Exploiting Clock-Slew Dependent Variability in CMOS Digital Circuits Towards Power and EM SCA Resilience

Archisman Ghosh*, Md. Abdur Rahman*, Debayan Das†, Santosh Ghosh‡, and Shreyas Sen*
*School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN, USA
†Indian Institute of Science, Bangalore, India
‡Intel Labs, Intel Corporation, Hillsboro, OR, USA

***Abstract*—Mathematically secured cryptographic implementations leak critical information in terms of power, EM emanations, etc. Several circuit-level countermeasures are proposed to hinder side channel leakage at the source. Circuit-level countermeasures (e.g., IVR, STELLAR, WDDL, etc) are often preferred as they are generic and have low overhead. They either dither the voltage randomly or attenuate the meaningful signature at V_{DD} port. Although any digital implementation has two generic ports, namely clock and V_{DD}, circuit-level countermeasures primarily focus on V_{DD} port, and countermeasures using the clock are mainly unexplored. System-level clock randomization is ineffective due to post-processing techniques. This work, for the first time, presents clock-based countermeasures by providing a controlled slew that exploits the inherent variability of digital circuits in terms of power consumption and transforms power/EM emanation into a complex function of data and slew. Due to this, minimum traces-to-disclosure (MTD) improves by 100× with respect to the unprotected one. Moreover, the slewed clock reduces the leaky frequency, and the clock randomization countermeasure is more effective as it becomes more difficult to post-process in the frequency domain. Clock slew and randomization together have a cumulative effect (1800x) more than the multiplication of individual techniques (100x & 5x respectively). In brief, this paper presents a clock-level generic synthesizable countermeasure technique that improved the minimum-traces-to-disclosure (MTD) by 1800× and incurs only 11$\%$ area overhead, $<3\%$ power overhead (measured) and $<6\%$ performance overhead (measured). Moreover, this can be easily combined with other power-port-based mitigation techniques for enhanced security.**

***Index Terms*—Hardware security, side-channel attacks, correlational power analysis, electromagnetic leakage, AES-256, TVLA, generic countermeasure, clock-based countermeasure, clock-slew, clock randomization.**

I. Introduction

Cryptographic algorithms that are considered mathematically secure can still inadvertently leak critical side-channel information, such as correlated power [1], electromagnetic (EM) emanations [2], timing [3], and cache hits/misses, etc. These side-channel leaks can lead to physical side-channel attacks (SCA). The presence of such side-channel information greatly reduces the time complexity of extracting a secret key from a cryptographic IC. For instance, the once-thought highly secure AES-256 encryption engine can be broken with a reduced time complexity of 2^{13} rather than the originally believed 2^{256}. Recent observations indicate that the AES-256 key can be easily intercepted from a distance using a low-cost EM probe, even from a meter away, without requiring detailed knowledge of the circuit or PCB implementation [4]. This underscores the significant threat EM side-channel attacks pose to integrated circuits.

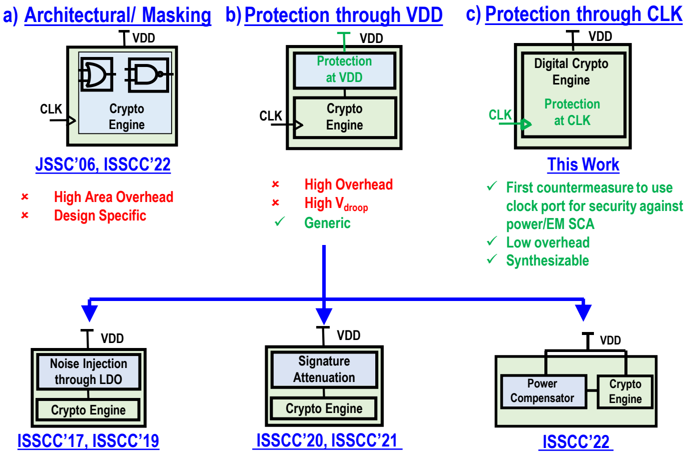


Fig. 1: State-of-the-art countermeasures for cryptographic circuits.

An attacker needs to collect power/EM traces from the cryptographic engine for a power/EM side-channel attack. Ciphertext is publicly available. Hamming weight (HW)/ Hamming Distance (HD) is calculated for all keybytes. Now, calculated HW/HD can be correlated with corrected traces. After enough traces, the correct key is revealed. This is the basic idea behind the Correlational Power Attack (CPA)/ Correlational EM attack (CEMA). It should be noted that these particular types of attacks are very generic in nature, and the attacker needs little knowledge of the architectures of the embedded crypto he/she is interested in.

Different types of countermeasures are well-explored in the side-channel community to thwart the threat of power/EM side-channel attacks. They can be divided into three broad categories: a) Masking/architectural countermeasure, b) physical countermeasure using V_{DD} port, and c) physical countermeasure using clock port, which is relatively unexplored. Masking /architectural countermeasures [5], [6] are well-explored in this context. These countermeasures provide provable security and

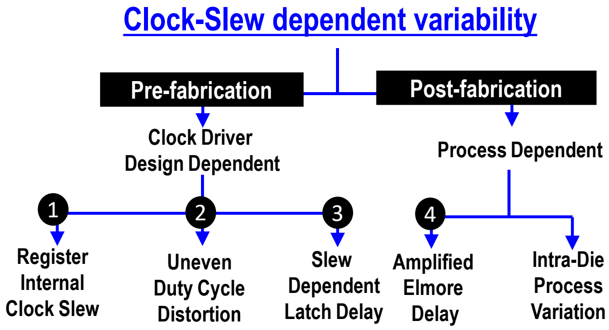

Clock-Slew dependent variability
Pre-fabrication
Post-fabrication
Clock Driver Design Dependent
Process Dependent
1
2
3
4
Register Internal Clock Slew
Uneven Duty Cycle Distortion
Slew Dependent Latch Delay
Amplified Elmore Delay
Intra-Die Process Variation

Fig. 2: Contributing factors to clock slew dependent variability which thwarts the side channel leakage.

are digital in nature. However, they often cause very high overhead. More importantly, these types of countermeasures are also design-specific, which implies that changing architectures/algorithms will require a complete redesign of the technique, which may not be preferred from an industry point-of-view. Recently, generic circuit-level countermeasures have gained popularity as they are considerably low area-overhead and design-agnostic. These countermeasures use V_{DD} port to dither/attenuate the meaningful leakage or compensate for power droop. However, they often have high droop (hence, high power overhead and empirically less power overhead than architectural countermeasures) as they utilize/modify power delivery networks as a defense mechanism. A typical digital cryptographic core has two controllable ports, namely, V_{DD} and clock. Most of the circuit-level countermeasures have primarily utilized the V_{DD} port to reduce the side-channel leakage. Related to the clocking port, well-studied system-level clock frequency randomization techniques have been rendered ineffective with edge-alignment of power traces based post-processing/ frequency domain attacks [7] as explained in section II.C. However, the impact of circuit-level changes in the clocking circuitry and its device-circuit-system level interactions with inherent properties of digital circuits and its impact on side channel leakage remains unexplored. Another critical requirement for the countermeasure is to make it fully synthesizable for scalability across different technology nodes. This work, for the first time, exploits the inherent variability of CMOS digital circuits by providing a controlled slewed clock and demonstrates an extremely low-overhead technique for immunity against power and EM SCA. If this is aided by clock randomization, frequency domain attacks become difficult. The combined effect of the individual countermeasures is more than the multiplication of improvement of individual techniques. These countermeasures can be easily integrated with any of the V_{DD} countermeasures to enhance SCA resilience.

The remainder of this article is organized as follows. We describe the related works on power and EM side-channel attack countermeasures in Section II. A detailed conceptual discussion of the slewing technique to thwart side-channel attacks (SCA) is presented in Section III. Section IV describes the system architecture and the implementation details of the two techniques: clock slewing and clock randomization. The efficacy of the countermeasure against CPA, CEMA, along with the test vector leakage analysis (TVLA), and the measurement setup is described in detail in section V before we conclude this article in section VI.

II. Related Works

Different countermeasures have been proposed with different side-channel analysis (SCA) techniques. We broadly classify these techniques into three categories: architectural/masking countermeasures, protection through V_{DD}, and protection through the clock port. We will discuss a few seminal works in each category first.

A. Power/EM SCA countermeasure using Architectural/masking

1st genre of these countermeasures is called architectural/masking countermeasures. These countermeasures include wave dynamic differential logic [8], additive masking techniques [9], [10], multiplicative masking [5], [11], heterogenious s-box [12], and threshold implementations [6] etc. These countermeasures offer provable security. Moreover, these countermeasures are fully synthesizable and are portable when transferred to a new technology node. However, they suffer from two important problems - 1) They often have very high overhead ($> 100\%$), and 2) They are not generic in nature. Masking techniques differ from algorithm to algorithm and vary significantly from software to hardware implementation. Circuit-level countermeasures solve this problem. They are often relatively low overhead and can be used with minimal modification on top of any crypto algorithm. Circuit-level countermeasures are gaining traction due to this reason. We discuss a few prominent circuit-level/physical countermeasures in the following subsection.

B. Protection through VDD port

As power side channel analysis is conducted through the V_{DD} port, having protection at V_{DD} port is intuitive. This is the intuition behind the physical SNR reduction-based countermeasures. These countermeasures are well explored in the circuit community but suffer from high droop-related overhead. it should be noted that these countermeasures are generic in nature and can be used on top of any crypto-system without changing the algorithm. These countermeasures include voltage regulator-based solutions, switched-capacitor current equalizer [13], ML-based targeted power compensation [14], [15] as well as signature attenuation. Voltage regulator-based solutions include the Integrated Buck Regulator (IBR) [16], [17]-based approach and the series Low-Dropout Regulator (LDO) with Loop Randomization (R-DLDO) [18], [19], both of which offer a moderate level of security ($< 10MMTD$) attributed to the incorporation of randomization techniques. Nevertheless, it is imperative to acknowledge that the IBR introduces substantial passive components, with the caveat that the Metal-Insulator-Metal (MiM) capacitor frequently emits important information through electromagnetic emanations.

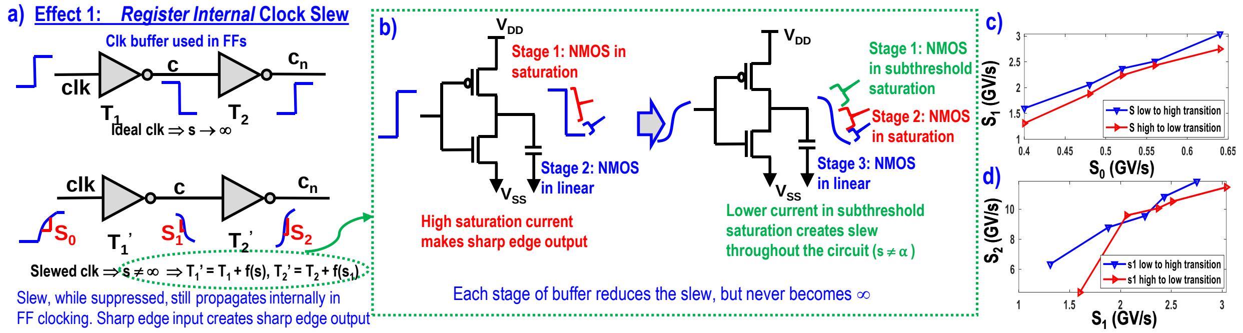

a) Effect 1: Register Internal Clock Slew
Clk buffer used in FFs
clk
c
c_n
T_1
T_2
Ideal clk ⇒ s → ∞
clk
c
c_n
S_0
T_1'
S_1
T_2'
S_2
Slewed clk ⇒ s ≠ ∞ ⇒ $T_1' = T_1 + f(s)$, $T_2' = T_2 + f(s_1)$
Slew, while suppressed, still propagates internally in FF clocking. Sharp edge input creates sharp edge output
b)
V_{DD}
Stage 1: NMOS in saturation
Stage 2: NMOS in linear
V_{SS}
High saturation current makes sharp edge output
V_{DD}
Stage 1: NMOS in subthreshold saturation
Stage 2: NMOS in saturation
Stage 3: NMOS in linear
V_{SS}
Lower current in subthreshold saturation creates slew throughout the circuit (s ≠ α)
Each stage of buffer reduces the slew, but never becomes ∞
c)
S_1 (GV/s)
3
2.5
2
1.5
1
0.4
0.45
0.5
0.55
0.6
0.65
S_0 (GV/s)
S low to high transition
S high to low transition
d)
S_2 (GV/s)
10
8
6
1
1.5
2
2.5
3
S_1 (GV/s)
s1 low to high transition
s1 high to low transition

Fig. 3: a) Slew is propagated through buffers of registers. b) We take an example of a 0-1 transition. For the ideal scenario, initially, NMOS is in saturation, and NMOS goes to a linear region. Initially, NMOS is in the subthreshold region, slowing down sharpness by buffer in the presence of a slewed clock. c) Simulated slew, $S1$ with respect to initial slew. d) Simulated slew, $S2$ with respect to $S1$. (c) and (d) reveal that slew is reduced but still remains while going through the buffers of registers.

Furthermore, the Digital LDO, inherently susceptible to information leakage, reveals critical data as voltage compensation closely aligns with the instantaneous current drawn by the cryptographic engine. Integrating noise injection and voltage/frequency modulation in Digital LDO yields an increased resistance of 6.8M MTD against power SCA. However, it is essential to note that employing LDO as a countermeasure against SCA often incurs a high overhead. A more robust security measure is achieved by implementing a Cascade of Non-Linear LDO (NL-LDO) with arithmetic countermeasures, attaining a security level exceeding 1B MTD against Correlation Power Analysis (CPA). Nevertheless, this approach is encumbered by a significant overhead attributed to LDO and lacks generality due to the specificities introduced by arithmetic countermeasures [12], [20]. Current Domain Signature Attenuation (CDSA) solves the problem of inherent leakage by series LDO. CDSA [21] achieves high MTD by using an analog cascoded current source as a power delivery circuit which provides high attenuation due to its high output impedance. This solution, for the first time, achieves $> 1B\ MTD$, but it is not synthesis-friendly. Syn-STELLAR [22] proposes a scalable signature attenuation-based solution which provides similar MTD ($> 1.25B\ MTD$) by cascading two solutions, namely Digital Signature Attenuation Circuit (DSAC) [23] and Time-Varying Transfer Function (TVTF) [24]. DSAC does not provide high attenuation compared to CDSA as the synthesizable realization of CS replicates source degenerated structure instead of cascoded structure, contributing to lower attenuation. Additional Ring Oscillator randomization-based power-supply noise along with TVTF helps to achieve higher security at the cost of high overhead.

C. Protection through Clock port

Any digital circuits, including cryptographic implementations, have two generic ports, namely V_{DD} and a clock port. It is intuitive to secure the power port against power/EM side-channel analysis. However, power/EM side channel mitigation through the clock is less explored. Existing clock-based SCA countermeasures can be divided into two broad categories, namely, a) system-level clock randomization techniques & b) non-ideal clocking techniques. We will discuss existing clocking countermeasures in detail in the subsequent subsections.

1) System-level Clock randomization techniques: System-level clock randomization techniques are well-explored [25], [26]. However, different post-processing techniques have been well-explored to bypass clock-randomization countermeasures. For example, this can be post-processed by trace alignment [7] with the help of a convolutional neural network (CNN). Brisfors et al. [27] suggest an attack on the first round of AES as that has the minimum effect of randomization. However, the attack is not straightforward as standard CPA does not work well [27] in this case. The authors utilized an MLP-based neural network for the attack. Tian et al. [28] have shown that traces can be aligned using horizontal alignment by detecting and aligning the appropriate peaks in the trace. The idea is to find an attack point and zoom into a particular cycle as per the template chosen earlier. The authors [29] have also shown that this processing technique is not the most effective when AES operates at higher frequency as higher frequency operation also causes amplitude changes. Tian et al. choose a vertical alignment technique for attack in their later work [29]. Several other techniques, such as sliding window-based integration techniques [30] and FFT-based frequency domain attack [31] techniques are well-explored to exploit clock randomization-based countermeasures. As our post-processing techniques, we focus on correlational frequency attacks initially proposed in [30], [32]. We often observe information leakage in a particular frequency (for a particular design), and frequency domain attacks effectively extract the correct key. We propose an attack utilizing a similar concept against clock-randomized AES as well which is one of the key contributions of this work. However, the clock randomization circuit becomes frequency domain attack-resistant when aided by the clock slewing technique explained in section V of the paper.

2) Non-ideal clocking techniques: Though we have implemented the clock slewing concept as a 65nm IC and demonstrated the efficacy of weak driving technique against power

& EM SCA, we also acknowledge that a similar technique (not at circuit level) is invented and discussed in [33], [34] independently. Patanjali et al. [34] proposes a Computer-Aided Design (CAD) technique to find the most vulnerable gate, which contributes maximum towards side channel leakage and changes the sizing of the gates to minimize the same. Sreekumar et al. [33] suggest a similar CAD flow for tuning of driver strength to minimize the power side channel leakage. It is important to note that though this work is conceptually similar, we explore circuit-level inherent variances due to slewed clock in fabricated IC for the first time. Moreover, this IC presents an increased efficacy of clock randomization techniques in the presence of clock slew. The theoretical explanation is presented in section III, and measured results have been presented in section V respectively.

III. Circuit Technique against Side-Channel Attack

First, we will discuss the effect of clock-slew-dependent variability of the digital circuit as a countermeasure, as shown in Fig. 2 in this section, followed by the effect on them on side-channel power traces. This section also presents a detailed analysis of functional correctness and a discussion on tool-level modification. We must note that we define slew $S = \frac{dv}{dt}$. Hence $S \propto \frac{1}{Transition\ time}$.

A. Register Internal Clock Slew

If clock slew is introduced, slew propagates through the internal buffers of flip-flops (FF). Propagating through buffers reduces the slew but never makes it to the near-ideal clock with a very high slew, as TSMC 65nm FF used here just has two internal buffers as shown in Fig. 3(a). When slew is provided at the clock port, it gradually improves but still persists. For example, if we observe a 0 to 1 transition in Fig. 3(b) with an ideal clock, NMOS is in saturation region drawing more current initially as $V_{DS} > V_{GS} - V_{tn}$. Here, V_{DS}, V_{GS}, and V_{tn} imply drain-to-source voltage, gate-to-source voltage, and threshold voltage for NMOS respectively. When V_{DS} reduces, NMOS reaches the linear region in stage 2. For this ideal scenario, we calculate fall time, t_f, which has two components, say t_{f1} and t_{f2}, due to the contribution of saturation region and linear region, respectively. For saturation region,

$$C_L \frac{dV_{out}}{dt} + \frac{k_n}{2}(V_{GS} - V_{tn})^2 = 0 \tag{1}$$

Where k_n is constant for NMOS derived from device characteristics and C_L is the output capacitance of the gate. It is important to note that here $V_{GS} = V_{DD}$. Integrating over time t_1 (corresponding $\mathrm{V_{out}} = (\mathrm{V_{DD}} - \mathrm{V_{tn}})$) to t_2 (corresponding to $V_{out} = 0.9V_{DD}$), we obtain

$$\begin{aligned} t_{f1} &= 2\frac{C_L}{k_n(V_{DD} - V_{tn})^2}\int_{V_{DD}-V_{tn}}^{0.9V_{DD}} dV_{\text{out}} \\ &= \frac{2C_L(V_{tn} - 0.1V_{DD})}{k_n(V_{DD} - V_{tn})^2} \end{aligned} \tag{2}$$

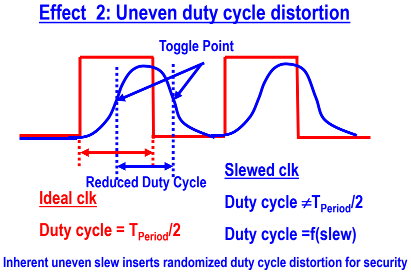


Fig. 4: Duty cycle is distorted due to clock slew.

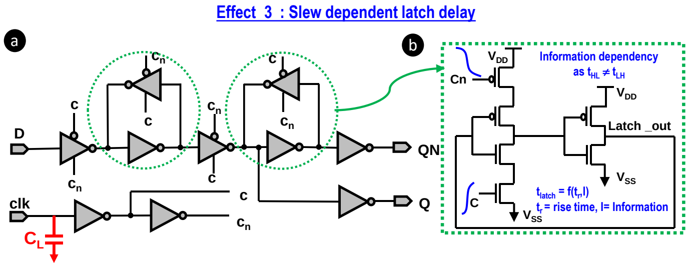

Effect 3 : Slew dependent latch delay
a
b
D
clk
C_L
c
c_n
QN
Q
V_DD
Cn
C
Information dependency as t_HL ≠ t_LH
Latch _out
V_SS
t_latch = f(t_r,I)
t_r = rise time, I= Information

Fig. 5: Latch delay is a function of slew. Latching times of 0 and 1 are different as they depend on posedge and negedge of the clock, which is driven by the different buffers. This leads to the dependency of latch delay by slew.

Similarly, we can solve for the linear region to calculate t_{f2}.

$$\begin{aligned} &C_L \frac{dV_{\text{out}}}{dt} + k_n\left[(V_{DD} - V_{tn}) \cdot V_{\text{out}} - \frac{V_{\text{out}}^2}{2}\right] = 0 \\ &\Rightarrow t_{f2} = \frac{C_L}{k_n(V_{DD}-V_{tn})}\int_{V_{DD}-V_{tn}}^{0.1V_{DD}} \frac{dV_{\text{out}}}{\frac{V_{\text{out}}^2}{2\left(V_{DD}-V_{tn}^{th}\right)} - V_{\text{out}}} \end{aligned} \tag{3}$$

Now, for the non-ideal clock, the scenario changes. Initially, NMOS is in the subthreshold saturation region as $V_{GS} < V_{tn}$, hence drawing a negligible amount of current, creating a new component in fall time (say t_{f0}). Moreover, t_{f1} is increased as V_{GS} slowly increases towards V_{DD} and $V_{GS} \leq V_{DD}$. Hence, t_f increases (similar logic holds for rise time too). In other words, the slew is increased with respect to the ideal scenario when it propagates through buffers.

It is important to note that slew $S1$ and $S2$ (as shown in Fig. 3(a)) are different, causing different latch times as discussed in the later part of this section. We simulate slew at different nodes of clock buffers of each flipflop to verify the intuition of slew. We observe that the slew is gradually improving from 1st inverter to the final inverter of the clock buffer (Fig. 3(c-d)) as expected. Slew provided at the clock port varies in the range of 0.4-0.6 GV/s. It is modified to 1.5-3 GV/s based on low-to-high or high-to-low transition as shown in Fig. 3(c). Slew is further improved to 4-12 GV/s when propagated through the final buffer, as shown in Fig. 3(d).

B. Uneven Duty Cycle Distortion

It is clear that a slewed clock never becomes ideal when propagated through 2 buffers. The toggle points of a flip-flop (FF) are determined by the presence of slews. The distortion of the duty cycle (as shown in Fig. 4) is influenced by the rise

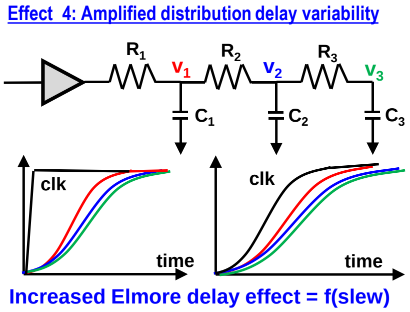

Effect 4: Amplified distribution delay variability
R_1
V_1
R_2
V_2
R_3
V_3
C_1
C_2
C_3
clk
time
clk
time
Increased Elmore delay effect = f(slew)

Fig. 6: Effect 4: Elmore delay is amplified by slew, which helps SCA resilience.

time (t_r), particularly in scenarios with high input slew (low slope). As shown earlier, rise time t_r and fall time t_f never become ideal when propagated through buffers or different clock paths. Rather, a high input slew causes a clock swing that is less than full-scale which is further aided by path delay as different slew follows different paths. This implies clock swings are not only less than rail-to-rail they differ from FF to FF, which are utilized as state registers of AES. As full swing differs, the duty cycle changes which in turn changes the timing between various leakage points in the power supply. As a result, the leakages from different flip-flops do not accumulate in an aligned fashion in the power supply at a particular time sample. Rather, information leakage is distributed over a large number of time samples, making it harder to exploit. Hence, this architecture is more challenging to exploit for attacks.

C. Slew Dependent Latch Delay

Power side channel leakage depends on state register switching. In other words, the transition between $1 \rightarrow 0$ and $0 \rightarrow 1$ causes leakage. The hamming distance-based attack model relies on these transitions. Hamming weight-based attack model relies on numbers of 1s in the state register. With an ideal clock, latching time depends solely on data as $t_{latchH \rightarrow L} \neq t_{latchL \rightarrow H}$. However, as slew is introduced propagated slews ($S1$, $S2$) are different at c and c_n as shown in Fig. 3(a). Fig. 5 shows an example. The utilized FF has two latches. If we think about 2nd latch as shown in Fig. 5(b), it is clear that latching 1 (or high) depends on $S2$ however, latching 0 (low) depends on slew at c ($S1$). A similar situation happens in 1st latch, too. These vary further as the slew reaches different flip-flops differently. Earlier, the latching time was similar; hence, they would contribute to the leakage point at the same time sample and power profile would solely depend on information. However, modified latching time becomes a function of data and slew, which creates extra variance in power traces.

D. Post-fabrication Artifacts: Amplified Elmore Delay Variability & Intra-Die Variation

The above-mentioned three pre-fabrication artifacts are aided by two other post-fabrication artifacts: Elmore delay variation and intra-die process variation. When a signal propagates through long metals, it gets distorted due to the non-negligible resistance of the wires, which initiates the Elmore effect [35]. In our design, the clock propagates throughout the design. As it is already slewed, it gets further slewed due to the Elmore effect (Fig. 6). This effect is further aided by an intra-die variation to enhance the variability in digital circuits towards side-channel resilience.

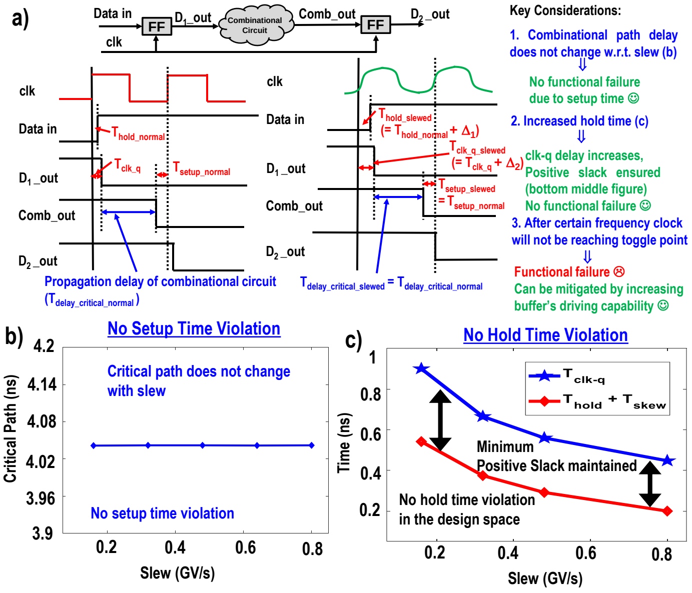


Fig. 7: a) No functional failure due to setup and holding time violations. Functional failure is possible due to insufficient time to reach the toggle point, causing a performance trade-off. b) The critical path does not change with slew, preventing any setup violation. c) Increased slew increases slew-dependent skew. However, the clk-q delay always increases and is greater than the hold time requirement (hold time +skew) in the entire design space, causing no functional failure related to hold time.

E. Constraints on Synthesis & Automatic Place and Route (APR) Tool

Our parallel AES design is synthesized with Synopsys design compiler targetting TSMC 65nm library. We place and route using the Cadence Innovus APR tool. The targetted critical path is 10ns, which is met with positive slack for all the paths. As our critical path is 10ns and the skew requirement is 10% of the same, it is easily met without extra buffer insertion in the clock path. This is important because buffers are often placed to counteract timing violations if we synthesize with very high frequency. However, inserting buffers drastically reduces the effect of slew. In this IC, the effect of buffer insertion to meet high frequency is not explored which can be done as part of future work. Cadence Innovus does not indicate any timing violation. The encryption throughput is 0.9Gbps, which is enough for our SCA resilience demonstration purpose.

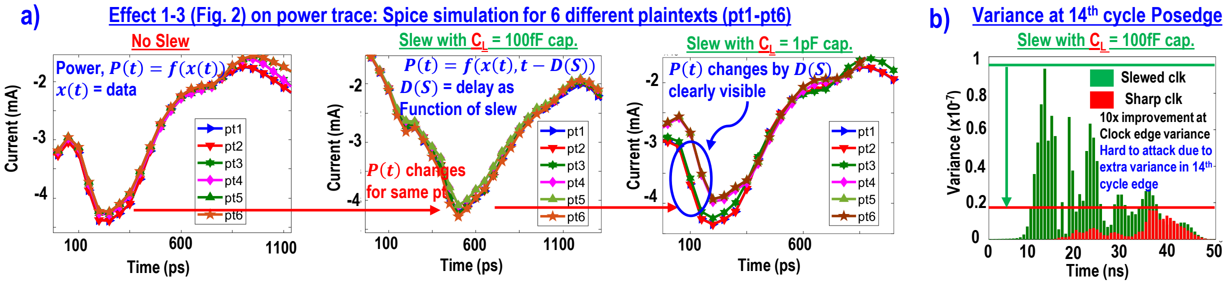


Fig. 8: a) spice simulation shows effects 1-3 in power trace. This power trace is taken for six different plaintexts in the 14th round with nominal slew, slew with 100fF load cap, and slew with 1pF load cap. b) Variance in the 14th cycle power trace shows the 10x improvement over the sharp clock.

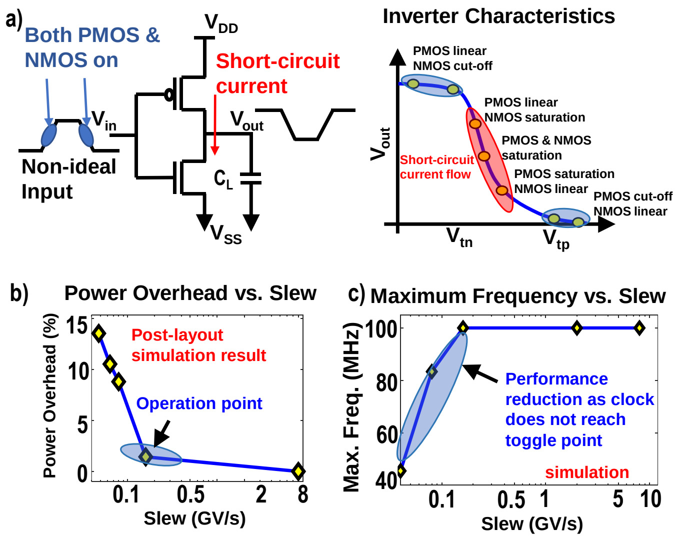


Fig. 9: a) Short circuit current is introduced when both PMOS and NMOS is on in CMOS devices. This overhead is increased for slew. b) Power overhead due to short-circuit current on our designed AES-256 parallel architecture. The operating point has $< 3\%$ overhead. c) Maximum frequency is reduced if the clock does not reach the toggle point due to excessive slew. Simulated performance overhead varies from 0% - 53% based on slew.

F. Functional Correctness

Changing clocking network comes up with the risk of timing failures. First, we discuss the possibility of timing violation and obvious trade-offs related to it. Combinational path delay does not vary with slew (Fig. 7(a)) as the delay of a gate is a device property, and it does not depend on input. We simulate the critical path with a different slew in the clock. It is observed that setup time does not change for slew, as shown in Fig. 7(b). Setup depends on the path delay, which depends on combinational cells placed on a path, which is a device property. However, increased slew increases hold time (t_{hold}). Intuitively, data should be held longer because the clock is delayed. However, we know that $t_{clk\_q} + t_{comb} > t_{hold} + t_{skew}$ is required to avoid hold time violation. Increased slew increases skew (t_{skew}) as well as t_{clk_q}. Data will be latched later due to the slewed clock increasing t_{clk_q}. It is always ensured in the design space that $t_{clk\_q} > t_{hold} + t_{skew}$, which ensures positive slack. This, in turn, ensures no hold time violation, as shown in Fig. 7(c). However, one important point to note is that if the clock is slewed too much, it may not reach the toggling point for flip-flop at a higher frequency, causing functional failure. This is the performance trade-off paid to gain the default security using clock-slewed countermeasure. Performance trade-off can be mitigated with stronger buffer insertion at the cost of security. The measured performance trade-off is presented in section V.B.

G. Power & performance overhead with Clock Slew

Short–circuit power is the key contributing factor in leakage power as clock slew is introduced. This phenomenon can be explained by taking a simple example of an inverter. During a transient on the input signal of an inverter, as shown in Fig., there will be a short period in which both NMOS and PMOS transistors will conduct simultaneously, causing a current flow through the direct path existing between power V_{DD} and ground terminals. In a static CMOS inverter, this current flows as long as the input voltage is higher than an NMOS threshold voltage (V_{tn}) above ground and lower than a PMOS threshold voltage (V_{tp}) below the power supply, as shown in Fig. 9(a). This is causing $\sim 1\%$ power overhead as demonstrated in Fig. 9(b) from post-layout extracted netlist (PEX) spice simulation of the implemented AES-256 parallel architecture. Similarly, performance simulation is done with different slew rates on post-layout extracted netlist. It should be noted that AES RTL is synthesized with a 100MHz target frequency. We observe it can not be operated at the targetted frequency when slew is > 0.1 GV/s as shown in Fig. 9(c). In those cases, a slewed clock cannot reach the toggle point of transistors, causing functional failure.

H. Effect of Clock Slew on Side-Channel Power Traces

To analyze the effect of clock-slew pre-silicon, we simulate power traces of AES-256 with the same key and different plaintexts in spice. Six such example traces with the same key and six different plaintexts are plotted in Fig. 8(a) to demonstrate the effect of clock slew. It should be noted that

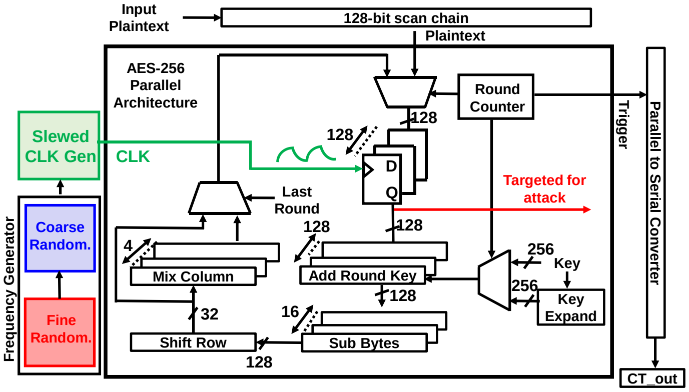


Fig. 10: Full system architecture of the design.

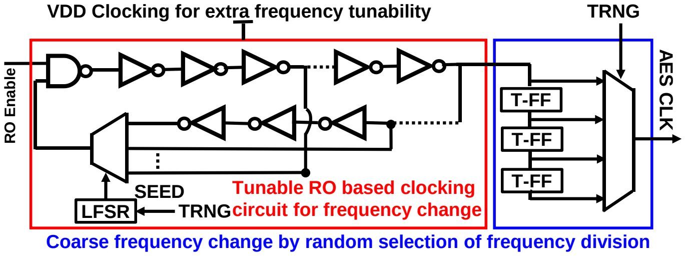

VDD Clocking for extra frequency tunability
TRNG
RO Enable
AES CLK
T-FF
T-FF
T-FF
SEED
LFSR
TRNG
Tunable RO based clocking
circuit for frequency change
Coarse frequency change by random selection of frequency division

Fig. 11: Clock randomization circuit. A tunable RO is used for fine randomization (shown in red). This is randomly divided by a frequency division circuit (shown in blue), which acts as a coarse frequency randomizer.

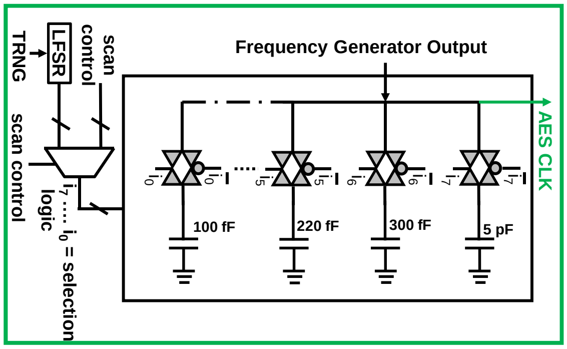


Fig. 12: Slewed clocking circuit. Clock slew is created by loading the clock node with different capacitors and switches. Note that other techniques, such as a weak clock buffer, can be used as a slewing technique as well.

these are simulated traces, and hence, only 1st 3-effects are visible here. We do not see any effect of amplified Elmore delay and intra-die process variation. We focus on the 14th cycle, which is the attack point for our design. In the presence of nominal slew, we observe that power traces are a function of information and, hence, can be attacked using Correlational Power Attacks (CPA). This 1:1 relation between information and power trace is broken once we introduce the clock slew. The power trace slightly changes when the slew is introduced with a 100fF load capacitor from purely information-dependent traces. When we introduce further slew, as shown in Fig. 8(a), we clearly observe different plaintexts have very different power profiles from the nominal slew one. Power profile at time point t, (P(t)) is data-dependent (x(t)) which is the basis of SCA (Hamming Distance (HD) model-based SCA detects $\frac{dP}{dx}$) in the absence of slewed clock. Due to clock slew, power consumption (P'(t) =f(x(t),t-D(s))) is dependent on slew (s)-related delay D(s), which is a non-linear function of the input data (x(t)). Significant SCA resilience could be achieved if $\frac{dP}{dx} \ll \frac{dP'}{dx}$.

We further plot the standard deviation of trace (σ_T) with nominal slew and slew with 100fF load capacitor to observe the statistical implications of leakage when we introduce slew. MTD can be approximated by the following equation 4 [32], [36].

$$MTD = k_1 * \frac{1}{\rho_{TH}^2} \approx k_1 * \left(1 + \frac{1}{SNR}\right) \tag{4}$$

Here, k_1 is a constant. ρ_{TH} implies peak pearson correlation co-efficient between trace & Hamming Distance based attack model. Here, signal-to-noise ratio (SNR) can be represented by equation 5.

$$SNR = \frac{\sigma_T^2}{\sigma_{\text{Noise}}^2} \tag{5}$$

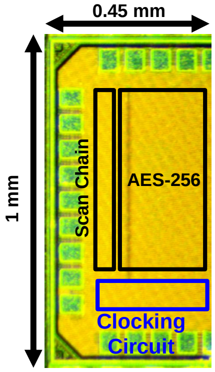
σ_T is increasing 10× in the positive clock edge of the 14th cycle, which is the attack point for our case as shown in Fig. 8(b). This improvement leads to 100× estimated improvement in MTD.

IV. System Architecture

Implemented AES-256 follows 128-bit datapath parallel architecture. The full system consists of a frequency generator followed by a slewed clock generator, as shown in Fig. 10. The frequency generator randomly creates the frequency before getting slewed by the slewed clock generator. 128-bit scan chain is used to send plaintext while testing. A trigger signal is generated at the end of the 14th round. Ciphertext is stored in a parallel to serial converter and taken out serially for functional correctness verification of each plaintext.

The clock randomization circuit or frequency generator circuit consists of 2 components, a coarse randomizer circuit, and a fine randomizer circuit, as shown in Fig. 11. It uses a Tunable Ring Oscillator (RO)-based clocking circuit. A multiplexer is used to select the number of stages of the ring oscillator, which creates different frequencies. We have eight configurations between 49 and 81 stages, which the MUX can randomly select. The MUX is controlled by a Linear Feedback Shift Register (LFSR). LFSR is seeded by an external true random number generator (TRNG) for further randomization. The clock generated by the fine randomizer is randomly frequency divided by a 3-stage toggle FF-based divider circuit as shown in Fig. 11. An external TRNG can randomly select between levels of frequency division to create coarse randomization.

The generated randomized clock is fed through a slewed clocking circuit as shown in Fig. 12. The slewed clocking circuit is realized by using a switched capacitor circuit. It has multiple switches implemented using the transmission



Test Chip	Process	65nm CMOS Low Power
	Package	Wire-bond (Glob-Top Encapsulation)
AES-256 Core	Performance	0.8V/10MHz/0.16mW
	Architecture	128b Datapath (parallel AES)
	Supply Decap	50 pF MOS Cap (0.005 mm^2)
	Active Area	0.1 mm^2
	Scan Chain	387b
Clocking Circuit (Slewed Clock+Clock Gen)	Operating Voltage	0.72V
	Active Area	0.011 mm^2
	Current (slewed clk)	627uA (Driving 10MHz clock)
	Current (slewed clk+randomized clk generator)	649uA (Tuned at 10MHz clock)
	Scan Chain	39b

Fig. 13: Fabricated IC micrograph & specification.

gates. A combination of different capacitors can be selected using a multiplexer to create different levels of slew. Different load capacitors are connected through the transmission gates. There is room for randomization for slewed clock generator circuits. However, in this work, we just show the efficacy of one particular slew. It should be noted that there are other techniques to create the clock slew. For example, we can use a weaker buffer instead of a switch capacitor circuit to generate a clock slew with even less power overhead than our circuit. Note that the main goal of this work is to show the efficacy of the slewing technique in silicon, while optimization of the slewing techniques could be pursued as part of future work. In brief, clock randomization can be rendered ineffective using frequency domain attacks or post-processing techniques. However, the presence of the slewed clock makes clock randomization more effective even in the presence of the post-processing techniques which we demonstrate in the next section.

V. Measurement Results

The IC micrograph and specification are shown in Fig. 13. The IC is fabricated with TSMC 65nm CMOS technology. Packaging is chip-on-board with glob-top encapsulation. The IC is operated with 0.8V and 10MHz frequency and consumes 0.16mW power. AES-256 architecture is 128b parallel datapath AES 256, which takes 14 cycles for encryption. A 50pF capacitor is used for the supply decoupling capacitor. The active area is 0.1 mm^2, and 387 bits of scan chain are used to configure the AES with key and plaintext. The clocking circuit has an active area of 0.011 mm^2. Clock slewing circuit draws 627μA. 39-bit scan chain is used to configure the clocking circuit. It should be noted that this IC demonstrates the efficacy of the technique against the countermeasure. Improved slewing clocking circuit (e.g., weaker buffer) will consume less power even at the same security level.

A. Measurement setup & Security assumptions

Side channel attack setup is presented in Fig. 14. 1Ω resistance is used as the current sensor. The current trace is collected using a 5GSps oscilloscope. We use a 10mm H-probe for collecting EM traces. This is further amplified by a 40dB

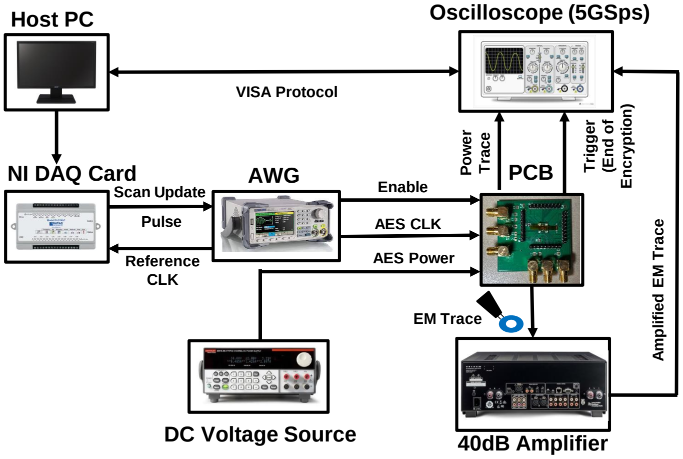


Fig. 14: Attack setup for side channel experiments.

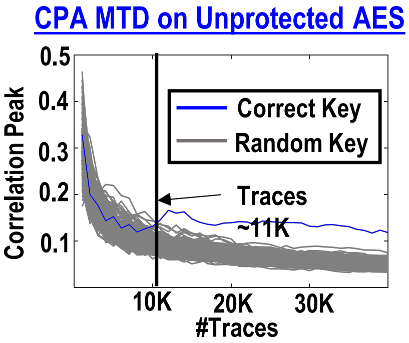


Fig. 15: Correlational power analysis on unprotected AES-256. The correct key is revealed within 11K traces.

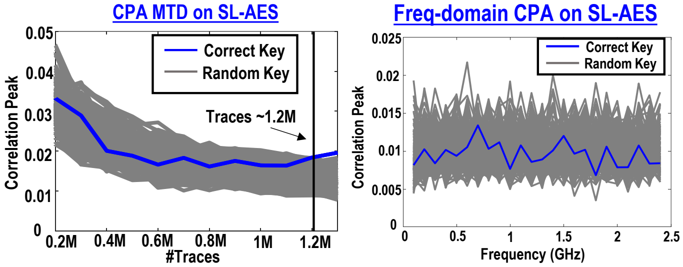


Fig. 16: Correct key is revealed with 1.2M individual traces. Each trace are averaged with 1000 encryptions. Frequency domain CPA does not reveal any correct key with 1.2M traces.

amplifier before being fed into the oscilloscope. The collected trace is sent to the Host PC using the VISA protocol for CPA/CEMA. PC also controls the data acquisition card (DAQ) to send the input to the IC. AWG is used for the enable signal. A DC voltage source is used for powering up the IC. Note that it is essential to average from an attacker's point of view against any physical countermeasure to reduce the physical noise as physical countermeasures often rely on device noise or measurement noise. We average any single trace 1000 times

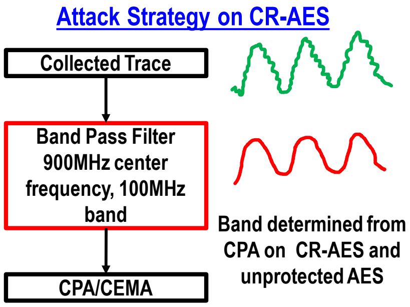


Fig. 17: Attack strategy on clock randomized AES (CR-AES). Trace is collected and filtered with 900MHz center frequency and 100MHz band. The correlational attack is explored against filtered traces.

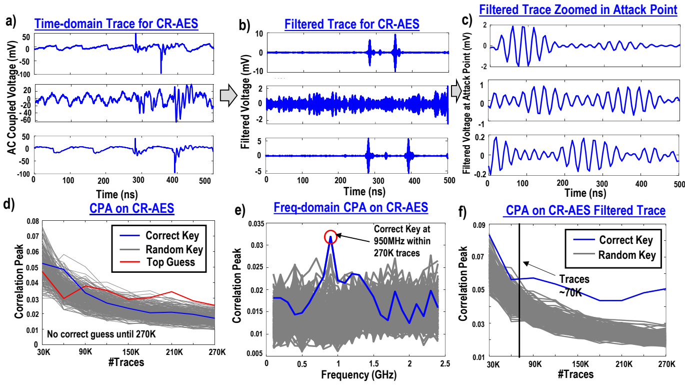


Fig. 18: a) Time domain trace for CR-AES. b) Filtered trace for CR-AES. c) Filtered traces zoomed in on the attack point. d) The correct key is not revealed within 270K traces without the post-processing technique. e) Frequency domain CPA on CR-AES reveals the correct key within 270K traces. f) CPA on CR-AES reveals the correct key can be revealed with just 70K traces.

in the case of the clock slewing technique. We used 1.2M individual encryptions, each with an average of 1000 traces. It should be noted that we count this as 1.2M encryptions. However, averaging creates extra noise in the presence of clock randomization. Hence, we use single averaging for 20M traces when clock randomization is turned on. Moreover, we have used a separate post-processing technique for clock randomization countermeasure. We discuss the techniques and results in section V.B.

B. Correlational Power/EM Attack & Leakage Analysis

Hamming Distance (HD) is used as the attack point between the 13th and 14th rounds on the state register. The trigger is used for the trace alignment. Correlational power analysis (CPA) attack is explored in all the cases, namely with the regular clock with nominal slew, slewed clock, and for the combined countermeasure with clock randomization. We build the HD model based on ciphertext for all possible key bytes and try to correlate with the collected power trace. An unprotected correct key is revealed with just 11K traces, as shown in Fig. 15.

1) Attack on Slewed-clock AES (SL-AES): AES with slewed clock (SL-AES) provides $> 100\times$ enhanced SCA security as indicated by Fig. 8(b). Minimum-traces-to-disclosure (MTD) is 1.2M individual traces, as shown in Fig. 16, which matches our expectations. It is important to note that the correct key is revealed in time-domain traces. However, if we convert it into the frequency domain and try to utilize it, the correct key is not revealed even with 1.2M traces. This gives us the intuition to combine this technique with the clock randomization-based countermeasure as clock randomization is rendered ineffective in frequency domain attacks.

2) Attack on Clock-Randomized AES: Clock-randomized AES (CR-AES) alone provides SCA security against CPA attacks with an MTD $> 270K$. However, a standalone CPA is not enough for CR-AES. Simple post-processing, like trace alignment, will make it ineffective. However, collecting hundreds of thousands of traces and manually aligning traces has a high turn-around time. We use the concept of correlational frequency analysis (CFA) [32] to automate this process. Note that a particular frequency is most leaky at a given process node and a defined architecture. Hence, filtering out that particular frequency will be enough to extract the correct key. To demonstrate that attack, after collecting traces, we use a bandpass filter of 900MHz center frequency and 100MHz band as shown in Fig. 17. The center frequency is decided by scanning in frequency domain traces. Filtered traces are attacked using CPA/CEMA. Collected time domain traces are shown for CR-AES in Fig. 18(a) for different clock frequency for demonstration. Filtered traces are shown in Fig. 18(b). Zoomed-in version of filtered traces is shown in Fig. 18(c).

CPA on CR-AES does not reveal any correct key byte even after 270K traces as shown in Fig. 18(d). Frequency domain CPA shows a correlation peak at 950MHz and 270K traces (Fig. 18(b)). This helps us to decide the center frequency and band frequency range for the filter. CPA is explored against filtered traces to reveal the correct key within 70K traces as shown in Fig. 18(f), which is only $5\times$ improvement with respect to unprotected implementation.

3) Attack on Clock Randomized & Slewed-clock AES: Similarly, both time and frequency domain CPA attacks are performed on clock-randomized and slewed AES (CRSL-AES). The correct key byte is not revealed with $> 20M$ traces (Fig. 19(a)) with time domain attack. Frequency domain CPA is performed throughout the entire frequency spectrum of the power traces, confirming that leaky components cannot be determined in the entire spectrum with 20M traces, as shown in Fig. 19(b). There is no leakage observed using time-domain TVLA until 6M traces using fixed vs. random $|t|$-test (Fig. 19(c)), where unprotected starts to leak with just 110 traces. This is a $40000\times$ improvement over unprotected implementations. We observe no leakage with 0.5M traces with SL-AES, which is $3333\times$ greater than unprotected implementation. Clock slew is introduced with 220fF capacitance here.

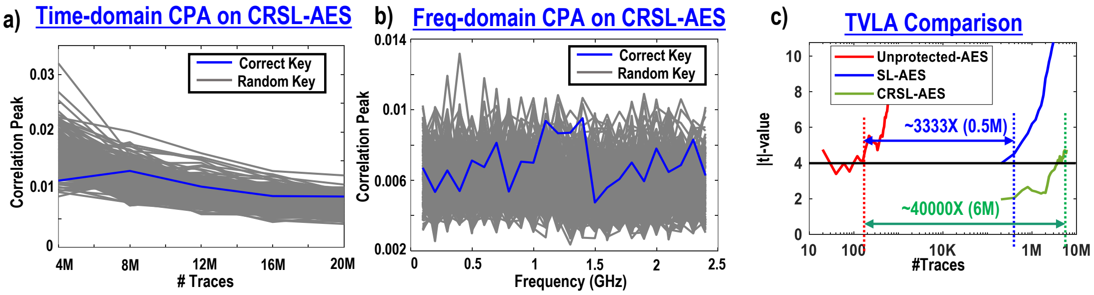


Fig. 19: a) Time domain CPA on Clock Randomized and Slewed AES (CRSL-AES). b) Frequency domain CPA on CRSL-AES. c) TVLA comparison with unprotected correct key shows 40000× improvement in CRSL-AES with respect to unprotected AES.

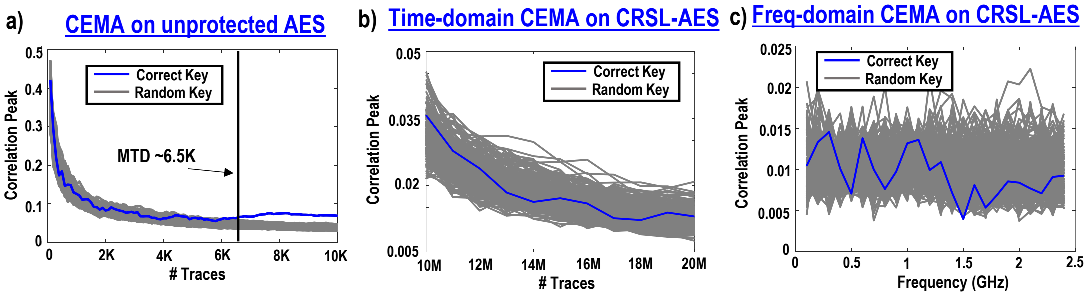


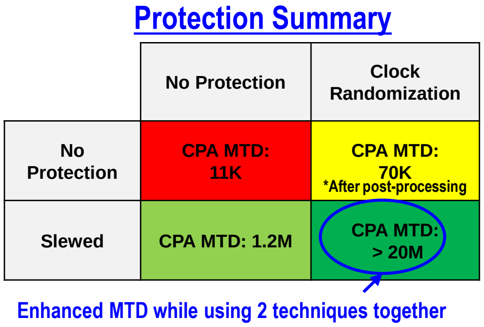
Fig. 20: Time-domain CEMA on a) unprotected b) CRSL-AES. c) Frequency domain CEMA on CRSL-AES.

			This Work	ISSCC'22 [14]	ISSCC'22 [10]	ISSCC'21 [23]	ISSCC'20 [19]	JSSC'20 [15]	ISSCC'20 [21]	JSSC'20 [18]	ISSCC'17 [16]	ISSCC '09 [13]	JSSC'06 [8]
Countermeasure Technique			Clock-slew variability+ clock randomization	Run-time Machine-Learning based	Random Additive masking + Address randomization	Digital Signature Attenuation	Edge-Chasing Quantizer based digital LDO	ML-based HD distribution	Current Domain Signature Attenuation	Digital LDO with randomization	Integrated Buck Regulator	Switched Capacitor Current Equalizer	Wave dynamic differential logic
CMOS Process			65nm	40nm	7nm	65nm	65nm	28nm	65nm	130nm	130nm	130nm	180nm
Crypto Algorithm			AES-256	AES-128, PRESENT	AES-128/256	AES-256	AES-128	AES-128	AES-256	AES-128	AES-128	AES-128	AES-128
Design Overhead	Area		11%	93%	120%	52%	27.5%	36%	37%	36.9%[b]	1%[c]	33%	300%
	Power		<3% + 11%[d]	8.60%	120%	50%	19.4%	32%	49.80%	32%	5%[c]	20%	400%
	Perf.		<6%-46%[d]	0%	8%	0%	4.5%	0%	0%	10.40%	3.33%	50%	25%
SCA Analysis	Time/Freq Domain		Time, Freq	Time	Time	Time, Freq	Time	Time	Time, Freq	Time, Freq	Time, Freq	Time	Time
	MTD	Power	>20M (>1,800X)	>1.2B (>120,000x)	1B [a] (>40,000x)	>1.25B (>178,000x)	>7M (14000X)	1.5M (446X)	>1B (>125,000x)	8M (4210x)	>100K (20x)	>10M (2500x)	255K (120x)
		EM	>20M (>1,800X)	>1.2B (>60,000x)		>1.25B (>138,888x)	NA NA	NA	>1B (>83,333x)	6.8M (136x)	-	-	-
	TVLA	Power	> 6M (>40,000X)	937,500x	>27,000x [a]	290,000x	NA	NA	-	-	-	-	-
		EM	>6M (>40,000X)	277,780x		70,000x	NA	NA	-	-	-	-	-
	Attack Mode		Power/EM	Power/EM	Power/EM	Power/EM	Power	Power	Power/EM	Power/EM	Power	Power	Power

[a]Not reported separately for power and EM, [b]Does not include MIM Cap area, [c]Does not include regulator area/power, [d]All the experiments are done with 220fF capacitor with <6% performance overhead. 11% power overhead is from clock driver + AES w.r.t. unprotected AES with standard clock driver. We do not include this design-specific overhead as power overhead of AES because this is not fundamental to the SCA resiliency technique. Performance degradation can be mitigated by overdesign or increasing buffer's driving capability at the cost of power overhead.

TABLE I: Comparison with respect to other state-of-the-art.

In brief, unprotected implementation can be attacked using just 11K traces. Clock randomization improved MTD by 5×, which is 70K traces. SL-AES improved the MTD by 100×, which is 1.2M individual traces. The cumulative effect (CPA MTD>20M (1,800×) for CRSL-AES) is even more than the multiplicative effect of the individual techniques (CPA MTD for SL-AES: 1.2M (109×), CR-AES: 70K (6.4×)) as shown in Fig. 21. We did a similar experiment with Correlational EM



Protection Summary

	No Protection	Clock Randomization
No Protection	CPA MTD: 11K	CPA MTD: 70K *After post-processing
Slewed	CPA MTD: 1.2M	CPA MTD: > 20M

Enhanced MTD while using 2 techniques together

Fig. 21: Protection summary. We observe that combined MTD is higher than the multiplicative effect of clock randomization and clock slewing technique.

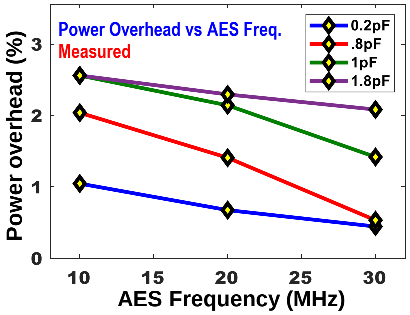


Fig. 22: Power overhead vs frequency. It should be noted that with a higher slew there is observable frequency reduction.

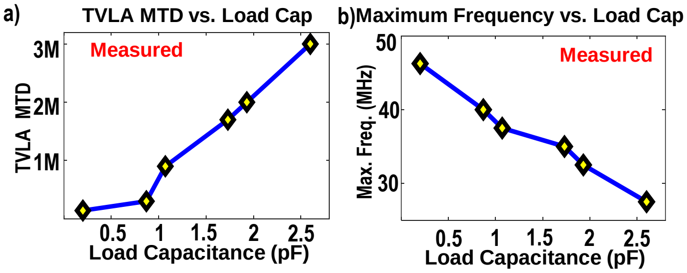


Fig. 23: a) Measurement from TSMC 65nm prototype IC shows an increase in TVLA minimum traces to disclosure as we increase slew by introducing more loading to the clock port. b) Inversely, maximum frequency reduction is achieved with an increase in slew.

Analysis (CEMA). Unprotected implementation can be broken with just 6.5k traces as shown in Fig. 20(a). However, the CEMA attack fails to extract the correct key even after 20M traces. We see a similar phenomenon against both time-domain and frequency-domain attacks, as shown in Fig. 20(b-c). Both time domain and frequency domain attacks fail to retrieve the correct key byte with 20M traces.

4) Protection-Overhead Trade-off: We observe that the power consumption increases owing to the short-circuit current as both PMOS and NMOS are turned on for extended time, as shown in Fig. 22. This is significantly less compared to the current drawn at the slew rate we are operating. However, this is $< 5\%$, the lowest reported amongst the countermeasures to date. Note that this implementation has no large droop-related overhead, making it one of the lowest overhead solutions to date. Area overhead (11%) is one of the lowest compared to existing state-of-the-art countermeasures. Clock generation needs just 81 inverters along with a multiplexer. All these components are minimum-sized and contribute to area overhead minimally. The main area overhead comes from capacitors. However, the total capacitors used is $< 8pF$, which is significantly lower overhead with respect to other circuit-level countermeasures. DCAP cells are used as loading capacitors. DCAP cells are standard cells placed & routed with industry-level tools without any modification from the standard script, making it a fully synthesizable solution. There are alternate ways of creating the slewed clock. For example, a weaker buffer is one strategy that can be utilized to benefit more in terms of area/power overhead. This will be explored as part of future work. Fig 22 shows a detailed power overhead vs frequency. Loading the clock port with a capacitor of $>$ 1pF creates more slew; however, it has a high-performance trade-off. Measurement results show leakage reduces when more slew is introduced (Fig. 23(a)). Fig. 23(b) presents performance overhead for the load capacitor at the clock port. Hence, we have chosen to load the clock port with a maximum of 870fF, ensuring minimum performance drawback.

5) Comparison with State-of-the-art: A detailed comparison with existing state-of-the-art is presented in Table I. This technique has the lowest overhead in terms of area/power with respect to other circuit-level countermeasures and, hence, can be used in modern-day lightweight devices for medium security. This design, for the first time, focuses on circuit-level effects of the clock port and its interaction with inherent clock-slew-dependent variability of CMOS digital circuits that can be easily combined with existing and emerging power-port countermeasures for a multiplicative effect on SCA resilience.

VI. Conclusion

The clock slewing technique is a low-overhead, synthesizable, and generic countermeasure. It enhances the efficacy of the system-level clock randomization. This lightweight countermeasure is suitable for edge devices, and can be augmented with any other power-port/architectural countermeasure for multiplicative effect, as the overhead of this countermeasure is almost negligible. This is the 1st known countermeasure exploiting the inherent variability of digital circuits by introducing the clock-slew. A combination of slew and clock randomization provides strong resilience against side-channel analysis. This technique opens up a new area of possible optimized physical countermeasure using a clock port as well as a combination of both clock and V_{DD} port.

References

[1] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, number 1666 in Lecture Notes in Computer Science, pages 388–397. Springer Berlin Heidelberg, August 1999.

[2] Paul Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi. Introduction to differential power analysis. *Journal of Cryptographic Engineering*, 1(1):5–27, March 2011.

[3] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO '96*, number 1109 in Lecture Notes in Computer Science, pages 104–113. Springer Berlin Heidelberg, August 1996.

[4] Fox-IT. TEMPEST attacks against AES. Technical report.

[5] Raghavan Kumar, Vikram B Suresh, Sachin Taneja, Mark A Anders, Steven Hsu, Amit Agarwal, Vivek De, and Sanu K Mathew. A 7-gbps sca-resistant multiplicative-masked aes engine in intel 4 cmos. *IEEE Journal of Solid-State Circuits*, 58(4):1106–1116, 2022.

[6] Begül Bilgin, Benedikt Gierlichs, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. Higher-order threshold implementations. In *Advances in Cryptology–ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, ROC, December 7-11, 2014, Proceedings, Part II 20*, pages 326–343. Springer, 2014.

[7] Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff. Convolutional neural networks with data augmentation against jitter-based countermeasures. In *CHES*, 2017.

[8] David D Hwang, Kris Tiri, Alireza Hodjat, B-C Lai, Shenglin Yang, Patrick Schaumont, and Ingrid Verbauwhede. AES-Based Security Coprocessor IC in 0.18um CMOS With Resistance to Differential Power Analysis Side-Channel Attacks. *IEEE Journal of Solid-State Circuits*, 41(4):781–792, April 2006.

[9] David Canright and Lejla Batina. A very compact "perfectly masked" s-box for aes. In *Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings 6*, pages 446–459. Springer, 2008.

[10] Raghavan Kumar, Vikram B Suresh, Mark A Anders, Steven K Hsu, Amit Agarwal, Vivek K De, and Sanu K Mathew. An 8.3-to-18gbps reconfigurable sca-resistant/dual-core/blind-bulk aes engine in intel 4 cmos. In *2022 IEEE International Solid-State Circuits Conference (ISSCC)*, volume 65, pages 1–3. IEEE, 2022.

[11] Lauren De Meyer, Oscar Reparaz, and Begül Bilgin. Multiplicative masking for aes in hardware. pages 431–468, 2018.

[12] Raghavan Kumar, Xiaosen Liu, Vikram Suresh, Harish K Krishnamurthy, Sudhir Satpathy, Mark A Anders, Himanshu Kaul, Krishnan Ravichandran, Vivek De, and Sanu K Mathew. A time-/frequency-domain side-channel attack resistant aes-128 and rsa-4k crypto-processor in 14-nm cmos. *IEEE Journal of Solid-State Circuits*, 56(4):1141–1151, 2021.

[13] C. Tokunaga and D. Blaauw. Secure AES engine with a local switched-capacitor current equalizer. In *2009 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, pages 64–65,65a, February 2009.

[14] Qiang Fang, Longyang Lin, Yao Zu Wong, Hui Zhang, and Massimo Alioto. Side-channel attack counteraction via machine learning-targeted power compensation for post-silicon hw security patching. In *2022 IEEE International Solid-State Circuits Conference (ISSCC)*, volume 65, pages 1–3, 2022.

[15] Weiwei Shan, Shuai Zhang, Jiaming Xu, Minyi Lu, Longxing Shi, and Jun Yang. Machine learning assisted side-channel-attack countermeasure and its application on a 28-nm aes circuit. *IEEE Journal of Solid-State Circuits*, 55(3):794–804, 2020.

[16] Monodeep Kar, Arvind Singh, Sanu Mathew, Anand Rajan, Vivek De, and Saibal Mukhopadhyay. 8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator. In *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pages 142–143, February 2017.

[17] Monodeep Kar, Arvind Singh, Sanu K Mathew, Anand Rajan, Vivek De, and Saibal Mukhopadhyay. Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator. *IEEE Journal of Solid-State Circuits*, 53(8):2399–2414, August 2018.

[18] Arvind Singh, Monodeep Kar, Venkata Chaitanya Krishna Chekuri, Sanu K Mathew, Anand Rajan, Vivek De, and Saibal Mukhopadhyay. Enhanced Power and Electromagnetic SCA Resistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO. *IEEE Journal of Solid-State Circuits*, 55(2):478–493, February 2020.

[19] Yan He and Kaiyuan Yang. 25.3 a 65nm edge-chasing quantizer-based digital ldo featuring 4.58ps-fom and side-channel-attack resistance. In *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, pages 384–386, February 2020. ISSN: 2376-8606.

[20] Raghavan Kumar, Xiaosen Liu, Vikram Suresh, Harish Krishnamurthy, Mark Anders, Himanshu Kaul, Krishnan Ravichandran, Vivek De, and Sanu Mathew. A sca-resistant aes engine in 14nm cmos with time/frequency-domain leakage suppression using non-linear digital ldo cascaded with arithmetic countermeasures. In *2020 IEEE Symposium on VLSI Circuits*, pages 1–2. IEEE, 2020.

[21] Debayan Das, Josef Danial, Anupam Golder, Nirmoy Modak, Shovan Maity, Baibhab Chatterjee, Donghyun Seo, Muya Chang, Avinash Varna, Harish Krishnamurthy, et al. 27.3 EM and Power SCA-Resilient AES-256 in 65nm CMOS Through >350× Current-Domain Signature Attenuation. In *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, pages 424–426, February 2020. ISSN: 2376-8606.

[22] Archisman Ghosh, Debayan Das, Josef Danial, Vivek De, Santosh Ghosh, and Shreyas Sen. Syn-stellar: An em/power sca-resilient aes-256 with synthesis-friendly signature attenuation. *IEEE Journal of Solid-State Circuits*, 57(1):167–181, 2021.

[23] Archisman Ghosh, Debayan Das, Josef Danial, Vivek De, Santosh Ghosh, and Shreyas 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 *2021 IEEE International Solid-State Circuits Conference (ISSCC)*, volume 64, pages 499–501. IEEE, 2021.

[24] Archisman Ghosh, Debayan Das, and Shreyas Sen. Physical time-varying transfer function as generic low-overhead power-sca countermeasure. *IEEE Open Journal of Circuits and Systems*, 2023.

[25] Arvind Singh, Monodeep Kar, Sanu K Mathew, Anand Rajan, Vivek De, and Saibal Mukhopadhyay. Improved power/em side-channel attack resistance of 128-bit aes engines with random fast voltage dithering. *IEEE Journal of Solid-State Circuits*, 54(2):569–583, 2018.

[26] Shengqi Yang, Wayne Wolf, Narayanan Vijaykrishnan, Dimitrios N Serpanos, and Yuan Xie. Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach. In *Design, Automation and Test in Europe*, pages 64–69. IEEE, 2005.

[27] Martin Brisfors, Michail Moraitis, and Elena Dubrova. Side-channel attack countermeasures based on clock randomization have a fundamental flaw. *Cryptology ePrint Archive*, 2022.

[28] Qizhi Tian and Sorin A Huss. A general approach to power trace alignment for the assessment of side-channel resistance of hardened cryptosystems. In *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 465–470. IEEE, 2012.

[29] Qizhi Tian and Sorin A Huss. On clock frequency effects in side channel attacks of symmetric block ciphers. In *2012 5th International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5. IEEE, 2012.

[30] Dor Fledel and Avishai Wool. Sliding-window correlation attacks against encryption devices with an unstable clock. In *Selected Areas in Cryptography–SAC 2018: 25th International Conference, Calgary, AB, Canada, August 15–17, 2018, Revised Selected Papers 25*, pages 193–215. Springer, 2019.

[31] Oliver Schimmel. Correlation power analysis in frequency domain, cosade, february 4-5 2010. *Cited on*, page 65.

[32] Edgar Mateos and Catherine H Gebotys. A new correlation frequency analysis of the side channel. In *Proceedings of the 5th Workshop on Embedded Systems Security*, pages 1–8, 2010.

[33] Saideep Sreekumar, Mohammed Ashraf, Mohammed Nabeel, Ozgur Sinanoglu, and Johann Knechtel. X-volt: Joint tuning of driver strengths and supply voltages against power side-channel attacks. *arXiv preprint arXiv:2211.08046*, 2022.

[34] Patanjali Slpsk, Prasanna Karthik Vairam, Chester Rebeiro, and V Kamakoti. Karna: A gate-sizing based security aware eda flow for improved power side-channel attack protection. In *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 1–8. IEEE, 2019.

[35] William C Elmore. The transient response of damped linear networks with particular regard to wideband amplifiers. *Journal of applied physics*, 19(1):55–63, 1948.

[36] O-X Standaert, Eric Peeters, Gaël Rouvroy, and J-J Quisquater. An overview of power analysis attacks against field programmable gate arrays. *Proceedings of the IEEE*, 94(2):383–394, 2006.