On-Chip SCC Topologies for Security Enabling 50% Power Reduction and 114× Attack Traces

Justin Pabot[1], Yasser Moursy[1], Maxime Lecomte[1], Romain Wacquez[1,2], and Gaël Pillonnet[1]
[1]Univ. Grenoble Alpes, CEA, Leti, F-38000 Grenoble, France
[2]CEA-Leti, Mines Saint-Etienne, Equipe Commune, Gardanne France
justin.pabot@cea.fr

***Abstract*—As hardware security becomes a major requirement in edge-AI systems, countering Side-Channel Attacks (SCAs) with minimal overhead is increasingly important. In recent CMOS technologies, digital Advanced Encryption Standard (AES) cores require a step-down converter from the system bus voltage. Such a converter can therefore also be exploited as an intrinsic first layer of side-channel protection. To guide the design of future AES-based systems, three fully integrated SCC topologies are experimentally compared in a 22nm FD-SOI to *supply and protect* an AES core. At system level, AES power consumption is reduced by up to 50% thanks to 3:1 voltage scaling, leading to a *negative* power overhead compared to the 2:1 baseline. In addition, the number of traces required to recover the key is improved by up to 114× and 750× for CPA and TVLA, respectively, compared to an unprotected AES. These results show that SCC topology can simultaneously reduce system power and provide an intrinsic *first line of defense* against side-channel attacks.**

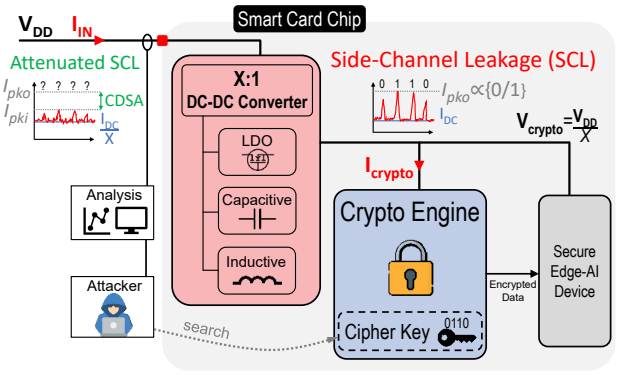
***Index Terms*—hardware security, switched-capacitor converter, side-channel attack.**

I. Introduction

As secure computing moves toward distributed edge devices, hardware-level protection against side-channel attacks is becoming a key design requirement. Although encryption algorithms may be mathematically secure, their hardware implementation can still leak information through power consumption or electromagnetic (EM) emissions. Among these attacks, Correlation Power Analysis (CPA) is particularly prevalent: an attacker records the device current profile and correlates it with hypothetical leakage models to recover the secret key, as illustrated in Fig. 1.

Traditional countermeasures reduce Side-Channel Leakage (SCL) by modifying the encryption core itself [1] or by integrating dedicated obfuscation circuits on the same die [2], often at significant area and power cost. By contrast, embedding part of the protection in the power delivery path is especially appealing because the converter is already required for voltage scaling: its security function therefore comes with no dedicated overhead and may even lead to a *negative* power overhead at system level by lowering the secure core supply voltage. In step-down converters, the resulting Current-Domain Signature Attenuation (CDSA), together with temporal reshaping of the current signature, degrades the effectiveness of side-channel attacks [3], [4].

In secure embedded applications such as smart cards, the external bus typically remains at 1.8V, whereas advanced digital cores operate around 0.9V or below. Switched-Capacitor



Side-Channel Attack Protection Schemes		
Additional Area	Embedded in Converter	
Core Modification	**Converter Feedback**	**LDO**
AES core e.g. [7]	IVR feedback e.g. [8]	e.g. [4]
☹ design specific ☹ high overheads	☺ Low overheads ☹ Limited bandwidth	☺ No passive ☹ Low efficiency
Analog Countermeasure	**Inductive**	This work **Switched Capacitor**
obfuscation circuit AES e.g. [6]	e.g. [5]	e.g. [1], [2], [3]
☺ high security ☹ high overheads	☹ Inductor integration ☹ EM radiation	☺ Voltage conversion ☺ High efficiency

Fig. 1. On-chip supply for SCA mitigation.

Converters (SCCs) are therefore particularly attractive because they combine fully integrated step-down conversion with intrinsic leakage attenuation: they store energy in capacitors and redistribute it over switching phases instead of directly transferring the instantaneous secure core current to the input supply. By contrast, obfuscation-oriented LDOs do not provide efficient voltage down-conversion and therefore inherently introduce a power overhead [5], while inductive converters rely on bulky or externally accessible magnetic components [6] [7]. Despite the growing interest in converter-assisted side-channel protection, the available literature remains limited and still largely simulation-based [8], especially regarding the impact of SCC topology on the trade-off between security, conversion ratio, and implementation overhead.

This work investigates three SCC topologies to simultaneously *power and secure* an Advanced Encryption Standard (AES) engine. Beyond voltage conversion, SCC-based supply

protection enables a *negative* power overhead of up to -50% thanks to AES voltage scaling, while improving side-channel resilience by up to 114× and 750× in terms of CPA and TVLA xMTD, respectively, compared to an unprotected AES.

II. Topology Trade-Offs and IC Implementation

A. Explored SCC Topologies

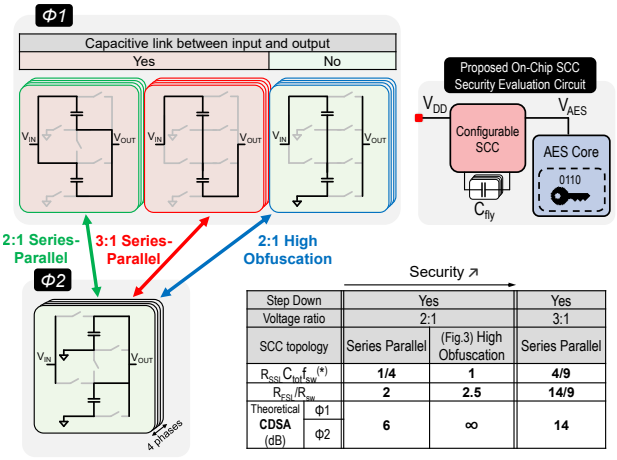
The SCC topologies considered in this work are shown in Fig. 2. They are selected to explore the trade-off between side-channel protection, voltage conversion capability, and power delivery. To guide this comparison, Fig. 2 reports two key metrics. The first one is $R_{\mathrm{SSL}} C_{\mathrm{tot}} f_{\mathrm{sw}}$, which reflects the ability of a topology to provide a low output impedance for a given total flying capacitance C_{tot} and switching frequency f_{sw}; the lower this value, the better the expected current delivery capability and efficiency. The second metric is the Current-Domain Signature Attenuation (CDSA), used to assess the SCA resilience [4]. CDSA quantifies how much of the AC output current is transferred to the input current, and depends on both the converter topology and the operating phase. Although a high CDSA does not strictly guarantee immunity to SCA, a low CDSA is a strong indicator of direct Side-Channel Leakage (SCL).

For a given flying-capacitance budget, the conventional 2:1 Series-Parallel (SP) topology provides the lowest output impedance and thus the best efficiency for a given $C_{\mathrm{tot}} f_{\mathrm{sw}}$, which makes it the natural baseline. However, its protection remains limited because, during one operating phase, the AES current is directly transferred from output to input through the flying capacitor. If encryption activity occurs in this phase, a significant fraction of the AES current signature is directly visible from the supply input.

The 2:1 High-Obfuscation (HO) topology improves isolation by removing any direct input-to-output current path. It therefore maximizes CDSA and provides the strongest intrinsic attenuation of the AES current signature. This benefit, however, comes at the cost of a much higher Slow-Switching-Limit (SSL) resistance, hence a larger output impedance and lower current delivery capability for a given efficiency target.

The 3:1 SP topology offers a different compromise. Although some direct coupling remains during its first operating phase, it provides a higher CDSA than the 2:1 SP case and generates a lower output voltage, which reduces the AES current consumption itself. Side-channel leakage is therefore mitigated both by partial attenuation and by lower load activity, at the expense of lower efficiency than the 2:1 SP topology for a given Silicon area budget.

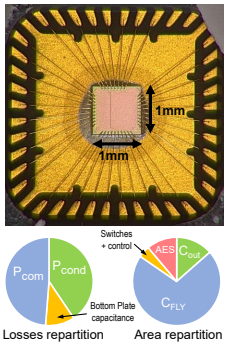
As a result, the 2:1 SP topology achieves the best efficiency but limited protection. In contrast, the 2:1 HO topology maximizes isolation but degrades power delivery, while the 3:1 SP topology combines moderate attenuation with voltage scaling. Quantifying the practical security-efficiency trade-off of these architectures is therefore essential, especially since side-channel behavior is difficult to assess accurately from simulation alone.



Step Down		Yes		Yes
Voltage ratio		2:1		3:1
SCC topology		Series Parallel	(Fig.3) High Obfuscation	Series Parallel
$R_{SSL} C_{tot} f_{sw}$ (*)		1/4	1	4/9
R_{FSL}/R_{sw}		2	2.5	14/9
Theoretical CDSA (dB)	Φ1	6	∞	14
	Φ2			

Fig. 2. Evaluated SCC topologies and key metrics.

B. IC Implementation



AES	Type	AES-128	Unit
	Power	0.68, 0.8V/50MHz	mW
	Voltage	0.54 – 0.9	V
	Area	6270	µm²
SCC Converter	Input Voltage	1.8	V
	Output Range	0.6-0.9	V
	Active Area	0.05	mm²
	Flying Cap	265	pF
	Output Cap	64	pF
	Switching Freq.	11.25	MHz
	Nominal Power	0.7	mW
	Max. Power	2.1	mW
Test Chip	Process	22nm FD-SOI	-
	Switch type	1.8V LVT	-
	Capacitor Type	Integrated MOM	-

Fig. 3. Chip overview and main specifications.

The main characteristics of the 22nm FD-SOI test chip are summarized in Fig. 3. It integrates a fully on-chip SCC together with a standard 50 MHz AES core. A reference AES supplied externally is also included, enabling direct comparison between unprotected and protected implementations.

The SCC relies on a reconfigurable switched-capacitor cell that can be configured for 2:1 conversion, from single-phase up to 4 interleaves, with or without High-Obfuscation (HO), as well as for a 3:1 conversion ratio. This enables the comparison of multiple topologies on the same hardware platform.

Since the average AES power consumption is 0.7 mW, the flying capacitance, switching frequency, and switch sizing are optimized for maximum efficiency around this operating point. The switching frequency is also selected with respect to the AES clock: reducing f_{sw} increases the temporal averaging performed by the SCC, but requires larger flying capacitors and thus more silicon area. A 45 MHz output ripple frequency, slightly below the AES clock frequency, is chosen to minimize SCC area while preserving the intended protection effect.

At this operating frequency, the flying capacitance is chosen to achieve more than 85% efficiency in the baseline 2:1 mode, corresponding to a 3.3× reduction in losses compared to an

LDO. Owing to the capacitor density available in this technology, the converter area is largely dominated by the flying capacitors, leading to a total SCC area of 0.05 mm^2. Only MOM capacitors are used, allowing the converter to be stacked above the smart-card core and thereby reducing its system-level footprint. Finally, the fully integrated implementation requires no additional external components, pins, or process options, which is often a strong industrial requirement.

III. Measured Performance

A. Electrical Performance

Before discussing the security metrics, the conventional DC-DC performance of the three evaluated SCC topologies is summarized in Fig. 4. As expected from the analysis of Section II, the conventional 2:1 topology achieves the highest efficiency, with a peak value of 84% at the AES operating point (0.7 mA). The 2:1 HO topology reaches 72% efficiency, while the 3:1 topology further drops to 65%. This trend is mainly explained by the poorer capacitance utilization of the more secure topologies, which degrades the $R_{\mathrm{SSL}}C_{\mathrm{tot}}f_{\mathrm{sw}}$ factor reported in Fig. 2. The SCC reaches a power density of 42 mW/mm^2, mainly limited by the capacitor density available in the technology (6.5 nF/mm^2), while maintaining higher efficiency than LDO-based solutions. When only the non-capacitive area is considered, i.e., assuming MOM capacitors can be stacked above other functions, the corresponding power density rises to 809 mW/mm^2.

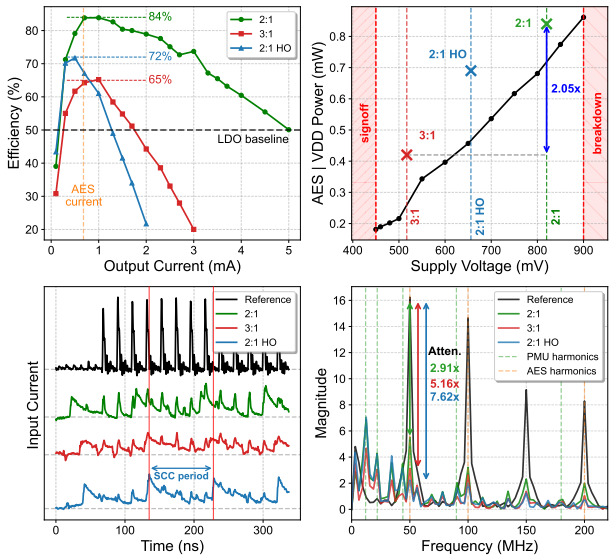


Fig. 4. Measured electrical performance.

At system level, however, the most relevant metric is the power drawn from the external V_{DD}. Owing to the reduced AES supply voltage, the AES power consumption decreases by about 2.5× from the 2:1 to the 3:1 configuration. As a result, despite its lower conversion efficiency, the 3:1 topology still draws about 2.05× less power from V_{DD} than the baseline 2:1 case. Accordingly, the power overhead reported in Table I becomes *negative*, reaching -50% for the 3:1 configuration and -18% for the 2:1 HO configuration, both referenced to the baseline 2:1 case. This result highlights the benefit of integrating the mandatory step-down conversion stage, which not only reduces the overall power consumption—a particularly relevant advantage for edge-AI devices—but also provides side-channel protection at no additional system cost. Since the SCC does not degrade AES throughput, the performance overhead is considered to be 0%. Regarding area overhead, the use of MOM capacitors allows stacking above other circuits, implying 0% area overhead. Moreover, for consistency with prior literature, the converter itself is not counted as an additional area cost, since it already fulfills the voltage-conversion function.

B. Side-Channel Security Evaluation

Because SCC-based supply protection improves security while reducing overall power consumption, the security benefit of the evaluated topologies must be quantified explicitly. As introduced in Section II, CDSA is first used as a qualitative indicator. The measured input-current waveforms in Fig. 4 show that SCC operation modifies the observable current signature in both amplitude and timing. In particular, the 2:1 HO topology strongly averages the sharp AES current spikes, which significantly increases the attack difficulty. In the frequency domain, AES-related components remain partly visible with the 2:1 and 3:1 configurations, whereas they are mainly shifted toward the SCC switching frequency in the 2:1 HO case. This coexistence of AES-related and SCC-related components degrades attack synchronization, while CPA fundamentally relies on accurate sample alignment.

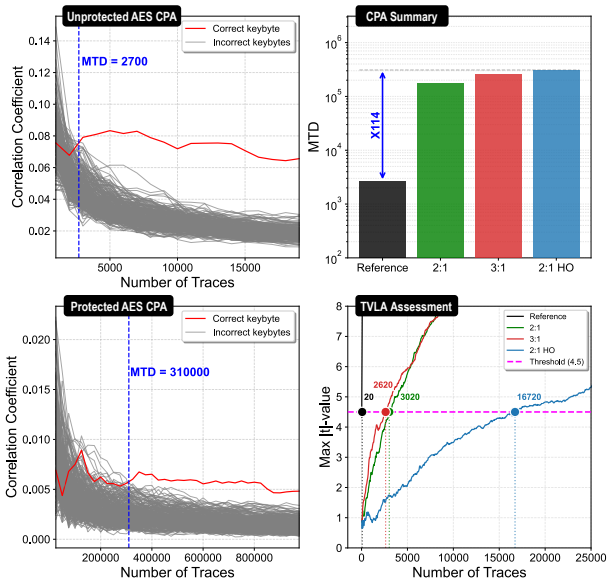


Fig. 5. Measured side-channel resilience.

TABLE I
STATE-OF-THE-ART COMPARISON.

			This Work			JSSC-10 [11]	VLSI-24 [6]	JSSC-19 [7]	OJSSCS-25 [10]	JSSC-21 [5]	VLSI-25 [9]
Additional Countermeasure			No			Switched capacitor current equalizer	Distributed supply + dynamic switching	Noise Injection	Constant current sink	NL-LDO + core modifications	Adaptative ML power compensation
Converter	Type		Capacitive			Capacitive	Inductive (off-chip)		LDO		
	Step –Down ratio		2:1	**3:1**	2:1HO	1:1	< 3:1	< 3:2	< 3:2	< 7:2	-
	Pk. Efficiency		84%	65%	72%	67%	88%	-	67%	71%	-
	Pwr. Den. (mW/mm^2)	w. passives	42			136[b]	-	-	5.7	-	<10[b][c]
		w/o. passives	809			340[b]	460	35	-	1100[b]	-
AES Power			0.7mW	0.26mW	0.46mW	33.3mW	-	13.1mW	0.275mW	11mW	-
Overheads [a]	Area		0%	0%	0%	20%	1.7%	6.6%	35%	>40%[b]	300%[b]
	Power		0%	**-50%**	**-18%**	20%	2.5%	3.5%	50%	8%	5%
	Perf.		0%	0%	0%	50%	0%	17.4%	0%	0.7%	0%
Power SCA Resilience	CPA	MTD	180k	275k	310k	>10M	>1M	900k	>200M	>1B	>1.8B
		xMTD	67	96	114	>2.5k	>1.25k	900	>87k	>125k	>180k
	TVLA	MTD	3k	2.6k	16.7k	-	-	-	5M	>250M	852M
		xMTD	150	130	750	-	-	-	500k	>250k	1M
FoM $xMTD_{TVLA,dB}/Area_{rel}/Power_{rel}$			22	**42**	**35**	16	30	23	28	35	14

[a]Excluding core converter following SoA convention [b]Estimated from die photo [c]Estimated considering a 10mW AES

Fig. 5 reports the results of standard side-channel evaluations, namely CPA and TVLA, which are also summarized in Table I. In time-domain last-round CPA, the correct key byte separates after 2.7 k traces for the unprotected AES (top left), whereas 310 k traces are required when the AES is supplied by the 2:1 HO topology (bottom left). The introduction of the SCC therefore improves the Minimum Traces To Disclosure (MTD) by 114×. Similar protection levels are observed for the 2:1 and 3:1 configurations (top right). TVLA is also performed to detect other possible leakage sources (bottom right). In this case, 16.7 k traces are required to distinguish the two datasets, compared to only 20 traces for the unprotected AES. The 2:1 HO topology again shows the best performance among the evaluated configurations, confirming that suppressing the direct input-to-output path strongly reduces exploitable leakage.

Table I compares this work with prior-art side-channel protection schemes based on voltage regulators. LDO-based solutions do not provide efficient step-down conversion and therefore cannot reduce AES power consumption at system level [9] [10]. Inductive converters generally rely on off-chip implementations, which introduce vulnerabilities through external inductor current probing and EM radiation. Capacitive approaches remain scarce; the only prior capacitive implementation provides a 1:1 conversion ratio with significant area, power, or performance penalties [11]. By contrast, the SCA resilience reported here is obtained solely from the intrinsic properties of SCC step-down conversion, without any additional dedicated countermeasure. A Figure-of-Merit combining xMTD with relative area and power overheads is therefore introduced, showing that SCCs are promising candidates for an intrinsic first line of defense with zero, or even negative, overhead.

IV. CONCLUSION

This work demonstrates that on-chip SCC topologies can simultaneously provide AES supply and intrinsic side-channel protection. Experimental results show that the baseline 2:1 SCC already improves CPA robustness with no additional overhead, while the 2:1 HO topology achieves the highest protection with 114× and 750× xMTD improvements for CPA and TVLA, respectively. In parallel, 3:1 voltage scaling reduces AES power consumption by up to 50%, resulting in a negative power overhead at system level. Overall, SCC-based power delivery appears as a promising first line of defense for future secure low-power integrated systems.

REFERENCES

[1] T. De Cnudde *et al.*, "Masking aes with d+1 shares in hardware," in *Cryptographic Hardware and Embedded Systems – CHES 2016*. Berlin, Heidelberg: Springer, 2016, pp. 194–212.

[2] S. Sen and A. Ghosh, "Circuit-Level Techniques for Side-Channel Attack Resilience: A tutorial," *IEEE Solid-State Circuits Magazine*, vol. 16, no. 4, pp. 96–108, 2024.

[3] W. Yu and S. Kose, "Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 2, pp. 244–257, Apr. 2018.

[4] J. Yang *et al.*, "Analysis of Shunt LDO With Physical Security to Power/EM Side-Channel Attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, pp. 1–14, 2026.

[5] R. Kumar *et al.*, "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*, vol. 56, no. 4, pp. 1141–1151, Apr. 2021.

[6] X. Liu and P. Ampadu, "A Fast Transient Response Distributed Power Supply With Dynamic Output Switching for Power Side-Channel Attack Mitigation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pp. 1–14, 2024.

[7] A. Singh *et al.*, "Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, Feb. 2019.

[8] N. Mirchandani *et al.*, "A High-Efficiency Power Obfuscation Switched-Capacitor DC–DC Converter Architecture," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 10, pp. 2868–2873, Oct. 2024.

[9] T. Wang *et al.*, "Online Learning-Based Countermeasure Against Power Analysis Attacks," in *2025 Symposium on VLSI Technology and Circuits (VLSI Technology and Circuits)*, Jun. 2025, pp. 1–3.

[10] A. Ghosh *et al.*, "R-STELLAR: A Resilient Synthesizable Signature Attenuation SCA Protection on AES-256 With Built-In Attack-on-Countermeasure Detection," *IEEE Open Journal of the Solid-State Circuits Society*, vol. 5, pp. 167–179, 2025.

[11] C. Tokunaga and D. Blaauw, "Securing Encryption Systems With a Switched Capacitor Current Equalizer," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010.