His work has been covered by 250+ news releases worldwide, invited appearance on TEDx Indianapolis, Indian National Television CNBC TV18 Young Turks Program, NPR subsidiary Lakeshore Public Radio, and the CyberWire podcast. He has authored/coauthored three book chapters, over 175 journal and conference papers, and has 15 patents granted/pending. He serves as the Director for the Center for Internet of Bodies (C-IoB). His current research interests span mixed-signal circuits/systems and electromagnetics for the Internet of Things (IoT), biomedical, and security.

Dr. Sen was a recipient of the NSF CAREER Award in 2020, the AFOSR Young Investigator Award in 2016, the NSF CISE CRII Award in 2017, the Intel Outstanding Researcher Award in 2020, the Google Faculty Research Award in 2017, the Purdue CoE Early Career Research Award in 2021, the Intel Labs Quality Award in 2012 for industry-wide impact on USB-C type, the Intel Ph.D. Fellowship in 2010, the IEEE Microwave Fellowship in 2008, the GSRC Margarida Jacome Best Research Award in 2007, and nine best paper awards, including IEEE CICC in 2019, 2021, and in IEEE HOST 2017–2020, for four consecutive years. His work was chosen as one of the top-ten papers in the hardware security field (TopPicks 2019). He serves/has served as an Associate Editor for IEEE SOLID STATE CIRCUITS LETTERS (SSC-L), *Frontiers in Electronics*, *IEEE Design & Test*, an Executive Committee Member of the IEEE Central Indiana Section and a Technical Program Committee Member of the ACM Design Automation Conference (DAC), the IEEE Custom Integrated Circuit Conference (CICC), Design, Automation and Test in Europe (DATE), the ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED), the International Conference on Computer-Aided Design (ICCAD), the International Test Conference (ITC), VLSI Design, among others.