Physical Design Strategies for Mitigating Fine-Grained Electromagnetic Side-Channel Attacks

Meizhi Wang[1], Vishnuvardhan V. Iyer[1], Shanshan Xie[1], Ge Li[1], Sanu K. Mathew[2], Raghavan Kumar[2], Michael Orshansky[1], Ali E. Yilmaz[1], and Jaydeep P. Kulkarni[1]
[1]University of Texas, Austin, TX, [2] Intel Labs, Hillsboro, OR
E-mail: wang.mz@utexas.edu, jaydeep@austin.utexas.edu

Abstract: We present physical design strategies viz. (i) power grid shielding, (ii) power grid twisting, (iii) increased local decoupling capacitors with VSS shields, and (iv) isolated S-Box module placement to improve the resilience of the Advanced Encryption Standard (AES-128) cryptographic core against fine-grained electromagnetic (EM) side-channel analysis (SCA). Localized EM field measurements are performed using a 0.5 mm radius H-field probe on 3 different, 40nm CMOS test-chips implementing 9 physical design configurations of the AES core. These physical design strategies show 2.45x, 1.51x, 2.61x, and 2.71x higher measurements to disclosure (MTD) respectively compared to the baseline design without incurring any power overhead. These strategies can be applied independently or optimally combined further improving fine-grained EM SCA resilience.

Need for fine-grained EM SCA techniques: Data-dependent current switching causes information leakage through both EM and power side-channels in cryptographic modules [1]. Compared to power attacks, EM SCA attacks are non-invasive and can be more potent. Typically, countermeasures against EM SCA focus on coarse-grained measurements using large-diameter EM probes [2]. Such attacks have very low signal-to-noise ratio (SNR), as signals from information-leaking blocks are obfuscated by uncorrelated sources picked up by the probe resulting in a spatial-averaged EM profile. Fine-grained EM SCA attacks, on the other hand, scan a chip's surface using small probes in multiple orientations and can isolate high SNR configurations to recover secure information at a significantly lower cost [3]. Simulations of fine-grained EM SCA attacks [4] using an EM probe of 50 μm diameter and placed 75 μm above an AES core, show that most of the 16 key bytes can be revealed within 1000 traces at 3 different locations (Fig. 1a-1d). EM waveforms at optimal locations can further reduce measurements to disclosure (MTD) of key bytes, although with higher simulation cost. In this work, we systematically demonstrate four physical design strategies to mitigate fine-grained EM SCA vulnerability at no power cost and controlled area increase.

Physical design strategies for fine-grained EM SCA resilience:

1. Power grid shielding: The EM emanations originating from leaking components in an AES core can be minimized by inserting internal metal shields. Four AES cores having different power grid designs are implemented in Chip-1 (Fig. 2a). The baseline AES core (Design-1) floorplan is done with a flattened netlist using M1-M6 metal layers. Design-2 and Design-4 are built upon the baseline Design-1 but insert additional power/ground tracks in M7 and M8 metal layers. Design-2 adds 8 sets of 3 μm wide power grids on M7 and 8 sets of 4 μm power grids on M8 layer for both VDD and VSS rails. Design-4 adds 8 vertical 12 μm M8 VSS stripes and 8 horizontal 10 μm M7 VSS stripes which are shorted with via-7. These top two metal layers act as robust VSS shields and are connected to the VSS power ring outside the AES core.

2. Twisted power grids: In a conventional power grid, VDD and VSS metal lines are arranged in parallel. The supply current and the ground return current flows in opposite directions and generates EM fields surrounding the metal tracks. The magnetic field lines due to these two power grid lines carrying currents in opposite directions are canceled partially at far ends but add up in the middle which can be readily sensed by optimal positioning of the EM probe and can reveal the underlying data-dependent signature. We propose the use of twisted power grids to mitigate the fine-grained EM SCA vulnerability (Fig. 2b). Design-3 adds a twisted power grid with 8 sets of 2.5 μm power grid on M7 while leaving some space for cross-layer twisting from above M8 layer and 8 sets of 4 μm VDD and VSS stripes which are twisted 7 times along Y-direction on M8 layer over the AES core. The periodic M8 layer power grid twisting can cancel the local EM fields symmetrically along the x- and y-orientations (Fig. 2c-2d).

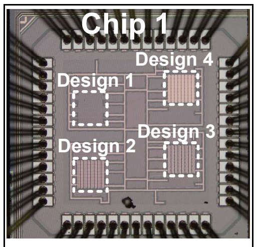


Fig. 7 Chip-1 die photo showing 4 AES cores

3. Local decoupling capacitors: The EM emanations from the AES core can be minimized by lowering the peak switching current which attenuates the SNR. This can be achieved by enabling a local energy storage in the form of standard-cell-based decoupling capacitors (Decap). Decap cells are implemented as MOSFET capacitors and are placed adjacent to logic gates performing AES computations. Design-5 (Fig. 3a) implements extra Decap cells consisting of a total of ~15 pF capacitance while incurring 20% larger area. Design-6, 7, and 8 are built upon Design-4 and include M7-M8 layer shields. Design-6 adds dense 4 μm wide M7 and M8 VSS shield which is connected to power ring outside AES core. Design-7 increases the width of VSS shielding stripes to 10 μm on M7 and 12 μm on M8; Design-8 removes Via-7 to make two M7 and M8 shielding VSS layers isolated from each other over the AES core.

4. Isolated S-box module placement: During the AES execution, the Substitute-Byte (S-Box) modules execute in parallel for all 16 bytes (Fig. 3b). If all S-box logic is randomly placed, it can create one large current path due to the concurrent operation creating high SNR. Design-9 separates S-box and Mix-Column modules and place them in 5 by 5 matrix evenly across the AES core (Fig. 3c). Isolating S-box modules results in shorter current paths inside each module, lowering the SNR, thus improving fine-grain EM SCA resilience.

Measurement results: Fig. 4a and Fig. 7 show die-photographs of 3 different 40nm CMOS test-chips implementing a total of 9 physical design strategies for the AES core to improve fine-grained EM SCA resilience. The fine-grained EM SCA attacks are implemented using a high-fidelity EM measurement setup (Fig. 4b) and an adaptive acquisition protocol which rapidly isolates potent measurement configurations [3]. The protocol is split into two phases – phase-I identifies initial configurations to recover key bytes from the AES module and phase-II performs multiple, progressively constrained scans using a greedy search algorithm on the configurations identified by phase-I, to identify the most optimal configuration. To observe the effect of countermeasures on probe orientation, phase-II scans are performed using a probe in x- and y-orientations. For each byte b, the orientation o with the lower MTD_b^o is chosen as the final MTD_b cost of recovering that byte. The automated, high-fidelity measurement setup (Fig. 4b) uses a 0.5 mm radius H-field probe, at a height of 0.1 mm above the package, scans an area of 8 mm × 8 mm (Fig. 5a), and uses a 30 dB amplifier to boost the captured EM signal strength. An MTD map is generated for each scan (Fig. 5b) and the MTD_b^o is quantified by monitoring the correlations. EM measurements show that for the baseline design, (Design-1) the peak-to-peak voltage on the last encryption cycle is ~110mV (Fig. 5c), the first byte requires $\mathrm{MTD}_1 = 2520$ measurements (Fig. 5d) and the total cost of recovering all keys is $\sum_{b=1}^{16} \mathrm{MTD}_b = 34650$ measurements (Fig. 6a). The baseline design, with the smallest peak-to-peak voltage due to vacant M7 and M8 layers, still recovers keys with the lowest cost (Fig. 6b). EM signal amplitude does not show a linear relationship with MTD demonstrating that reduced EM sensor amplitude does not necessarily increase EM SCA resilience (Fig. 6b). Creating a dense metal grid (Design-2) improves total MTD by 1.15x which further improves to 2.45x with wider VSS shields (Design-4) (Fig. 6c). Twisted lateral power grids improve fine-grain EM SCA resilience by 3x along the Y-direction and by 1.5x along the X-direction (Design-3). This suggests that power grid twisting along lateral as well vertical directions can be robust against both X and Y directional EM SCA. Adding local Decaps increases resilience by 1.3x (Design-4) which can be improved to 2.67x by additional top metal shields (Design-8). Isolating S-box placement increases EM SCA resilience by 2.7x (Design-9). These physical design strategies do not incur power overhead (Fig. 4c).

Acknowledgments: This research is supported in parts by Intel, Silicon Labs, and NSF. Authors thank TSMC for chip fabrication.

References: [1] Mangard, *et al*., 2007 [2] G. Ding, *et al., WMWA*, 2009 [3] V. V. Iyer, *et al. WMCS*, 2019 [4] A. Kumar, *et al. ICCAD*, 2017

978-1-7281-7581-2/21/$31.00 ©2021 IEEE

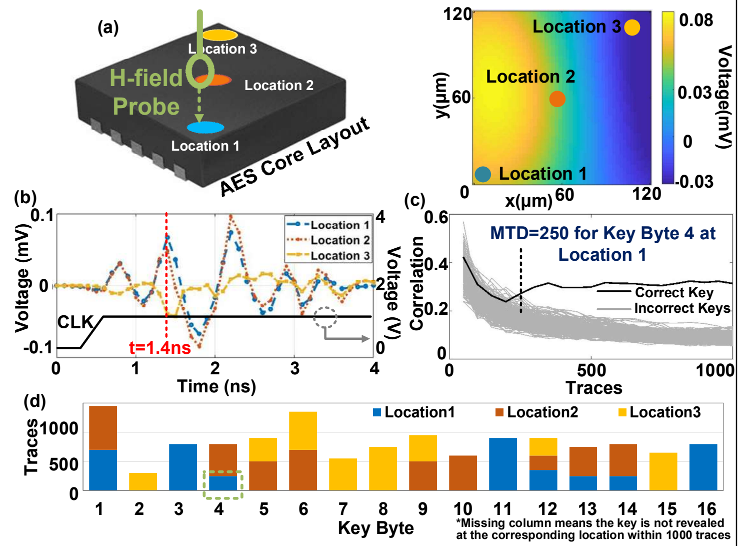


Fig. 1. (a) Fine-grained EM simulation on the AES core layout, EM emanation map at t=1.4 ns (b) Simulated waveforms at 3 locations across a 4 ns attacking window (c) EM SCA results of Key Byte 4 at location 1 for illustration (d) MTD of 16 Key Bytes at 3 locations

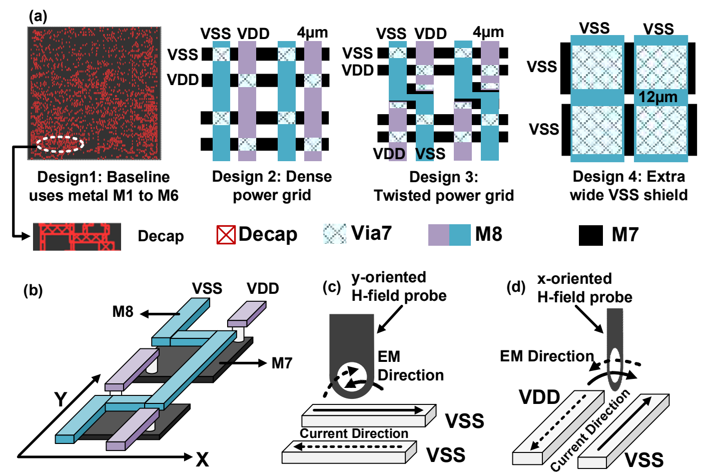


Fig. 2. (a) Design-1 to Design-4, implemented in Chip-1, explore different power grid design strategies for improving fine-grained EM SCA resilience (b) Twisted power grid shown in 3-D illustration (c) Current flowing in X-direction generating/cancelling EM fields measured using y-oriented probe (d) Current flowing in Y-direction generating/cancelling EM fields measured using x-oriented probe

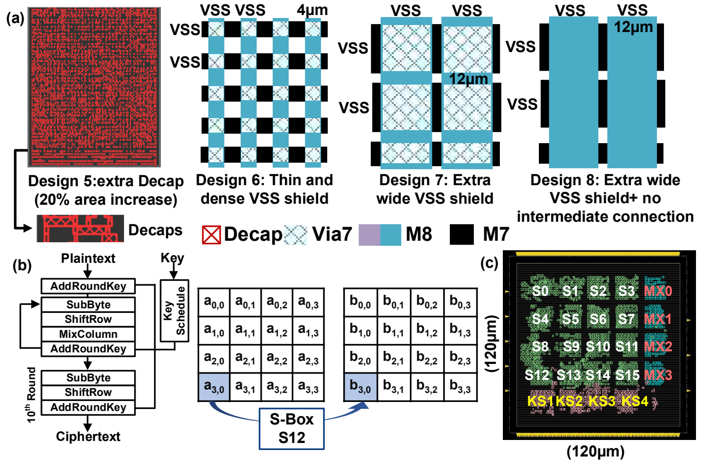
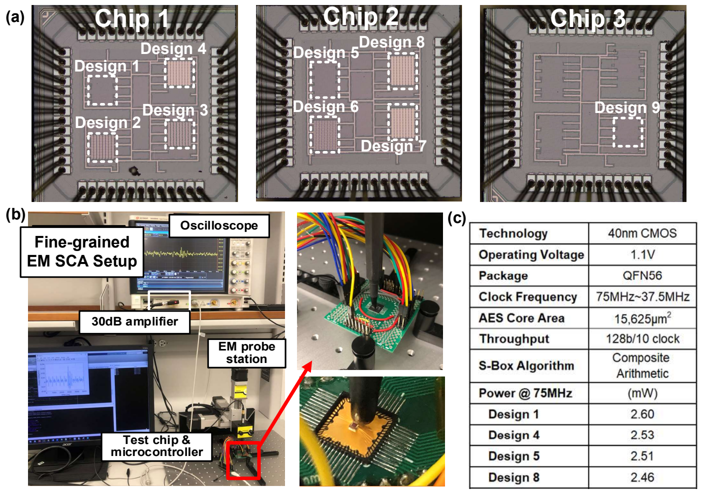

(a)
VSS VSS 4μm
VSS
VSS
VSS VSS
VSS
VSS
12μm
VSS VSS
12μm
VSS
VSS
Design 5:extra Decap (20% area increase)
Design 6: Thin and dense VSS shield
Design 7: Extra wide VSS shield
Design 8: Extra wide VSS shield+ no intermediate connection
Decaps
Decap
Via7
M8
M7
(b)
Plaintext
Key
AddRoundKey
SubByte
ShiftRow
MixColumn
AddRoundKey
Key Schedule
10th Round
SubByte
ShiftRow
AddRoundKey
Ciphertext
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S-Box S12
(c)
S0 S1 S2 S3 MX0
S4 S5 S6 S7 MX1
S8 S9 S10 S11 MX2
S12 S13 S14 S15 MX3
KS1 KS2 KS3 KS4
(120μm)
(120μm)

Fig. 3. (a) Design-4 to Design-8, implemented in Chip-2, explores Decap cells and VSS shield for improving fine-grained EM SCA resilience (b) AES encryption flowchart and SubByte step illustration (c) Design-9: Isolated S-Box placement (Chip-3): AES core layout showing S-Box (S*), MixColumn (MX*), and Key Schedule (KS*) module locations



Technology	40nm CMOS
Operating Voltage	1.1V
Package	QFN56
Clock Frequency	75MHz~37.5MHz
AES Core Area	15,625μm^2
Throughput	128b/10 clock
S-Box Algorithm	Composite Arithmetic
Power @ 75MHz	(mW)
Design 1	2.60
Design 4	2.53
Design 5	2.51
Design 8	2.46

Fig. 4. (a) Die photos of Chip 1: power grid designs, Chip 2: Decap cells with VSS shield designs, and Chip-3: isolated S-Box placement design (b) Fine-grained EM SCA setup, closeup photo of the EM probe with the packaged and de-packaged chip (c) AES core design parameters and measured power consumption

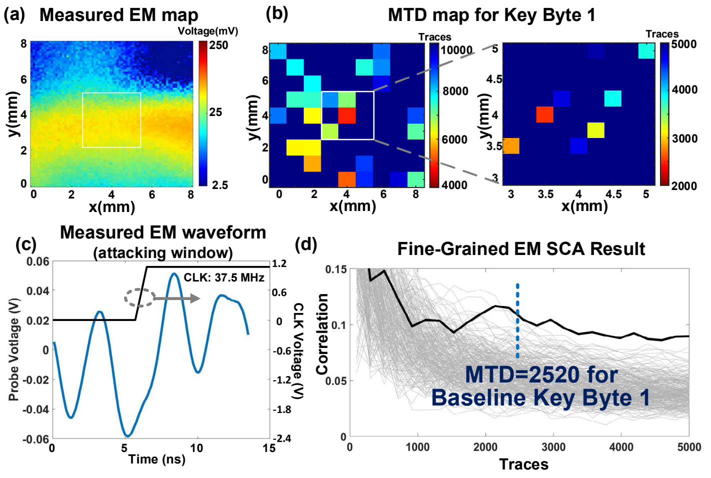
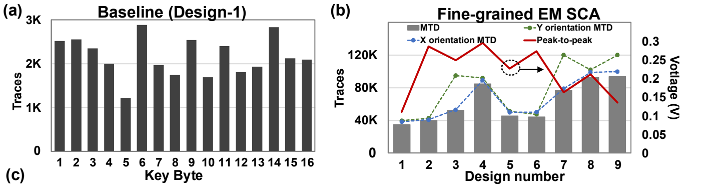


Fig. 5. Fine-grained EM SCA on baseline (Design-1) (a) Observed EM emanations at 101 × 101 locations across the package in x-orientation (b) MTD map for Key Byte 1 across the package for phase-I and phase-II (c) Observed EM trace at the package center (d) Correlation result for Key Byte 1 for illustration



Design #	Design strategy	$\sum_{b=1}^{16} \mathrm{MTD}_b^y$	$\sum_{b=1}^{16} \mathrm{MTD}_b^x$	$\sum_{b=1}^{16} min\{\mathrm{MTD}_b^x, \mathrm{MTD}_b^y\}$	Improvement compared to Design 1
Design 1	Baseline Design	39850	38400	34650	-
Design 2	Dense PG on M7/8	42650	41000	39850	1.15x
Design 3	Dense twisted PG on M7/8	94970	53170	52500	1.51x
Design 4	Wide VSS shield on M7/8	92030	89010	84750	2.45x
Design 5	Extra DeCap cells	51250	50000	45300	1.31x
Design 6	Extra DeCap + Thin VSS shield on M7/8	47400	50100	44200	1.28x
Design 7	Extra DeCap + Wide VSS shield on M7/8	120000<	78850	76650	2.21x
Design 8	Extra DeCap + Wide VSS shield on M7/8 (no Via7)	101950	98850	92350	2.67x
Design 9	Isolated S-box placement	120000<	99800	93850	2.71x

Fig. 6. (a) Byte-wise breakdown of total cost for baseline AES core (b) MTD cost of recovering key for each orientation along with final MTD cost of attack versus peak-to-peak EM signal measured at chip center (c) Improvement of fine-grained EM SCA resilience for each of the proposed physical design strategies