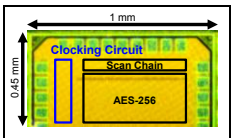
Power and EM SCA Resilience in 65nm AES-256 Exploiting Clock-Slew Dependent Variability in CMOS Digital Circuits

Archisman Ghosh[1], Md. Abdur Rahman[1], Debayan Das[1,2], Santosh Ghosh[2], Shreyas Sen[1]
[1]Purdue University, IN, USA, [2]Intel Corp. Portland, OR, USA,

Side channel analysis (SCA) is a low time-complexity technique of extracting secret information from a cryptographic IC, which calls for low-overhead generic resilience techniques. While architectural and logical countermeasures [1] are explored widely, recently generic circuit-level countermeasures (e.g. voltage regulators [2-4], power balancing [5] or through a switched capacitor current equalizer [6], using an on-chip machine learning model [7, 8], and signature attenuation [9, 10]) have gained prominence due to low overheads and being architecture agnostic. Typical digital cryptographic core has two controllable ports, i.e., supply and clock. Most of the circuit-level/physical layer countermeasures have primarily utilized the power port to reduce the side-channel leakage signal-to-noise ratio (SNR). Related to the clocking port, well-studied system-level clock frequency randomization techniques have been deemed ineffective with post-processing. 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 SCA leakage remains unexplored. Another key 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, which can be easily combined with any of the supply port countermeasures for multiplicative effect on SCA resilience.

While CMOS digital circuits are abstracted logically in terms of their functionality guaranteed up to the f_{max}, their power consumption profile is a strong function of circuit-level changes in the clocking network. Controlled clock-slew results in the following effects: 1) register internal clock slew propagation leading to 2 important variability in digital circuits, namely 2) duty cycle distortion, and 3) slew-dependent latch delay variability (hence flip-flop (FF) toggle point variability). In presence of the controlled clock slew, 2 important process dependent factors, namely 4) location-dependent variability in Elmore delay and 5) intra-die process variation (device mismatch) also get amplified increasing 1-3 which increases the SCA security further. Additionally, system-level clock randomization is now more effective in presence of the slewed clock as the post-processing techniques become ineffective when the sharp edges are absent. The effect of the clock slew is gradually reduced as it passes through internal buffer stages of FF (Fig. 1, Effect 1), but not fully suppressed (bottom right). Slews S1, S2 present at the master and slave stages of FF determine its toggle points (Fig. 1, bottom), making the power profile a complex function of the input and slew, instead of just the input. Note that S1 and S2 are internal to register and hence do not drive clock of different parts of the designs ensuring functional correctness. Duty cycle gets distorted (Fig. 2, Effect 2) based on the rise time (t_r), especially for high input slew (low slope) cases with less than full-scale clock swing, which in turn changes the time between different leakage points in the power supply, making it harder to attack. Providing slewed clock to FF makes latching time (Effect 3) a function of t_r as well as the input since $t_{latch\_HL} \neq t_{latch\_LH}$. Slewed clock affects the Elmore delay (Effect 4) which further increases cumulative slewness at clocks of different FFs, enhancing SCA security. Combinational delay does not vary with slew (Fig. 2, bottom left) ensuring no set-up violation in the design. Large slew (very small slope) could lead to hold time increase; however, clock-q delay increases with respect to slew as well ensuring significant positive slack (Fig. 2, bottom middle). Due to this, we observe no functional failure in the IC. Performance can be impacted only by <1% (up to C_L=0.87pF) to <10% (C_L=1pF) in terms of f_{max}, if clock buffer is not able to drive the clock port and does not reach toggle point due to extra capacitance in this design. However, this is not fundamental to this SCA resilient technique. We can mitigate the performance degradation by overdesigning clock buffer or by increasing the driving capability of the same buffer at the cost of power overhead. This performance trade-off benefits in SCA resilience (<1% f_{max} degradation, but 1800x improvement in MTD). Fig. 2 (bottom right) shows ~10x increase in variance of power trace of clock-slewed AES design (red) with respect to unprotected (green) near 14th cycle posedge (empirically highest leakage point) which confirms the basis of SCA resilience.



Die micrograph.

The IC consists of a parallel AES256 with slewed clock buffer and clock randomization circuit as shown in Fig. 3. HD between 13th and 14th rounds on state register is used as the attack point. Trigger is used for the trace alignment. Slewed clocking buffer provides the tunability to load the clock with different capacitors ranging from 100fF to 5pF (Fig. 3). We utilize a LFSR (seeded by an external TRNG for high randomness) which randomly selects between capacitors for enhanced security (Fig. 3, top right). A tunable ring oscillator is designed for the clock randomization (Fig. 3, bottom left). The number of stages is determined by the LFSR output to provide clock frequency randomization. Coarse frequency change is performed using a 3-stage frequency divider (Fig. 3, bottom left). Time domain waveform of the 14th cycle of AES256 for a set of 6 different plaintexts are shown for different configurations (Fig. 4, top). Clearly, 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 dP/dx) in absence of slewed clock. Due to clock slew, power consumption ($P'(t) = \boldsymbol{f}(\boldsymbol{x}(\boldsymbol{t}), \boldsymbol{t} - \boldsymbol{D}(\boldsymbol{s}))$) is dependent on slew (s)-related delay $D(s)$, which is a non-linear function of the input data ($x(t)$) as shown in Fig 4. Significant SCA resilience could be achieved if $dP'/dx \ll dP'/dD$. Clock randomization (CR) is combined with the clock slew for enhanced security. Prior CR-based countermeasures with sharp clock were deemed ineffective as the traces can be aligned in time-domain using post-processing or can be bandpass filtered for frequency-domain attack. With slewed clock, 1) power profile gets smeared in time-domain creating Inter-Symbol Interference (ISI) and 2) determining randomized clock edge variations is hard to distinguish from power profile with slewed randomized clock, making time-realignment attacks extremely difficult. Leaky frequency components (~900MHz is most leaky as shown in measurements, Fig. 4, 5) could not be determined with 20M traces rendering frequency domain post-processing-based attacks on combined clock randomized slewed AES (CRSL-AES) extremely difficult. Entire circuit is completely synthesizable and fully placed and routed using commercial tools. Capacitors are implemented using DCAP cell from standard library.

Correlational power analysis (CPA) attack is explored both in case of regular clock, slewed clock, and for the combined countermeasure with clock randomization. AES with slewed clock (SL-AES) provides >100x enhanced SCA security (MTD = 1.2M) with respect to the unprotected core (MTD = 11K). CR-AES alone provides SCA security against CPA attack with an MTD > 270K, however, correct key is revealed within 70K traces utilizing a bandpass filter. Time and frequency domain CPA attack performed on CRSL-AES could not reveal the correct key byte with >20M traces (Fig. 5). Frequency domain CPA is performed throughout the entire frequency spectrum of the power traces which confirms that leaky component cannot be determined in entire spectrum with 20M traces. The cumulative effect (CPA MTD>20M (1,800x) for CRSL-AES) is even more than multiplicative effect of the individual techniques (CPA MTD for SL-AES: 1.2M (109x), CR-AES: 70K (6.4x)). Correlational EM Analysis (CEMA) attack fails to extract correct key even after 20M traces. There is no leakage observed using time-domain TVLA until 6M traces using fixed vs random |t|-test (Fig. 5). We observe that the power consumption is increased owing to the short-circuit current as both PMOS and NMOS common turn on time increases (Fig. 5), however this is <5%, the lowest reported amongst the countermeasures till date. Area overhead (11%) is one of the lowest compared to existing state-of-the-art countermeasures. Any capacitance beyond 870fF is not used to ensure high performance. A detailed comparison along with current overhead is presented in the table of Fig. 6. 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.

References:
[1] R. Kumar et al., ISSCC, 2022. [2] A. Singh et al., ISSCC, 2019. [3] Y. He et al, ISSCC, 2020. [4] M. Kar et al., ISSCC, 2017. [5] D. D. Hwang et al., JSSC, 2006. [6] C. Tokunaga, et al., ISSCC, 2009. [7] Q. Fang, et al., ISSCC, 2022. [8] W. Shan et al., JSSC, 2020. [9] D. Das, et al., ISSCC, 2020. [10] A. Ghosh, et al., ISSCC, 2021.

2023 IEEE Custom Integrated Circuits Conference (CICC) | 979-8-3503-9948-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/CICC57935.2023.10121240

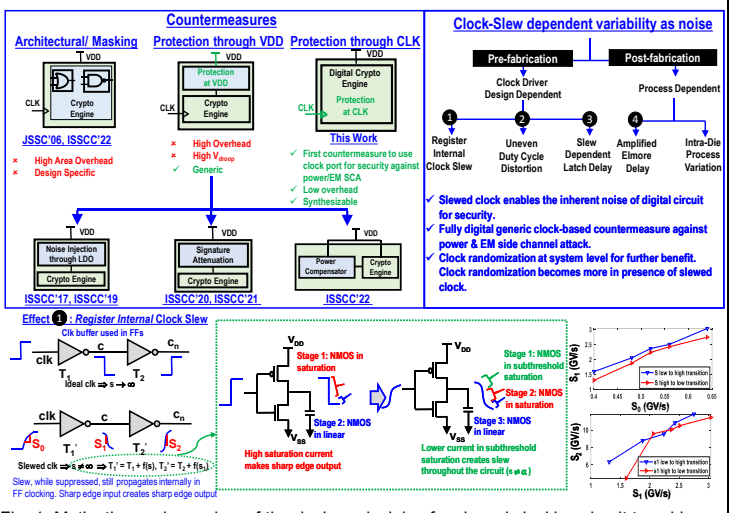


Fig. 1. Motivation and overview of the design principles for slewed clocking circuit to achieve both power and EM SCA resilience. Effect 1 (bottom figures) shows the clock slew propagates through the register's internal buffer. Change of slew through the buffers is shown in bottom right.

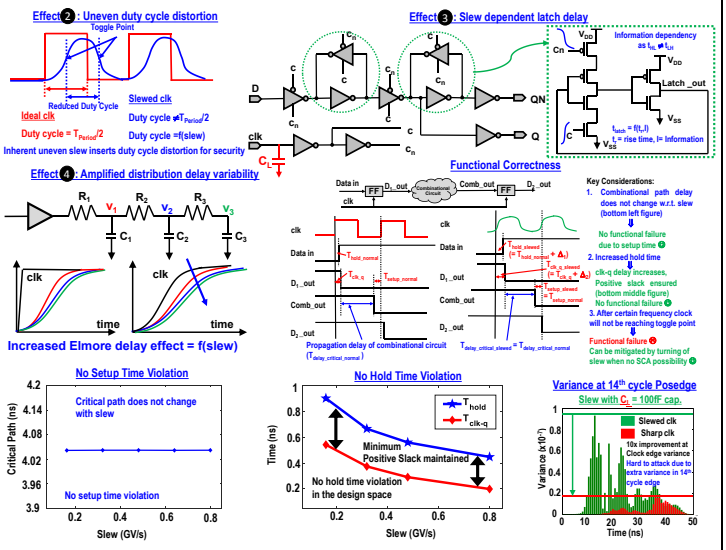


Fig. 2. Impact of the clock slew namely uneven duty cycle distortion (effect 2), slew dependent latch delay (effect 3), amplified distribution delay (effect 4), probability of functional correctness along with design considerations are shown. No setup/hold violation is ensured.

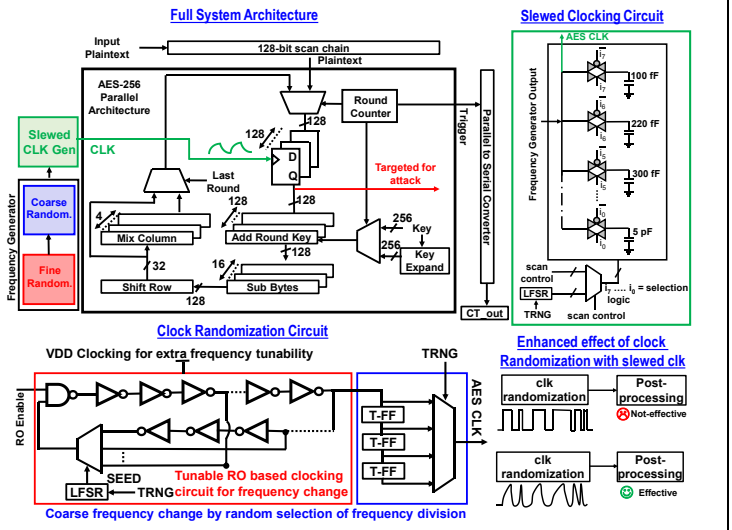


Fig. 3. System architecture showing the circuit details of the slewed clock AES (SL-AES), clock randomized AES (CR-AES), and the combined countermeasure clock randomized slewed AES (CRSL-AES). CRSL-AES is hard to be broken using SCA and more effective than CR-AES and SL-AES combined.

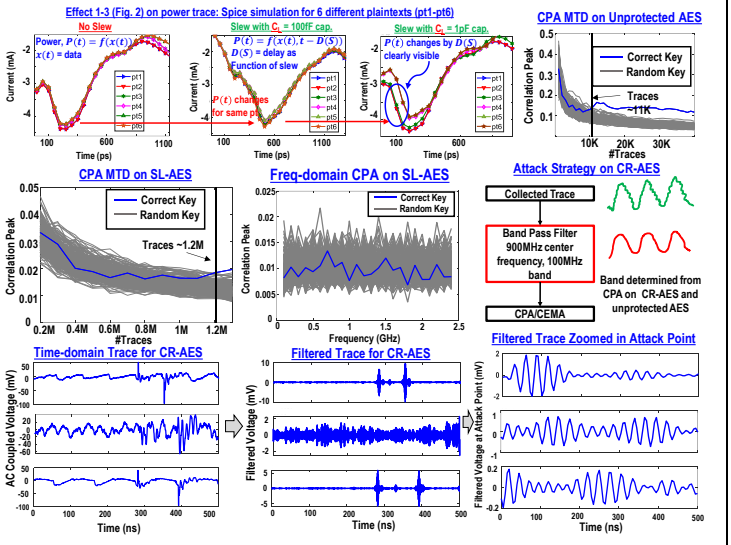


Fig. 4. Measurement Results: Power SCA (standard and post-processing based) demonstrating the resiliency of unprotected AES, SL-AES and CR-AES. SL-AES shows an MTD of 1.2M traces compared to 11K for the unprotected AES implementation.

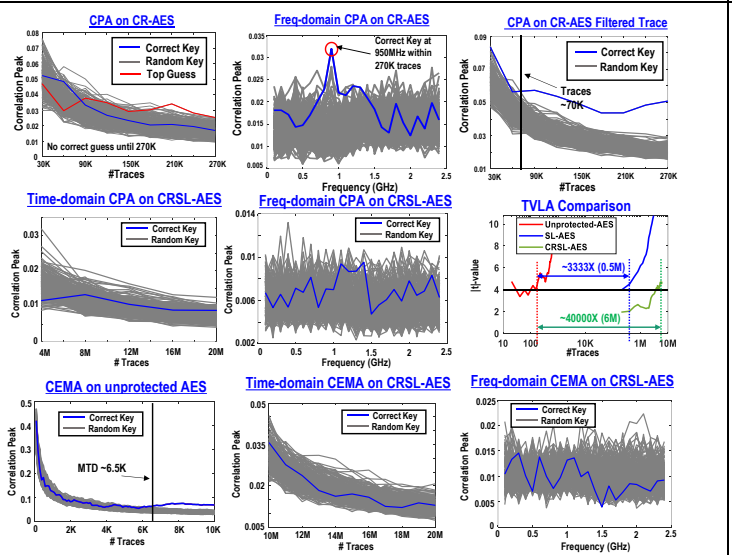
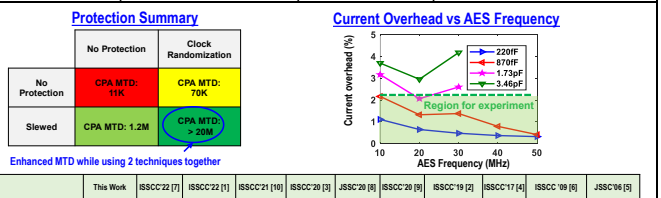


Fig. 5. Measurement Results: Standalone CR-AES is broken with 70K traces using band pass filtering. Time and Frequency Domain CPA/CEMA attack and TVLA on the unprotected vs. CRSL-AES256. CRSL-AES shows an MTD of >20M traces, which is >1800x improvement over the unprotected AES. TVLA shows 40000x improvement over unprotected design.



			This Work	ISSCC'22 [7]	ISSCC'22 [1]	ISSCC'21 [10]	ISSCC'20 [3]	JSSC'20 [8]	ISSCC'20 [9]	ISSCC'19 [2]	ISSCC'17 [4]	ISSCC '09 [6]	JSSC'06 [5]
Countermeasure Technique			Noise Injection by clock slew	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		<5% + 11%[d]	8.60%	120%	50%	19.4%	32%	49.80%	32%	5%[c]	20%	400%
	Perf.		<1%-40%[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 * (>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	>1B (>83,333x)	6.8M (136x)	-	-	-
	TVLA	Power	> 6M (>40,000X)	937,500x	>27,000x *	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 <870fF capacitor with <1% 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.

Fig. 6. Protection summary, current overhead, and comparison with State-of-the-Art countermeasures.