A High Efficiency Power Obfuscation Switched Capacitor DC-DC Converter Architecture

Nikita Mirchandani, *Member, IEEE,* Majid Sabbagh, *Member, IEEE,* Yunsi Fei, *Senior Member, IEEE,* and Aatmesh Shrivastava, *Senior Member, IEEE*

***Abstract*—Side channel attacks (SCA) have been shown to be very effective in breaking cryptographic engines. In this paper, we present a new power obfuscation switched capacitor (POSC) DC-DC converter. To a first order approximation, it equalizes the charge such that the same amount of charge is drawn from the input power supply in each cycle. We evaluated the design by analyzing the power supply to an Advanced Encryption Standard (AES) unit powered by the proposed converter. CPA fails after evaluation with $10k$ traces. Two different topologies of the switched capacitor circuit are analyzed for their contribution to side channel power information leakage. The three phase POSC is designed with both switched capacitor converters (SCC1 and SCC2) and achieves efficiency of 77% and 70%.**

***Index Terms*—Hardware Security, Side-channel Attack, Regulators, Switched-capacitor Converters, Power Management.**

I. Introduction

Cryptographic algorithms like Advanced Encryption Standard (AES) are used to protect the confidentiality of sensitive data. However, unprotected implementations of cryptographic engines show vulnerabilities to side channel attacks (SCA). Several countermeasures against power analysis attacks have been proposed. Domain Oriented Masking (DOM) or Threshold Implementations are popular digital logic based implementation. However, area of AES implementation increases by almost $3\times$ with unsecured AES taking about 2.3 kilo-gate equivalent (KGE) and an efficient DOM taking 6.6 KGE [1]. Charge recycling adiabatic logic [2] has been successfully used to prevent DPA attacks but it incurs higher area overhead. Other efforts involve masking [3], and hiding [4]. Other works use multi-phase interleaved switched capacitor converters (SCC) with randomized activation pattern [5], [6] and switched-capacitor current equalizers [7].

The first step in alleviating side channel power leakage is to integrate the AES power supply on-chip. Inductive voltage regulators (IVR), digital LDO and shunt regulator have been used to suppress the AES current signature. Switched capacitor (SC) converters are a better alternative for power obfuscation as they are easily integrated, achieve high power density, and efficiency but they can easily leak. Fig. 1-(a) shows the charge transfer operation in a SC converter. In the phase ϕ_1, C_F is charged from V_{IN}, and in phase ϕ_2, the charge is transferred to C_{OUT}. Since C_F is directly connected to the load in ϕ_2, it carries information about the load current through sampling.

N. Mirchandani is with Intel, USA. M. Sabbagh is with Google, USA. Y. Fei, and A. Shrivastava are with the Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 02115, USA. E-mail: (mirchandani.n@northeastern.edu; sabbagh.m@northeastern.edu, yfei@ece.neu.edu, aatmesh@ece.neu.edu).

This work is supported in part by Center for Hardware and Embedded Systems Security and Trust (CHEST), and National Science Foundation (NSF) under grant ECCS 2125222 (*Corresponding Author: Aatmesh Shrivastava*)

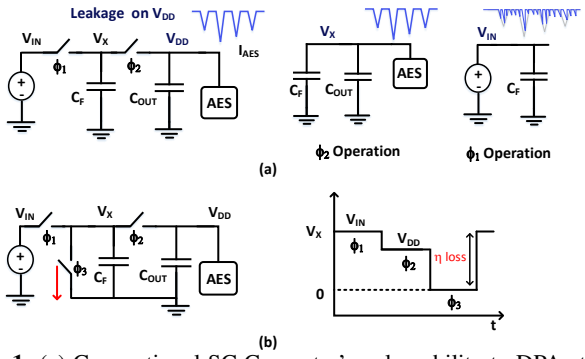


Fig. 1: (a) Conventional SC Converter's vulnerability to DPA attacks (b) Modified converter with shunt switch to prevent leakage

When C_F reconnects with the input in the next cycle, the load current information carried by C_F is available at the input node, which can be probed by the attacker. It can be secured by discharging C_F to ground in each cycle [7] as shown in Fig. 1-(b), ensuring that same charge is drawn in each cycle. However, recharging C_F leads to increased power loss, reducing the efficiency of the converter.

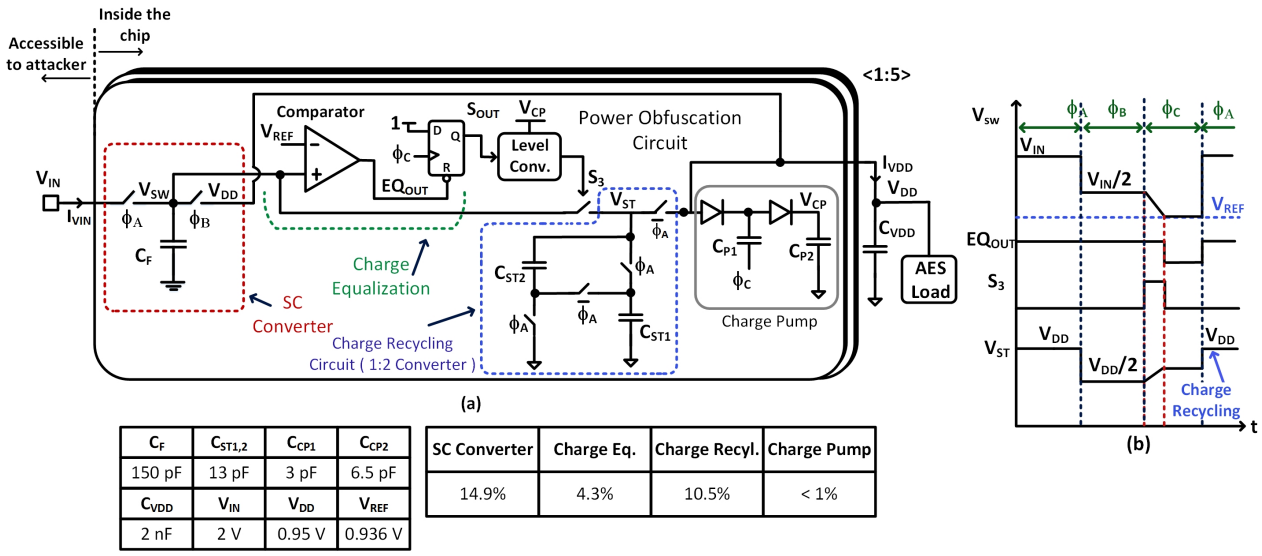
In this paper, we propose a new power obfuscation switched capacitor (POSC) converter that prevents side-channel leakage by drawing the same amount of charge using charge recycling. The POSC is designed with two switched capacitor converters (SCC1 and SCC2) to asses the effect of converter topology on leakage. Simulations on $10k$ AES traces did not reveal any byte of the secret key after Correlation Power Analysis (CPA).

II. Proposed Switched Capacitor Converter

The proposed architecture is shown in Fig. 2. It consists of a typical SC converter to power the AES load, a charge-equalization circuit, and a charge-recycling circuit to prevent excessive power loss and improve efficiency.

A. Architecture Overview

The proposed POSC converter works in three phases. In the first two phases ($\phi_{A,B}$), a typical 2:1 converter provides the power to the AES load, and the third phase (ϕ_C) is used for power obfuscation. In the beginning of ϕ_C, $C_{ST1,2}$ are at $V_{DD}/2$ while C_F is at V_{DD}. The comparator compares the voltage on C_F, V_{SW} with V_{REF} and enables switch S_3 which connects C_F to the parallel combination of C_{ST1} and C_{ST2}. Hence, V_{SW} starts discharging and raising the level of V_{ST} as shown in Fig. 2-(b). Once V_{SW} crosses V_{REF}, switch S_3 is disabled. In the next cycle, ϕ_A, C_F connects to V_{IN}, while C_{ST1} and C_{ST2} are connected in series to dump the extra charge back on V_{DD}. As C_F is always set to a fixed voltage before drawing charge from V_{IN}, it will draw the same charge in each switching cycle. The design also uses a charge-pump



(c)

C_F	$C_{ST1,2}$	C_{CP1}	C_{CP2}
150 pF	13 pF	3 pF	6.5 pF
C_{VDD}	V_{IN}	V_{DD}	V_{REF}
2 nF	2 V	0.95 V	0.936 V

(d)

SC Converter	Charge Eq.	Charge Recyl.	Charge Pump
14.9%	4.3%	10.5%	< 1%

Fig. 2: (a) Proposed POSC converter circuit for power obfuscation, (b) transient waveforms showing operation of POSC circuit, (c) device sizes, and (d) percentage power-loss of each block in the POSC converter.

to realize $2 * V_{DD}$ supply and level-converters to generate control voltages at V_{DD} and $2 * V_{DD}$ levels. This is done to avoid using V_{IN} for generating control signals which can pose a potential leakage point. The design of various circuit blocks for the POSC converter is described below.

SCA Resilience: The circuit achieves SCA resilience by both suppressing the signal as well as introducing additional random noise in the signal. The comparator and other circuits in the charge equalization block presents large gain ($>$ 60dB) in a negative feedback loop. Due to this negative feedback, the SCA signal which will appear at V_{SW}, is suppressed. Additionally, the comparator and other circuits will also present an input referred noise due to their device noise. The combined effect of these two factors reduces the signal to noise ratio (SNR) making SCA more difficult to accomplish.

B. 2:1 Converter

The architecture of the 2:1 converter can affect the side channel leakage of the POSC, and is discussed in Section III. The first two phases (ϕ_A and ϕ_B) implement typical operation, and no charge is transferred to the load in the third phase (ϕ_C). In steady state, flying capacitor C_F draws only small amount of charge from the input node in each phase ϕ_A.

C. Charge Equalization

The comparator performs a critical part in charge equalization, ensuring V_{SW} is discharged to the same voltage in every cycle. However, nonidealities in the comparator create second-order effects which can cause variation in the V_{SW} value. If the comparator delay is large and varies with load current, the amount of charge taken from C_F will vary, leaking both timing and power information. Similarly, if V_{SW} is higher due to offset, the comparator won't trip in some load scenarios leading to leakage. If V_{SW} is lower due to offset, the efficiency will decrease. The circuit architecture of the comparator is shown in Fig. 3-(a). The first two stages are fully differential resistive load amplifiers, drawing a DC current from V_{IN}. They provide gain of 38dB and consume 12μA bias current. The third stage is powered from V_{SW} for additional compensation and reduced power consumption. The comparator is only enabled in phase ϕ_C, and is disabled once it trips. Fig. 3-(b) shows the variation in input current of the POSC showing an equalized input current being drawn from V_{IN}. Fig. 4-(a) shows the variation in $V_{SW,f}$ (final value of V_{SW} after equalization in phase ϕ_C). It shows a low variation of less than $650\mu V$ for load variation of 5.5mA to 6.5mA.

Noise enhances side channel resilience by adding randomness to the side channel measurements. We simulated the variation of $V_{SW,f}$ at 6mA load with transient noise integrated up to 200MHz. Fig. 4-(b) shows that $V_{SW,f}$ shows standard deviation of $377\mu V$ in the presence of noise. Fig. 4-(a) shows the variation of $V_{SW,f}$ with AES load variation. The AES leakage point corresponds to the load range of 5.5-6.2mA (inset histogram) corresponding to a $V_{SW,f}$ variation of $400\mu V$. The level of noise seen on $V_{SW,f}$ is comparable to its variation with AES load. The noise source is the comparator which randomizes the trip point for V_{SW}.

In phase ϕ_C, capacitors C_F and $C_{ST1,2}$ are connected. In the absence of control from the comparator, node V_{ST} reaches a final value of V'_{ST} which is equal to $\frac{C_F}{C_F+C_{ST1}+C_{ST2}}V_{SW}$. Since V_{SW} is load dependent, V_{REF} must be in the range $[V'_{ST}, V_{SW}]$ for all possible load currents. A lower value of V_{REF} results in lower efficiency.

D. Charge Recycling Block

The extra charge from the switching node is stored on storage capacitors C_{ST1} and C_{ST2} connected in parallel. In phase ϕ_A, they are connected in series to raise their voltage above V_{DD}, to enable charge transfer to V_{DD}.

E. Control Logic and Level Converter

Switch S_3 turns on at the start of phase ϕ_C, and is turned off once the comparator output EQ_{OUT} goes low. The comparator output and control signals operate on a supply of less than $V_{IN}/2$, which is the voltage of C_F in phases ϕ_B and ϕ_C. This voltage is too low to drive the gate of switch S_3. Hence,

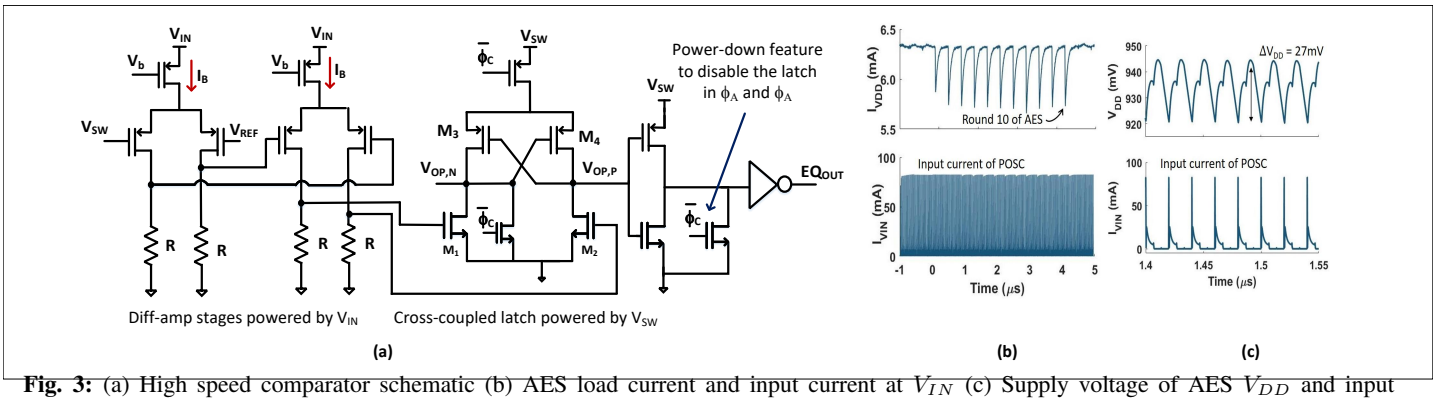


Fig. 3: (a) High speed comparator schematic (b) AES load current and input current at V_{IN} (c) Supply voltage of AES V_{DD} and input current at V_{IN} showing periodicity

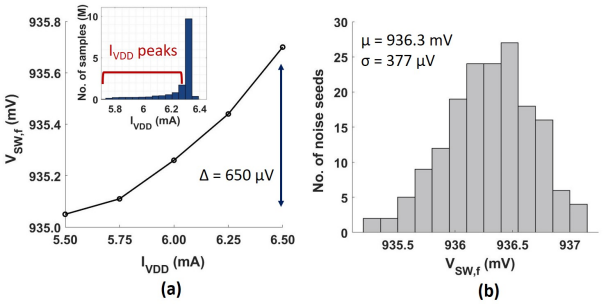


Fig. 4: (a) Variation of $V_{SW,f}$ with varying DC load current I_{VDD} (b) Variation of $V_{SW,f}$ with transient noise for a DC load of 6mA

a level converter is designed to shift the control logic output voltage level from V_{DD} to 2V level.

F. Charge Pump

Switch S_3 is directly controlled by the level converter. If the level converter is supplied by the external power V_{IN}, power information will be leaked out. Hence, an internal supply is provided by a two stage charge pump shown in Fig. 2-(a). The input of the charge pump is provided by V_{DD} ($\approx$ 1V), and an output voltage of 1.65V is obtained, which is enough to drive switch S_3 implemented using deep-nwell n-MOS.

III. Design Considerations

A. Switched Capacitor Converter Topology

The choice of 2:1 converter plays a critical role in preventing side channel leakage. The conventional 2:1 switched capacitor converter (SCC1) is shown in Fig. 5-(a). In phase ϕ_A, the input V_{IN} is directly connected to the output node V_{DD} through the capacitor C_F. Hence, even though capacitor C_F has the same charge on it at the start of the cycle in phase ϕ_A, the POSC can leak information as there is a direct path between V_{IN} and V_{DD}. To prevent this leakage, V_{IN} and V_{DD} should be isolated from each other. One such design is shown in Fig. 5-(b). Capacitors C_{F1} and C_{F2} are equal, and are connected together in phase ϕ_A. In this phase, the AES load is disconnected from the input. In phase ϕ_B, both C_{F1} and C_{F2} are connected in parallel and supply the AES load. In this phase, V_{IN} is disconnected from the 2:1 converter. In phase ϕ_C, the charge equalization operation takes place, discharging V_{SW} to V_{REF}. In all phases of operation, V_{IN} and V_{DD} are isolated, and hence there is no path for leakage current to flow through V_{IN}. We have used SCC2 in the POSC converter to reduce leakage at the expense of efficiency.

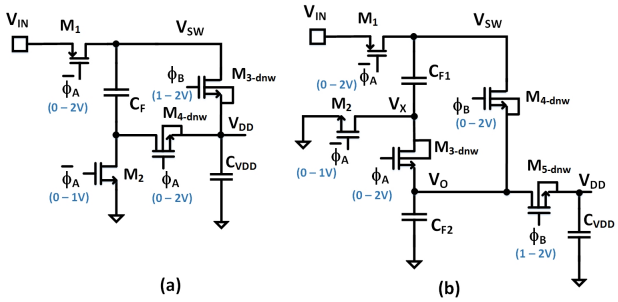


Fig. 5: (a) High efficiency 2:1 SC converter (SCC1) (b) Leakage resilient 2:1 SC converter (SCC2)

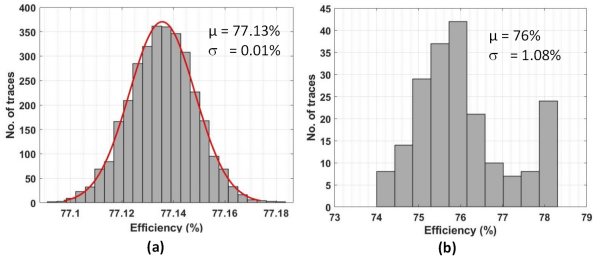


Fig. 6: (a) Efficiency histogram after 5k traces for POSC Converter designed using SCC1 (b) Efficiency histogram of POSC Converter with process variation for 200 samples.

B. Input Resistance

The amount of current drawn from the input node V_{IN} depends on the input resistance of the SC converter. To obtain constant peak current, R_{ON} must be constant in phase ϕ_A. Fig. 5 shows SCC1 and SCC2, along with the voltage swings of the control signals. A voltage swing of V_{DD} to V_{IN} is sufficient for switch M_1 to turn on in phase ϕ_A. The channel resistance R_{ON} of switch M_1 is given by

$$R_{ON} = \frac{1}{\mu_P C_{OX} \frac{W}{L}(V_{IN} - V_{DD} - V_{th})} \quad (1)$$

As the load current varies, V_{DD} varies as well, varying R_{ON}. Hence, the POSC starts to leak information at the input node. Constant R_{ON} in ϕ_A is achieved by making the control signal for M_1 swing from 0 to V_{IN}. It removes the dependency of input resistance on the load current at the cost of efficiency.

C. Switch Design

The second order effects resulting from the switch design in the SCC2 also contribute to the side channel leakage. In phase ϕ_C, both C_{F1} and C_{F2} get discharged to C_{ST1} and

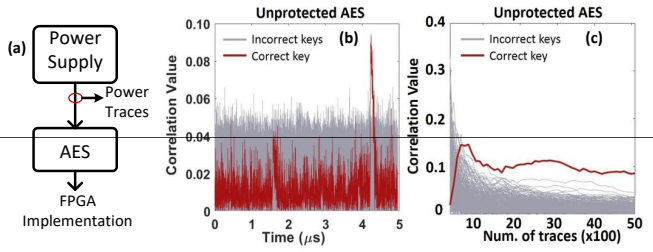


Fig. 7: CPA analysis method. (a) Acquiring unmasked AES power traces from FPGA. Unmasked AES unit showing the correlation coefficient of the correct and incorrect keys as a function of (a) time (b) number of traces.

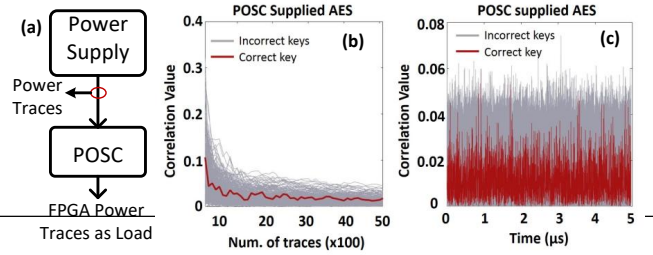


Fig. 8: CPA Analysis. (a) Acquiring power traces with AES-FPGA traces as load. Result showing the correlation coefficient of the correct and incorrect keys as a function of (a) time (b) number of traces.

C_{ST2}. Since M_2 and M_4 are both on, the on resistances of these two switches affect the amount of current flowing out of C_{F1} and C_{F2}. To ensure both the capacitors get discharged at an equal rate, switches M_2 and M_4 must be designed such that their on resistances are equal.

IV. Results

A. POSC Performance Evaluation

We designed the POSC converter in 65nm CMOS with a switching frequency of 50 MHz. It combines 5 parallel converters each optimized to drive a 1.2mA load. Fig. 6-(a) shows the variation of POSC efficiency with SCC1 across $5k$ power traces, achieving an efficiency of 77.1%. Fig. 6-(b) shows the efficiency variation of the POSC converter across statistical process variation showing a 3-σ variation of 3%. The comparator, charge-pump, $1:2$ converter and the control circuit incur an overhead of 25% over the SCC1 $2:1$ converter.

B. SCA Evaluation

We implemented an unmasked AES on FPGA and obtained the power traces. Fig. 7-(a) shows the power traces obtained from an unmasked AES implementation on a Sasebo-GII board, with a Xilinx Virtex-5 FPGA. These are used as a load current for the POSC converter. To recover the last-round AES key from the power traces byte by byte, we performed CPA with a power model of Hamming distance between the output cipher byte and the last round input state byte. The most leaky time-point is at 4.226μs, and CPA is applied at this point from all the traces. By finding the maximum correlation between the power consumption and predicted power under different key byte guesses, the correct key byte value is retrieved.

When the FPGA was powered using a DC supply, 100 power traces were sufficient to recover the key bytes, as seen in

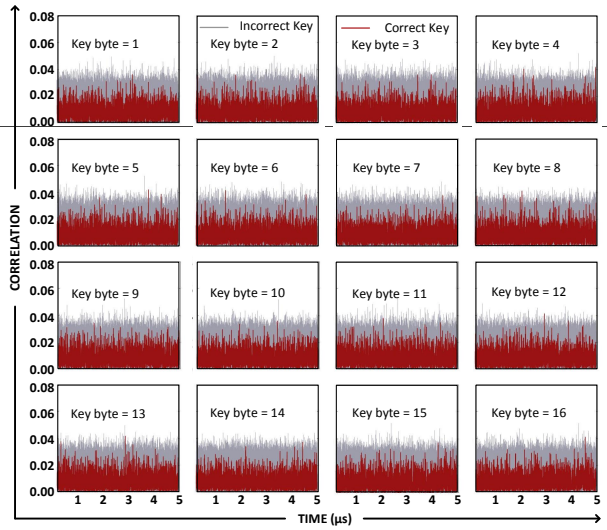


Fig. 9: Correlation coefficient of the correct and incorrect keys as a function of time for all 16 bytes of the SCC2 POSC.

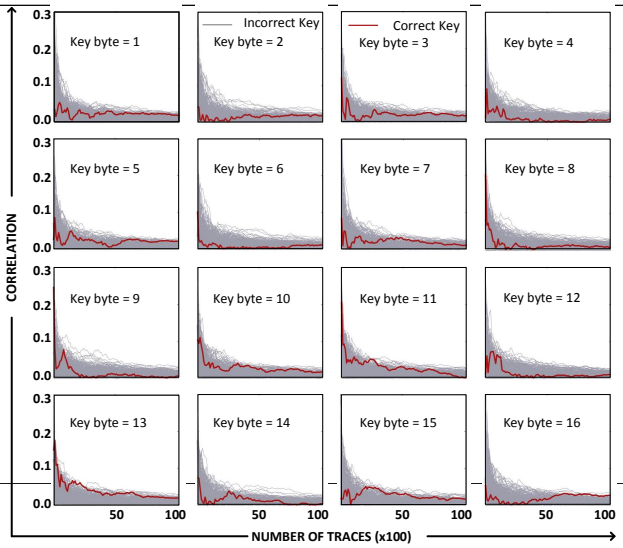


Fig. 10: Correlation coefficient of the correct and incorrect keys as a function of number of traces for all 16 bytes of the SCC2 POSC.

Fig. 7. To evaluate the performance of POSC, we applied the power traces obtained from FPGA (Fig. 7-(a)) as load to the POSC as these capture the power variation of an unmasked AES. Limited by the prohibitively long simulation time (1 trace took approx. 1 hour to simulate) of the POSC converter, SCC1 was evaluated with $5k$ traces, while SCC2 was evaluated with $10k$ traces as it is more robust against SCA. When the AES unit is powered from the POSC converter with SCC1, the key cannot be extracted even with $5k$ traces, as seen in Fig 8. The equivalent noise current sampled at the input V_{IN} is estimated from the noise variation seen at $V_{SW,f}$ (Fig. 4-(b)). Transient noise is enabled while evaluating the POSC converter and added to the traces prior to CPA evaluation. We introduce noise in the traces which captures device and set-up noise. Normally distributed random numbers were generated to generate a 75μV-rms equivalent noise which was added to the traces. The POSC converter is also evaluated for leakage with the SCC2 converter, which is more leakage resilient as it

TABLE I: POSC Performance comparison

	JSS'10 [7]	CIC'20 [8]	JSS'20 [9]	VLS'15 [2]	TVLS'21 [10]*	**This work***
Topology	SC	CDSA	Dig. LDO	BBL	SC	**SC**
Tec.(nm)	130	65	130	65	28 nm	**65**
Attack	DPA	ML-SCA	CPA TVLA	DPA	TVLA	**CPA/TVLA**
AES	128b	256b	128b	128b	256b	**128b**
Pow.(mW)	33.3	0.8	10.9	138		**6**
Area Over.(%)	25	36.7	36.9	25	16	25
Power Over. (%)	33	49.8	32 $\eta = 68$	30	15 $\eta \approx 85$	**13–20** $\eta = 77$–70
MTD CPA	>10M	>10M	6.8M	0.52M	2K	**5K / 10K**
Trace# / t-Peak	NA	NA	100K/21	NA	2K	**2K/14**

**Simulation-based Results*

has no direct path for current between V_{IN} and V_{DD}. Fig. 9 shows the correlation coefficient for both correct and incorrect keys for all 16 key bytes for 10k traces when the POSC was evaluated with SCC2. Fig. 10 shows the correlation coefficient for all 16 key bytes against number of traces.

Table I compares the proposed work with state-of-the-art power side channel resilient hardware designs. Simulation result of our work indicates that POSC can achieve highest reported efficiency of 77% with significantly lower power overhead. The POSC shows no leakage after evaluating 10k traces. Fig. 11-(a) shows the layout of the proposed POSC circuit. Compared to a conventional SC converter, POSC uses additional comparator, charge-recycling and charge-pump circuits which consume additional 25% area. Further, owing to the power consumption in these circuits, the efficiency of the converter further decreases by 13% and 20% compared to a conventional SC. The additional area and power overhead helps in achieving high SCA resilience.

Fig. 11-(b) shows the Monte-Carlo process variation simulation of critical V_{SW} node which carries the leakage information. The Monte-Carlo simulation includes normal distribution of total variation for all transistors. The simulation is carried out with a long duration of ϕ_C to enable comparator switching across corners. Results show only a few mV variation across process and min-max load variation. This high stability of V_{SW} will help in achieving high SCA resilience. To further improve the performance, conventional calibration methods can be used to tune the comparator across process corners to operate it at optimized frequency for best output efficiency.

We also evaluated our design using test-vector leakage analysis (TVLA). Fig. 12 shows that POSC achieves a TVLA peak of 14 with 2k traces compared to 152 obtained from unprotected AES. Our design achieves comparable or better TVLA result compared to other SCA resilient designs. Measurement of SCA resilient regulator designs have shown TVLA peak of 41 with 1K trace [11], 21 with 100K trace [9] and shows leakage with 2K traces in [10].

V. Conclusion

This paper presents a 2:1 switched capacitor converter with power obfuscation to protect against SCA. Two topologies of the SCC are evaluated. A charge equalization circuit ensures that the flying capacitor is always charged from a fixed voltage level which prevents internal switching patterns to leak outside. A charge recycling technique recycles the extra charge drawn from the flying capacitor back to the AES supply improving the efficiency of the POSC converter. It achieves an efficiency of 70% and has an area overhead of 25%. SPICE simulation based CPA on the POSC showed no side channel leakage with 10k-traces and peak TVLA of 14 with 2k traces.

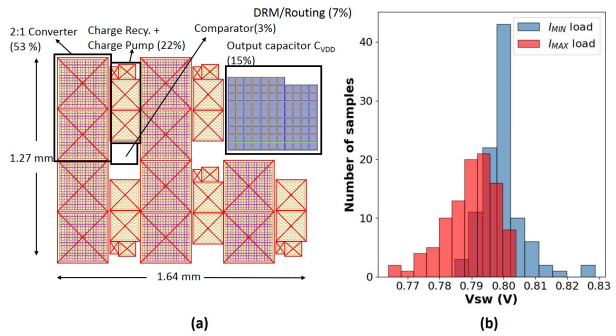


Fig. 11: (a) Layout of POSC converter with 5 parallel units (b) Process variation for minimum and maximum DC load

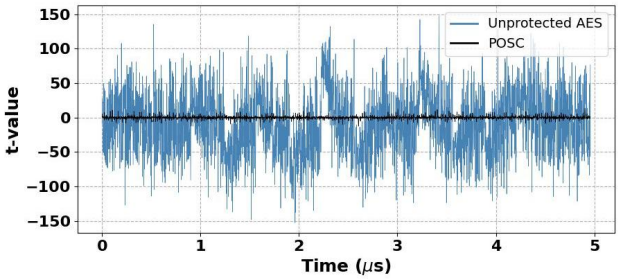


Fig. 12: TVLA simulation results with 2k traces

References

[1] A. Waage, *Secure Implementation of a RISC-V AES Accelerator*. PhD thesis, 2022.

[2] S. Lu, Z. Zhang, and M. Papaefthymiou, "1.32GHz high-throughput charge-recovery AES core with resistance to DPA attacks," in *VLSI Circuits*, pp. C246–C247, 2015.

[3] S. Nikova, V. Rijmen, and M. Schläffer, "Secure hardware implementation of nonlinear functions in the presence of glitches," *Journal of cryptology*, vol. 24, no. 2, pp. 292–321, 2010.

[4] W. Shan, X. Fu, and Z. Xu, "A secure reconfigurable crypto ic with countermeasures against spa, dpa, and ema," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 7, pp. 1201–1205, 2015.

[5] O. A. Uzun and S. Köse, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 4, no. 2, pp. 169–179, 2014.

[6] W. Yu, O. A. Uzun, and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, 2015.

[7] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *JSSC*, pp. 23–31, 2010.

[8] D. Das, J. Danial, A. Golder, S. Ghosh, A. R. Wdhury, and S. Sen, "Deep learning side-channel attack resilient aes-256 using current domain signature attenuation in 65nm cmos," in *CICC*, pp. 1–4, 2020.

[9] A. Singh, M. Kar, V. C. K. Chekuri, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Enhanced Power and Electromagnetic SCA Resistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO," *JSSC*, vol. 55, no. 2, pp. 478–493, 2020.

[10] R. Jevtic, M. Ylitolva, C. Calonge, M. Ojanen, T. Santti, and L. Koskinen, "Em side-channel countermeasure for switched-capacitor dc–dc converters based on amplitude modulation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 6, pp. 1061–1072, 2021.

[11] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "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, 2019.