EMI Shielding for Use in Side-Channel Security: Analysis, Simulation and Measurements

DANIEL DOBKIN**, Bar-Ilan University, Faculty of Engineering, Israel
EDUT KATZ*, Bar-Ilan University, Faculty of Engineering, Israel
DAVID POPOVTZER*, Bar-Ilan University, Faculty of Engineering, Israel
ITAMAR LEVI*, Bar-Ilan University, Faculty of Engineering, Israel

Considering side-channel analysis (SCA) security for cryptographic devices, the mitigation of electromagnetic leakage and electromagnetic interference (EMI) between modules poses significant challenges. This paper presents a comprehensive review and deep analysis of the utilization of EMI shielding materials, devised for reliability purposes and standards such as EMI/EMC, as a countermeasure to enhance EM-SCA security. We survey the current landscape of EMI-shields materials, including conductive polymers, metal-foams, carbon-based materials, and meta-materials, evaluating their effectiveness in attenuating emissions and preventing information-leakage, a task done with security-centric metrics for such materials for the first time. Through a systematic examination of existing literature, experimental studies and a construction of fully-simulatable EM environment in ANSYS-solver, we identify key factors influencing the performance of EMI-shield materials, such as shielding-effectiveness (SE), bandwidth, thickness, and material properties, on security characteristics. We devise a connection between SE and cryptographic-SNR, and we demonstrate from real hardware measurements how and in what conditions can such materials provide very high security levels. By synthesizing insights from multidisciplinary research domains, this paper aims to provide valuable two-way benefit and guidance for researchers, engineers, and practitioners in the design and deployment of robust side-channel security measures leveraging EMI-shields, already in utilization devised by reliability standards.

CCS Concepts: • **Security and privacy** → **Hardware security implementation**; **Cryptanalysis and other attacks**; Embedded systems security; **Side-channel analysis and countermeasures**; **Cryptography**; • **Hardware** → *Hardware test*; *System on a chip*; **Hardware reliability**; Signal integrity and noise analysis.

ACM Reference Format:
Daniel Dobkin, Edut Katz, David Popovtzer, and Itamar Levi. 2024. EMI Shielding for Use in Side-Channel Security: Analysis, Simulation and Measurements. *Proc. ACM Meas. Anal. Comput. Syst.* 37, 4, Article 111 (August 2024), 21 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Electromagnetic Interference (EMI) poses a significant challenge to the reliable operation of electronic systems. These unwanted electromagnetic signals can disrupt the normal operation of devices, leading to performance degradation, data corruption, or system failures. EMI can originate from diverse sources, including power

*All authors contributed equally to this research.

Authors' Contact Information: Daniel Dobkin, Bar-Ilan University, Faculty of Engineering, Ramat-Gan, Israel, daniel.dobkin@live.biu.ac.il; Edut Katz, Bar-Ilan University, Faculty of Engineering, Ramat-Gan, Israel, edut.katz@live.biu.ac.il; David Popovtzer, Bar-Ilan University, Faculty of Engineering, Ramat-Gan, Israel, david.popovtzer@live.biu.ac.il; Itamar Levi, Bar-Ilan University, Faculty of Engineering, Ramat-Gan, Israel, itamar.levi@biu.ac.il.

ACM 2476-1249/2024/8-ART111
https://doi.org/XXXXXXX.XXXXXXX

lines, electronic devices and even natural occurrences like lightning. To mitigate the impact of EMI and ensure the electromagnetic compatibility (EMC) of electronic devices, various standards and recommendations have been established. Organizations such as the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronics Engineers (IEEE) have developed standards [1–3] (e.g., Federal Communications Commission (FCC) Part 16 Class A, European standard CISPR 22, MIL-STD-46) providing guidelines on EMI/EMC testing, limits, and methods for various electronic equipment. Compliance with these standards is crucial for manufacturers to demonstrate the reliability of their products in the presence of electromagnetic disturbances.

Noise reduction and effective shielding are integral components of strategies aimed at enhancing the EMC of electronic systems. Noise, in the context of electronics, refers to unwanted signals or disturbances that can degrade the performance of circuits and devices. Implementing proper grounding, filtering, and shielding techniques helps mitigate the impact of noise, contributing to the overall reliability of electronic systems. Researchers and engineers continually contribute to the field, and relevant papers often provide insights into advanced techniques and methodologies for noise reduction and shielding in electronic systems.

In the pursuit of reliability, the establishment and adherence to industry standards and recommended practices become paramount. These standards not only set the benchmarks for electromagnetic compatibility but also provide a common framework for manufacturers and designers across different sectors. The existence of such metrics underscores *the universal applicability of these principles to all electronic systems, fostering a collaborative approach to ensuring the reliability and resilience of technology in the face of EM challenges.*

Cybersecurity faces an evolving landscape of threats, and among the sophisticated techniques employed by malicious actors, Side Channel Analysis (SCA) attacks pose a risk of particular interest to the field of EMI. One facet of SCA involves close proximity measurements and sensing, where attackers leverage the subtle electromagnetic emanations caused by the power consumption patterns of electronic devices and logical components to glean sensitive information. This method, known as electromagnetic side-channel analysis, has been a concern for over two decades [22, 30]. Since, many different studies have been published in the field [32] revealing how power-/EM- variations could be used to extract cryptographic keys from complex systems [26], with low cost [13] and from a long distance [15]. Fast-forwarding to the present, the threat landscape has only intensified [16, 36], with researchers continually discovering novel ways to exploit electromagnetic side channels for unauthorized access to sensitive information.

One noteworthy recent development in side-channel attacks involves the concept of "screaming channels" [9, 14] and recently other radio-frequency (RF) based long-distance direct read-out attacks [14]. These studies explores how electromagnetic information can be leaked from one element in a System-on-Chip (SoC) to the RF antenna, leading to amplification and transmission of this information with high power over long distances. This amplification of (sometimes) electromagnetic signals poses a significant threat as it enables attackers to eavesdrop on sensitive data from a considerable distance. Understanding and addressing these advanced side-channel attack vectors is crucial for cybersecurity. *It is therefore not only interesting to protect crypto. assets for near-field leakage of direct sensing but also to protect interactions between such assets and (e.g.,) RF-modules.* Consequently, it is imperative to fortify cryptographic implementations against such electromagnetic intrusions which we believe will give rise to a burgeoning field—*Electromagnetic Interference (EMI) Shielding materials for EM Side-Channel security.*

Notably, several relevant academic papers discuss EMI shielding materials specifically in the context of SCA. Even from 2008 "shielding"-boxes and enclosures from few (not standardized) materials were experimented [29]. Other works looked on the problem form the security application perspective, for example in [28, 34, 35] the authors mainly evaluated the ability of an active shield to detect penetration or probing attacks. In [20, 28] the authors have discussed the possible utilization of shielding against EM SCA. On a more general context and for far larger distributed systems and not lumped IC-chips, a wide investigation for EM prevention exists, e.g., [17].

In this work and for the first time we provide a through analysis of different materials already available and industrialized for reliability purposes while also considering their security benefits, mathematical connection to crypto. metrics, simulative framework and comparison to measurement campaigns.

Contribution: In this paper we make several observations relating to the entangled world between EMC and EM-SCA security, and we provide experimental evidence of how one more mature and standardized field can be used to increase security with a rather low electronic cost and simplicity as compared to complex logical SCA-countermeasures which require design modifications and are costly in performance and energy [10, 23, 31]. First, generally our observations are: (1) EMI shielding is a mature field, packed with standards, proposed materials and industry evidence. (2) SCA security mechanisms are typically expensive and require dedicated solutions in HW/SW / redesign cycles, and in some cases logical /mathematical modifications. We propose to synergetically use EMI shielding material to increase HW-security in a low-cost manner, i.e., these materials are already provided and embedded in various electronic-devices. As we list below in our contribution we have made a significant effort in listing a variety of such materials, surveying their physical operation mechanisms and effectiveness for *reliability*. From that point we continued to evaluate their potential use for SCA *security* with a costume constructed electronic evaluation and measurement setup. In addition we have modeled these materials within an high accuracy EM-solver simulator to verify and compare our experimental evidence with simulation, including providing mathematical connections between reliability metrics (such as communication SE or SNR) with crypto.-sense SNR. Briefly, our conclusions show that conductive fiber shields perform best, indicate a strong connection between high shielding effectiveness and lower adversarial success rate, and exponentially compounding shielding effectiveness with layering shields, and flexible customization of material depth.

2 BACKGROUND

In this section we shortly recall propagation of EM waves, attenuation of such waves, and mechanisms which are used to amplify such attenuation. Namely, absorption and reflection.

2.1 Electro-magnetic Waves

Electromagnetic interference can be described simply by propagation in standard Cartesian coordinates, providing understanding of the spatial distribution of electromagnetic fields. As interference emanates from its source, its propagation can be visualized as a dynamic interplay of electric and magnetic components along three orthogonal axes. The x-axis represents the direction of travel, while the y and z axes denote the transverse planes through which the electromagnetic wave oscillates. The interference patterns, dictated by the frequency and wavelength of the waves, manifest in the form of spatial variations in electric and magnetic field strengths.

The Electro-magnetic wave's properties can be fully described by Maxwell's equations, which are written as follows in the differential form :

$$\begin{aligned} \boldsymbol{\nabla} \times \mathbf{e}_{(\mathrm{t})} &= -\frac{\partial}{\partial \mathrm{t}} \mathbf{b}_{(\mathrm{t})}, \qquad \boldsymbol{\nabla} \cdot \mathbf{b}_{(\mathrm{t})} = 0 \\ \boldsymbol{\nabla} \times \mathbf{h}_{(\mathrm{t})} &= \mathbf{j}_{(\mathrm{t})} + \frac{\partial}{\partial \mathrm{t}} \mathbf{d}_{(\mathrm{t})}, \quad \boldsymbol{\nabla} \cdot \mathbf{d}_{(\mathrm{t})} = \rho_{\mathrm{e}\,(\mathrm{t})}, \end{aligned} \tag{1}$$

where, $\boldsymbol{\nabla}$, $\mathbf{e}_{(\mathrm{t})}$, $\mathbf{b}_{(\mathrm{t})}$, $\mathbf{h}_{(\mathrm{t})}$, $\mathbf{j}_{(\mathrm{t})}$, $\mathbf{d}_{(\mathrm{t})}$, and $\rho_{\mathrm{e}\,(\mathrm{t})}$ denotes the gradient, the electric field , magnetic flux density, magnetic field, electric current density and electric displacement, respectively.

2.1.1 Uniform plane wave. In our analysis we will deal with uniform plane waves[1][2] expressed by

$$\mathbf{E}_{(\mathrm{x,y,z})} = \mathrm{E}_0 \exp^{-j\mathbf{k}\cdot\mathbf{r}} \;\; ; \;\; \mathbf{H}_{(\mathrm{x,y,z})} = \mathrm{H}_0 \exp^{-j\mathbf{k}\cdot\mathbf{r}} \tag{2}$$

[1]Presents the simplest solution of harmonic Maxwell's equations
[2]The exact field produced by a source can be expressed by a linear combination of plane wave superposition

Where E_0 and H_0 are constant complex vectors defining the polarization (either linear, circular or elliptical), and the wavevector $\mathbf{k}$ expressed as $\mathbf{k} = k\mathbf{u}_r$. For a uniform plane wave $\mathbf{u}_r$ is a real unit vector defined as

$$\mu_\mathrm{r} = \cos\phi \sin\theta \mathbf{u}_\mathrm{x} + \sin\phi \sin\theta \mathbf{u}_\mathrm{y} + \cos\theta \mathbf{u}_\mathrm{z} \tag{3}$$

and k is the medium's wavenumber defined by it's permittivity ϵ_r, permeability μ_r and the frequency of the plane wave ω;

$$\mathrm{k} = \omega\sqrt{\mu_\mathrm{r}\epsilon_\mathrm{r}} \tag{4}$$

2.2 Attenuation by a Single Planar Shield

The most basic shielding configuration is illustrated in Fig. 1, where a uniform plane wave interacts with a shield. The shield has infinite extension in the transverse y and z directions (dimensions large enough to disregard edge effects) and a finite thickness d in the x direction, while the incident angle θ of the plane wave is considered

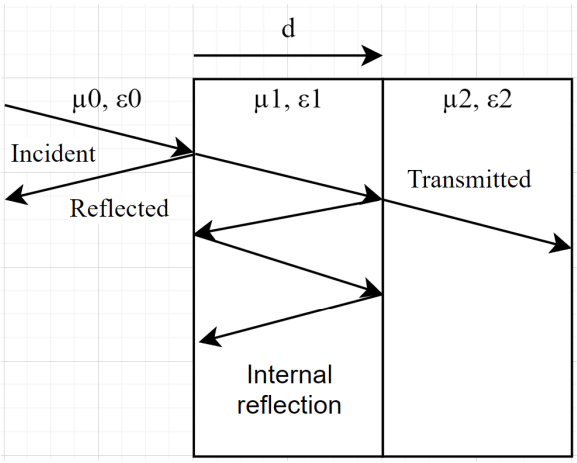

Fig. 1. Attenuation of an electromagnetic wave by a shield.

Defining the characteristic impedance of the transverse electric wave as

$$Z_\mathrm{i}^{\mathrm{TE}} = \omega\frac{\mu_\mathrm{i}}{k_\mathrm{xi}} \tag{5}$$

We arrive at the following [11] shielding effectiveness (SE)

$$\begin{aligned}\mathrm{SE} = -20\log\frac{4\mathrm{Z_0Z_s}}{(\mathrm{Z_0}+\mathrm{Z_s})^2}^{\mathrm{R}} \cdot \exp\{-\mathrm{j}k_\mathrm{xs}\mathrm{d}\}^{A} \\ \cdot\frac{(\mathrm{Z_0}+\mathrm{Z_s})^2}{(\mathrm{Z_0}+\mathrm{Z_s})^2-(\mathrm{Z_0}-\mathrm{Z_s})^2\exp\{-\mathrm{j}k_\mathrm{xs}\mathrm{d}\}}^{\mathrm{MR}}\end{aligned} \tag{6}$$

Z_0 and Z_S are the characteristic impedance's of free space and shield material, respectively.

2.3 Absorption & Reflection

In the context of electromagnetic wave interactions with materials, reflection and absorption are the main phenomena discussed in our study. Reflection, denoted by R in Eq. 6, represents the portion of incident energy that bounces off a surface resulting from impedance mismatch. On the other hand, absorption, denoted A in Eq. 6, accounts for the energy absorbed by the material. For the attenuation of a plane wave by a medium, with a thickness of d, this term is always positive, and it exponentially increases with ω (Eq. 4), as high frequencies are easy to absorb and scatter due to their short wavelength.

Additionally, when a wave penetrates a material with a layered structures (i.e., a laminated package with EMI shielding), it may undergo multiple reflections within the medium, denoted by MR. Such multiple internal reflections are often negligible when dealing with high frequencies [11]. In Section 6, under some noise assumptions, we make a mathematical connection between the communication sense signal to noise ratio (SNR), SE and the cryptographic-sense SNR (defined below). The goal is to be able to design materials, estimate and verify their security-level; e.g., estimating security metrics from well characterized and provided in data-sheets SE (and when these assumptions hold).

3 MATERIALS & COMPARISON

In the present era, the synthesis of new materials is a blooming field of research and industrial progress, continuously expanding the array of materials accessible for constructing shielding structures in large volumes and availability for products and the costumer. This section is aimed to introduce and generally review the various materials which may hold significance in relation to SCA ,which we will experiment with in the following.

3.1 Standardised and Industrialized Materials for EMI protection

3.1.1 Conductive polymers. Conductive polymers exhibit considerable potential in shielding electromagnetic radiation (EM) due to their notable conductivity and dielectric permittivity values, along with the convenient manipulation of these properties through chemical processes [21]. Thin samples of conductive polymers demonstrate high shielding efficiencies that are minimally affected by temperature variations (i.e., the heat form a processor or the cooling from ventilation). The ability to easily fine-tune intrinsic characteristics through chemical processing positions these polymers as promising candidates for shielding applications. The conductivity is contingent on both the doping level and the polymer's geometry.

3.1.2 Conductive Fabrics. Fabrics have very desirable mechanical qualities for EMI shielding, namely their flexibility, small thickness and lightweight. There is a wide range of techniques to incorporate various metals, usually ones with high conductivity, such as copper, silver and nickel into polyester and carbon nanotubes [18] resulting in highly advanced composite materials. Their thinness means such fabrics rely mostly on mechanisms of shielding by reflection, as they lack absorption depth. The main characteristic of these fabrics is their conductivity [11], which is also their downside as conductivity is affected by temperature [11]. Another interesting aspect from the application point of view is that due to their conductivity and typically mesh structure of ultra thin wires, they can be used to sense shorts, disconnections and adversarial activity with very high resolution, considering tampering adversaries which aims to bypass the mechanism generally utilizing the shield against FIB and probing attacks [20, 28, 34, 35].

3.1.3 Conductive Papers. Papers possessing conductive characteristics are produced through the integration of metal coated polyester fibers. The metal coatings vary, but are usually either copper or nickel. The frequency response of the shield can by tuned by varying the amount of metal in the fabric. Shielding designed for the Very High Frequency (VHF) [8] band (30-300 *MHz*) should contain metal amounts of up to $15\frac{g}{m^2}$ [33]. Similarly to

conductive fabrics, their similar qualities of high conductivity and mesh like structure allows sensing faults and adversarial activities [20, 28, 34, 35].

3.2 Comparison

Table 1. Conductive fiber and conductive paper based shielding available from Shieldex.

Material	Thread density (lowest)	Metal Plating	Surface Res. [Ω]	Thickness [mm]	Shielding Eff. @ 0.2 *MHz* [dB]
Berlin RS	450-490	silver	0.3	0.1	62
Kiel +30	spunbonded	Copper	0.02	0.25	107
Nora Dell CR	450-490	pure silver 99.9 + copper + nickel	0.0009	0.125	87
Balingen	Charmeuse	pure silver 99.9	0.6	0.26	57
Nantes	Mesh	Silver + Copper + nickel	0.03	0.11	92

Table 2. Properties of conductive silicone polymer available from Hexcel. ϵ' and ϵ'' denote the real and imaginary part of a complex permittivity respectively. In similar fashion, μ' and μ'' denote the real and imaginary part of a complex permeability respectively

Material	Surface Resistivity[Ω]	Thickness [mm]	ϵ'/ϵ''	μ' / μ''	Reflection Loss @ 1 *GHz* [dB]
DD-11393	$11 \cdot 10^9$	0.508	17/0	14/2	1
DD-13490	$11 \cdot 10^9$	1.5	17/0	14/2	1

We aim to survey the main different types of shields available on the market [5, 6] and their effectiveness in hampering EM SCA attacks. We perform both simulations and measurements on these materials on concrete hardware and measurement infrastructure to compare the results and open the discussion towards their low-cost embedding in systems *for security purposes, serving double-justification.*

3.3 Materials Evaluated

Table 1 lists a variety of materials that were chosen to test a variety of metal coatings (silver, copper, nickel and their combinations), shielding types (conductive fabrics and conductive papers) and SE (depending on large number of specified and unspecified parameters). We only evaluate commercial materials from clear reasons. Generally, these shields have low surface resistance and high SE (values higher then 50) at our testing frequency. Table 2 shows the tested polymer based shields, due to their *very high resistivity* such materials are ill-suited for the VHF band in which we performed tests, and have very low shielding effectiveness. As such these shields are tested and discussed, but do not represent the main body of our work. These materials are discussed as a comparison to other shields, and due to their relevance in L and S frequency band (1-4 *GHz*) [8], as modern CPU's and servers operate and emit data in these frequencies [4], *considering that modern data centers have some form of EMI shielding for EMC reasons, it eases one's mind to see the effectiveness of such shields in the hardware security sense.* Since the two different tables list materials intended for different use-cases and frequency bands, the SE specified is limited, as such we listed the value for lowest measured frequency, and we use this value to along with simulation results to approximate SE at our devices frequency. The materials that were chosen for the simulation environment offer some form of interest whether it is more extensive data sheets (DD-1393) and to

compare the performance of different metals that are embedded in the measured conductive fabrics. Comparing the simulation and measurement results should give us insights into the relations between the overall SE and linear SCA estimators, to open and expand the discussion for further integration of the established knowledge from EMI research into the field of EM SCA. Materials Based on carbon Foam [19, 25, 37] were also considered for comparison, owing to their popularity / availability in the industry. However, they were not included in the comparison owing to their non conductive nature, where for a relatively low frequency band this property is dominant.

4 CHOSEN TESTS AND ESTIMATORS

A variety of side-channel analysis (SCA) attacks and leakage-detection metrics are typically utilized to bound and determine the amount of data leaked from cryptographic devices. We use several notable tools used in the community in literature for known comparison points and more standardized metrics (such as TVLA) which are advised by standards (e.g., Common-Criteria). Then our goal is to compare these security results with relation to both theoretical and practical SE of a material, used to explain their EMI attenuation abilities in the context of reliability. Our devised set of estimators were chosen to model a limited/reasonable-complexity adversary, in a real world scenario where one might have access to some Internet of Things (IoT) device/mobile device and basic knowledge in the field of SCA crypto-analysis.

4.1 Signal to Noise Ratio

We evaluate Mangard's Signal to Noise Ratio (SNR) [27] defined by:

$$\mathrm{SNR(t)} = \frac{\mathrm{Var}_{x_i,k}(\mathrm{E}[l^t_{x_i,k}])}{\mathrm{E}_{x_i,k}(\mathrm{Var}_i[l^t_{x_i,k}])} \tag{7}$$

where Var represents the variance estimator and E denotes the expected value, and $l^t_{x_i,k}$ corresponds to the leakage (measurement) trace l at time point samples t, derived from a cryptographic operation that utilizes key k and processes a plaintext byte x_i classifying generally some internal computed value y-value. While the point-of-interest (POI) in time (t) where the computation of y is identified from the leakage is typically searched by:

$$\max \mathrm{SNR} = \mathrm{SNR}_{\mathrm{t=POI}} = \max_{\mathrm{t}}(|\mathrm{SNR}|) \tag{8}$$

The SNR metric is important owing to its'; **(1)** Low complexity of computation, **(2)** Dependence on the first two statistical moments **(3)** Mostly relevance for Gaussian distribution leakages such as field emissions, and **(4)** Large body of knowledge and reports, providing easy comparison. As discussed above, in Section 6 we make a mathematical connection between the cryptographic SNR to SE and measured voltage in a real device, under some assumptions about noise. Where, our goal is to be able to reason and give easy rule-of-thumb connections, and therefore the ability to design and select materials, estimate and verify their security-level.

4.2 Correlation Power Analysis

Correlation Power Analysis (CPA) [7] defined by

$$\rho_{\mathrm{l^t_{x_i,k}},\mathrm{h^t_{x_i,k^*}}}(\mathrm{t}) = \frac{\mathrm{Cov}(l^t_{x_i,k^*}, h^t_{x_i,k^*})}{\sigma_{l^t_{x_i,k}}\sigma_{h^t_{x_i,k^*}}} \tag{9}$$

The measured leakage l and randomly varying (key dependent) hypothesis from some internal computation h, Cov and σ are the covariance between both random variables and their standard deviations respectively. All possible (sub-) keys hypothesis k^* are enumerated, to generate the leakage hypothesis h stemming from some

internal y-value. Then the k^* which maximizes the correlation of these values to the leakage is estimated to be the correct key. Similarity to SNR, the point-of-interest (POI) in time (t) where the computation of y is defined:

$$\rho_{\text{t=POI}} = \max_{\text{t}}(|\rho|^2) \tag{10}$$

CPA is used to check the linear correlation between the leakage, and the key hypothesis, we use it to see the relation between the reduced leakage in **E** field affected by the shield. It is a well known and investigated attack apparatus which underlines some assumptions about the leakage model by which hypothesis are built. The level of CPA resistance is an easy to capture and compare stand-point for our evaluated materials.

4.3 Test Vector Leakage Assessment

Test Vector Leakage assessment (TVLA) methodology [12], based on the two-sided Welch's T-test is performed. It is a fast univariate method where in our fixed-versus-random experiments, the test populations are leakages from two sets S_f & S_r, where constant plaintext and a randomized plaintext were asserted, accordingly. This test allows us to quantify the availability of meaningful secret information which leaks from the device to an adversary in a general case (not associated with specific internal value). TVLA reflects a well known and standardized metric; as described by Eq. 11 where μ is the mean value and # denotes the size of the set. Below, we evaluate examples with T-values computed directly over the leakages (i.e., the raw first statistical moment), and we also show results of the test computed over the 2^{nd} central-moment, $CM_s^{2,t} = E((l_s^t - \mu)^2)$, for completeness[3].

$$\text{T} - \text{val.} = \frac{\mu_{S_f} - \mu_{S_v}}{\sqrt{\frac{\sigma_{S_f}}{\#S_f} + \frac{\sigma_{S_v}}{\#S_v}}} \tag{11}$$

5 RESULTS

Within our methodology we have tailored (1) a unique simulative framework in a full EM solver simulator which is first discussed. Then (2) a complete measurement campaign on concrete devices with all evaluated materials is performed and reviewed below.

5.1 Full EM-solver simulation results

The simulations were performed using an imported Process Design Kit (PDK) for TSMC's 65nm process-design-kit (PDK) layout within the Ansys HFSS simulator. Ansys HFSS is equipped to model electromagnetic (EM) radiation behavior in the context of integrated circuit (IC) technology, accounting for fabrication constraints. The simulation configuration, as depicted in Fig. 2, involves a 0.2mm metal wire placed at layer M3, serving as the EM radiation source. Positioned 0.01mm above the source, the shielding layer has a width and depth of 0.5mm, with varying heights based on the shielding material simulated. This shielding layer is electrically connected to the ground layer, located beneath the substrate. The distance between the shielding layer and the ground plane is approximately 700μm (which is reasonable for IC chips).

To assess the EM radiation attenuation capabilities of each shield, we introduced an additional layer into the layout's layer stack. This new layer was designed with parameters closely resembling those of the actual shields analyzed in Section III. For each shield type, we created a material-based shield, incorporating the key material associated with that shield. Specifically, our study considered three primary types: the Silicon-based shield (DD-11393), the Copper-based shield (Kiel +30), and the Silver-based shield (Nora Dell CR), considering Tab. 1 and Tab. 2. Our setup mimics the representative chosen materials in their monolithic form, and it approximates

[3]although there is no Masking involved in our evaluation which moves leakage to the second moment, it normally also contains information leakage

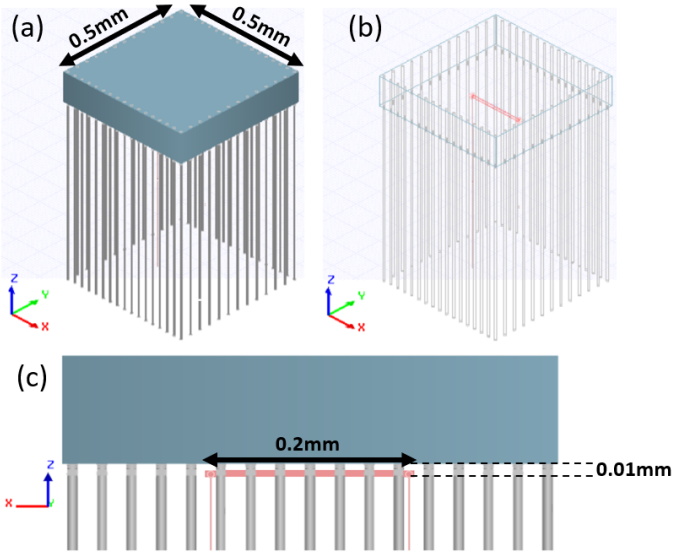

Fig. 2. (a) Top down view of the simulation.(b) Top down view of the simulation, showing the leakage source. (c) Horizontal view of the simulation layout.

Manufacturer	ARC Technologies		Shieldex	
Material	DD-11393	DD-13490	Kiel +30	Nora Dell RS
Shield configuration for simulation	Silicone-based shield	Silicone-based shield	Copper-based shield	Silver-based shield
Height	0.55mm	1mm	0.25mm	0.12mm
μ	14	14	0.99991	0.99997
ε	17	17	1	1

Table 3. Ansys HFSS simulation setup to test different material based shields. (a) The shielding layer is a 0.5mm X 0.5mm square. (b) Transparent view of the EM source (in red) and the surrounding shield. (c) Side view on the EM source - a 0.2mm wire at layer M3, and the shielding layer located 0.01mm above the source.

the behaviour of non monolithic (e.g., Fibers) materials, a point which can be improved in future work. Emulated parameters are listed in Tab. 3.

5.1.1 Shielding effectiveness. The SE was computed based on the maximum E field results obtained from simulations at a distance of $1mm$ above the radiation source. Fig. 3 illustrates the SE of various shielding materials across different source frequencies (most interesting for our purpose is the range $48MHz$-$1GHz$). As anticipated, shields composed of metal exhibit higher SE, indicating their superior ability to attenuate emitted EM radiation. In contrast, silicon-based shields demonstrate consistent SE values across varying thicknesses, suggesting that thickness has minimal impact on their effectiveness. Furthermore, for lower frequency the metal based shields has better SE, and silicon based shields higher frequencies yield better SE. I.e., one class behaves more like a low-pass and another more like a high-pass filter in our region of interest. This observation also guided us in selecting materials for further time consuming measurement campaigns as demonstrated below.

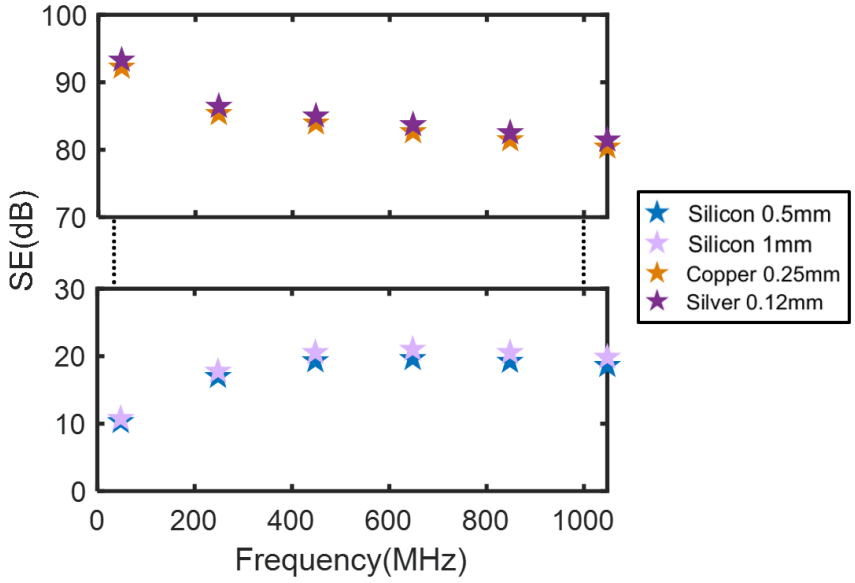

Fig. 3. SE of shields based on different materials for the frequency range of 48MHz-1GHz.

Fig. 4 illustrates the SE of silver and copper-based shields when layered. I.e., effectively increasing the material depth d, which will reflect a very strong knob in later experiment section to significantly increase security level. Both metals, Fig. 4(a) and Fig. 4(b), exhibit quite similar SE values for single-layer and double-layer shielding. However, the triple-layer shielding exhibits significantly higher SE values, with an approximate 10dB increase compared to the SE values of the single and double layers. Notably, this observation emphasizes the influence of shielding thickness on metal-based shields: increased thickness of metal layers results in improved SE values and enhanced attenuation of EM radiation exponentially as can be understood from Eq. 6, with an exponential dependence.

5.1.2 Cryptographic Metrics. To assess information leakage using various material-based shields, we connect simulation results with two of the most common cryptographic metrics: SNR, and Test Vectors Leakage Assessment (TVLA). It is important to note that the abilities of cryptographic distinguishers to extract information depend on various factors, not only field magnitudes, therefore are also required for the effectiveness of the shield assessment in reducing leakage of information.

To calculate the SNR and T-test for SE evaluation we generated pseudo leakage traces combined with the EM simulation results in the IC environment. Randomized noise was added to those leakage traces using the following formula, $n = Rand \cdot \sigma_{signal} \cdot \sigma_{noise}$. Where σ_{signal} was calculated from the EM simulation results, σ_{noise} has values between $10 - 1000$, and $Rand$ is a normally distributed random number between -1 and 1 which was determined for each signal point. The number of measurements (or traces) practiced and captured by the simulation is $10 \cdot 10^6$.

Fig. 5 shows the SNR values for different frequencies. The SNR of the silicon based shields demonstrate similar values for different frequencies. For the metal based shields the SNR significantly increase with higher frequencies for lower σ_{noise}. The silicon based shields have SNR of around 10^{-3} only for high noise $\sigma_{noise} = 1000^2\sigma^2_{signal}$.

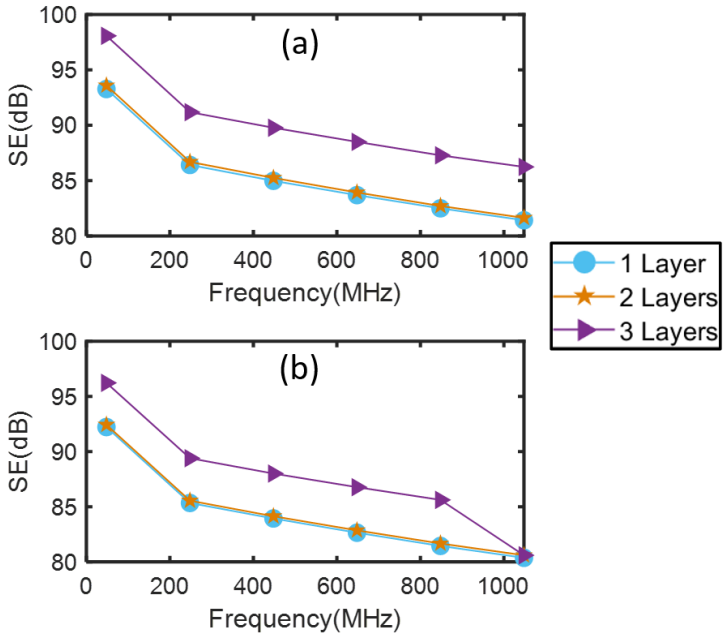

Fig. 4. SE of layered shields. (a) Silver based shield, each layer has a thickness of 0.12mm. (b) Copper based shield, each layer has a thickness of 0.25mm.

For the metal based shields the SNR is below 10^{-3} for $\sigma_{noise} = 1000^2\sigma^2_{signal}$ and for lower frequencies for $\sigma_{noise} = 100^2\sigma^2_{signal}$.

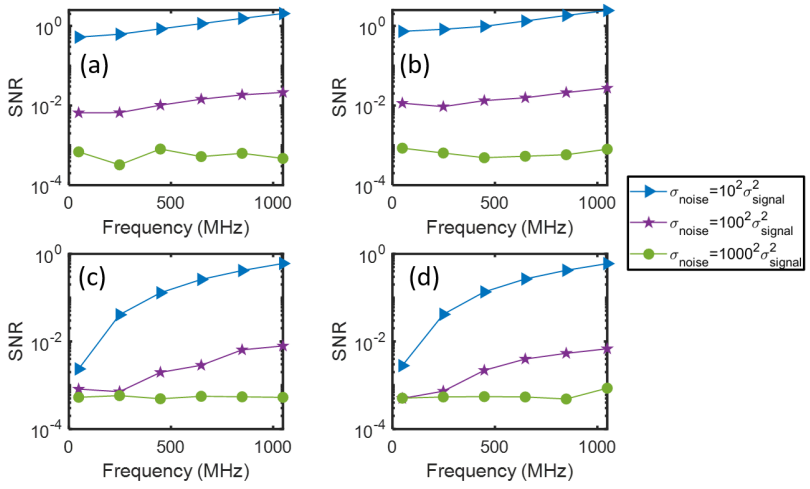

Fig. 5. Calculated SNR constructed from the max E field resulting from the Ansys HFSS simulations. (a) Silicon based shielding 0.5mm. (b) Silicon based shielding 1mm. (c) Copper based shielding 0.25mm. (d) Silver based shielding 0.12mm.

The other cryptographic metric, which is commonly used in such evaluations, is the T-test. The TVLA results in Fig. 6, show T-values below the threshold for all the shielding materials for noises level of $\sigma_{noise} = 1000^2\sigma^2_{signal}$, $\sigma_{noise} = 100^2\sigma^2_{signal}$. The metal based shields demonstrate also T-values below the threshold for noise level of $\sigma_{noise} = 10^2\sigma^2_{signal}$, for lower frequencies.

The SNR and TVLA results show the shielding ability to decrease the leakage of information. As expected the metal based shields better decrease the leakage of information which corresponds the SE results.

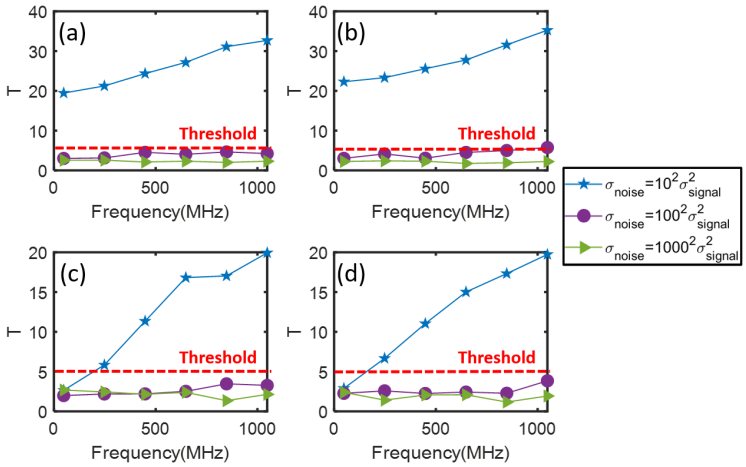

Fig. 6. Calculated T-values constructed from the max E field resulting from the Ansys HFSS simulations. (a) Silicon based shielding 0.5mm. (b) Silicon based shielding 1mm. (c) Copper based shielding 0.25mm. (d) Silver based shielding 0.12mm.

The goal of the next section is to show correspondence of the simulation results to actual measurements (and on what conditions), to exercise more in depth the analysis and draw concrete connection between cryptographic metrics and SE, and devise concrete intuition relating to promising solutions in this context.

5.2 Measurement results

Traces were captured with Riscure's EM probe station and amplifier, recorded with a picoscope 5404d series as described in Fig. 7. The tested encryption scheme is a non-secure 128bit AES implemented in Verilog implemented on a Sakura-G board with a Xilinx Spartan-6 target chip operating with an $f_{clock} = 48MHz$. We assign plaintexts and keys as needed per simulation view: I.e., Conventional randomized TVLA test vectors are different than those of a CPA attack and an SNR evaluation.

As a baseline example, in Fig. 8(a), 8(b) one can capture the mean leakage trace, the repeating pattern of encryption rounds are visible from the leakage shape. The variance is observed as well showing data dependency vulnerability and high-quality of the setup and meaningful signal in the leakage. Indicating the vulnerability of our setup to such side channels, therefore deeming for SCA protection, even from contactless EM attacks. To set a baseline measurement of such un-protected design, Fig. 8(c) and 8(d), demonstrate the calculated SNR and ρ, with a clearly visible peak at the first encryption cycle, where the POI is denoted on the graphs associated with the point in time secret hypothesized or classified calculations take place. The POI is defined in Eq. 8 and Eq. 10 respectively.

Measured in a grid above the Spartan-6 evaluated chip, we divided the measured (x,y) surface into a 30X30 mesh, with each cell (referred to as pixel henceforth) the size of $0.66^2[mm]$. An approximate 3D normal distribution

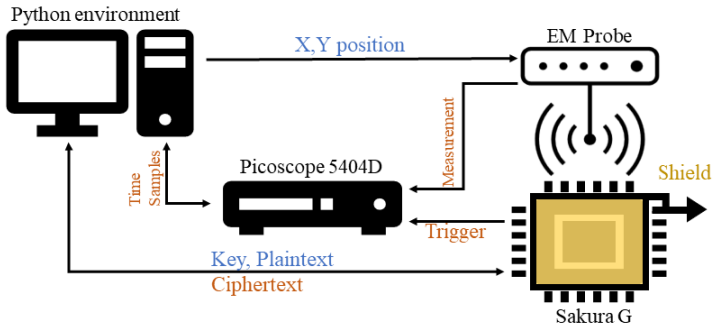

Fig. 7. Connection scheme of the measurement setup

of SNR is captured in Fig. 9(c) for unprotected design. This is owed to the fact that other logical operations and noise mask information further away from the central (x,y) leakage coordinate and the signal weakens. Fig. 9(a), 9(d) and 9(d), illustrate the results for Balingen grounded, Kiel +30 Grounded , and $0.5mm$ conductive Silicone materials, respectively. The concrete values of the peak SNR of these materials after the shield clearly significantly vary (two magnitudes or order) for these configurations and materials. Note that for all metrics computed and all materials the optimum-(x,y) coordinate is searched and used. Only light variations exist in these locations for different materials. This happens from several reasons: the FPGA setup is fixed relatively to the EM probe (relative) location, the placed logic on the FPGA was also fixed, and changing materials only refract slightly the position as materials are generally flat.

Fig. 10 shows the convergence-views versus the number of used traces in our campaign of the correlation and SNR. It can be concluded from the figure that conductive materials are in a class of their own when it comes to SE in such low frequencies for both estimators. This is apparent not only in a significantly lower number of traces needed to converge (by at least 1 order of magnitude), but also the actual converged magnitude (Value). The plots also list all material results when the materials are grounded. Counter intuitively, grounding the material doesn't necessarily provide a substantial increase in neither parameter. The main factor for this is the non-perfect conductivity. The only material that shows a substantial increase in Fig. 10 is Nora Dell CR, as its surface resistance is lower by 2 orders of magnitude when compared to other materials with similar SE at $0.2GHz$ 1 giving this material superior characteristics and significant immunity. Grounding a shield with high conductivity such as Nora Dell CR has the added benefit of increasing σ_{noise}, observed from big jumps and variations in convergence value in Fig. 10 (a).

TVLA evaluation: Fig. 11 shows the TVLA results over time, i.e., T-value versus time of a non-shielded board, because fixed versus random TVLA doesn't use classification or key hypothesis, the peaks coincide with the encryption rounds seen in Fig. 8(a) and 8(b) rather then the meaningful POI's observed in the first round in Fig. 8(c) and 8(d). The graphs hence-forth shows the first two statistical moments of the leakage as described above in the maximum T-value over time, where clearly both in this unprotected scenario leaks considerably.

Having established that conductive fabrics and papers are best suited for the frequency band leaking from our implementation and device, we aimed to compare the performance of such shields in a broader term. Fig. 12 shows us the TVLA convergence of these shields. It is immediately apparent that the second order T value loses its statistical significance with even 1 layer of shielding, where only Shieldex Nantes converges to a significant value

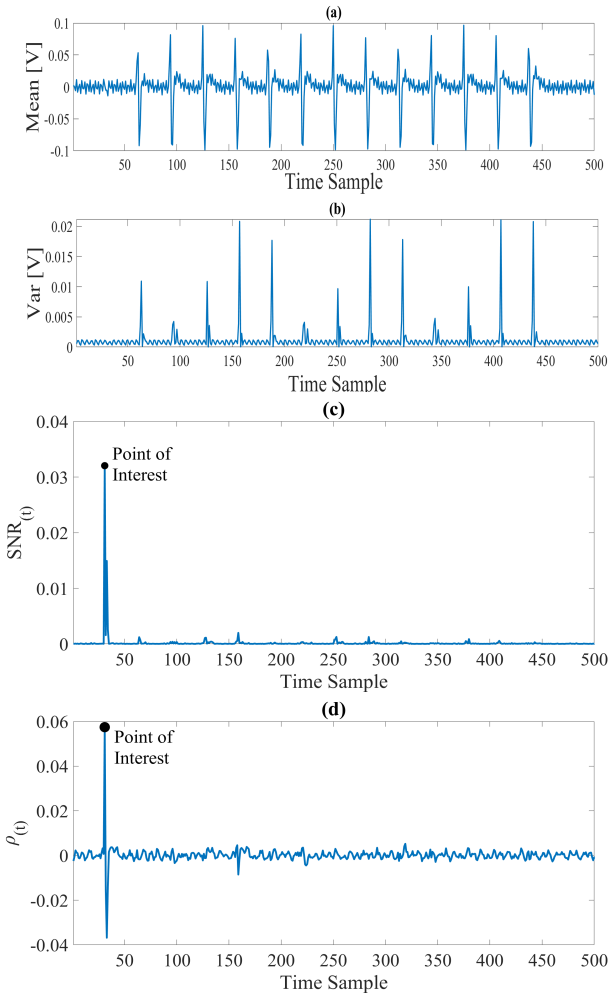

Fig. 8. Example unprotected leakages: (a) Mean of 10k sampled traces (b) Variance of 10k Sampled traces. Measured on a non shielded FPGA using an EM probe (c) SNR as a function of time, with POI marked at the first round calculated for $1{\cdot}10^6$ Sampled traces (d) ρ over time, with corresponding POI in the first round ($1{\cdot}10^6$ traces)

after more then 90% of sampled traces. So considering for example a masked implementation [10, 23, 31] with masking order d=2 most materials can provide already significant EM protection, as anyway the first statistical moment would not leak. **This is an important motivation as Masking security is exponential with d demanding d-1 achieving similar security can be very significant [23, 31]**. Furthermore, observing T-values results of the first statistical moments, they gradually vary from (Kiel+30) to (Nora Dell CR), and one can observe security increase. However, this will not always be enough as the number of traces needed to significantly (non specific) extract information increases by 10x-100x, but does still not reach significant $10{\cdot}10^6$ or $100{\cdot}10^6$ traces typically considered as a strong(er) adversary. We therefore, move to the next observation relating to thicker sheets and layering, achieving higher security levels.

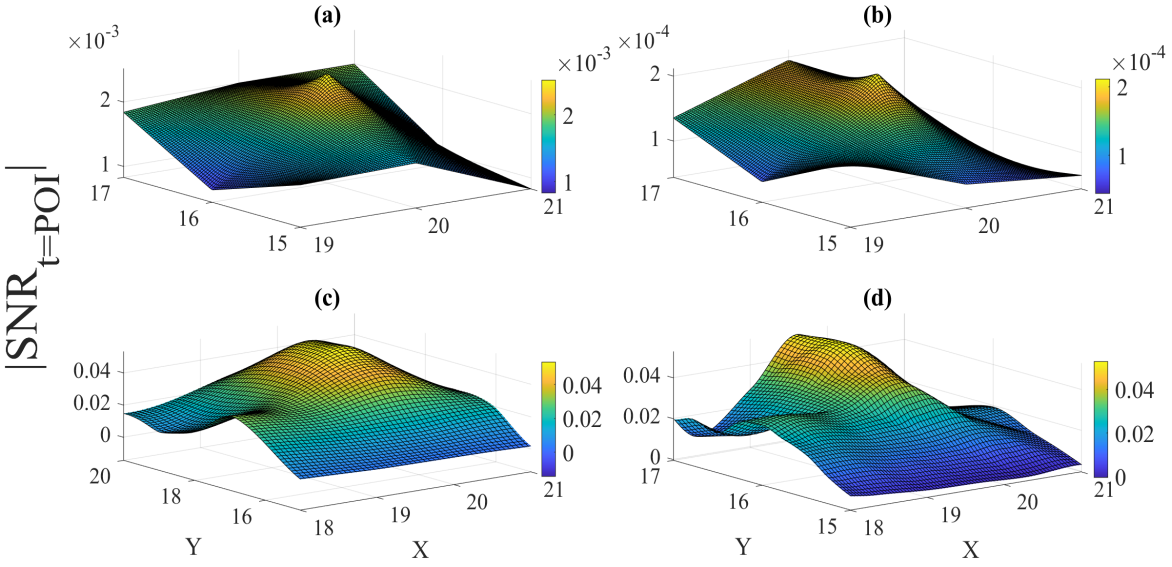

Fig. 9. Surface plots for SNR measured above the spartan 6 target, calculated for 500k sampled traces. (a) Balingen grounded (b) Kiel +30 Grounded (c) No shield (d) 0.5mm conductive Silicone

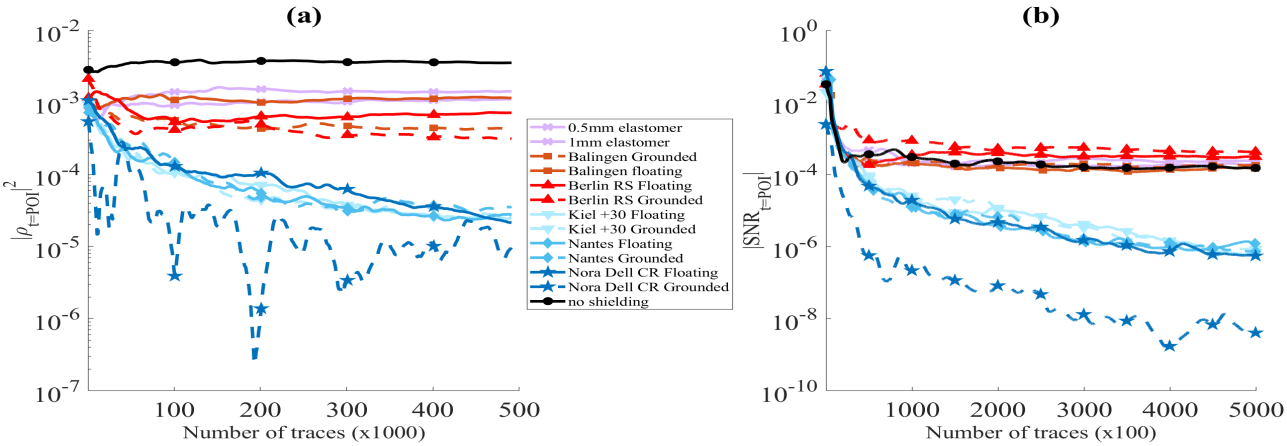

Fig. 10. Convergence plots @POI and optimum (x,y): (a) ρ value over number of traces. (b) SNR value over number of traces.

5.3 Exp. Amplification by Effective d and Concrete Security

Improving upon the results from the previous section, we layered the shields to rely upon the absorption mechanism, the absorption loss term defined by

$$Absorption\ Loss = \exp\{-jk_{xs}d\} \tag{12}$$

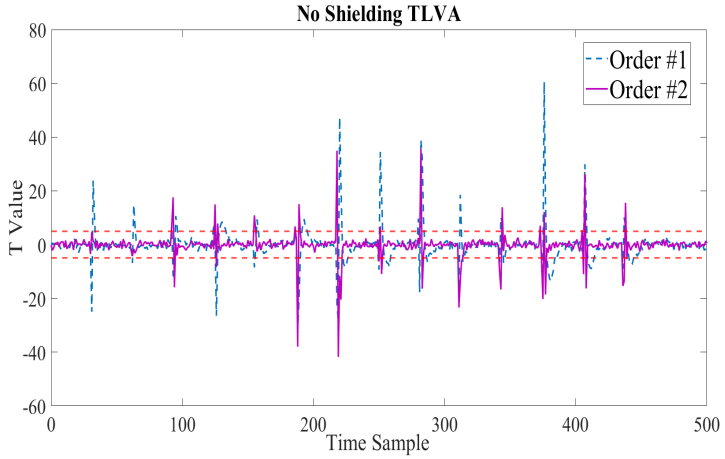

Fig. 11. TVLA over time of the first two statistical leakage moments, no shielding. Calculated over 1M samples

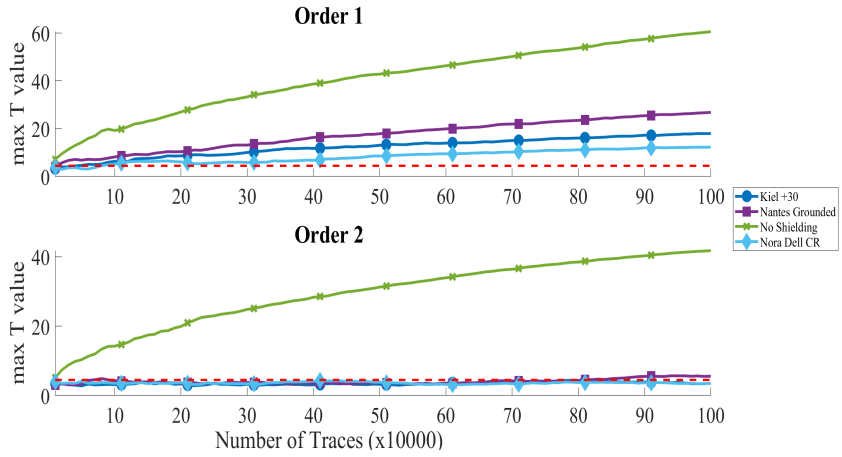

Fig. 12. Convergence of T-value, for a single layer of different materials.

Fig. 13 shows the drastic increase in the amount of traces required to reach a significant value in the 1-st order TVLA with layering of one to three layer, for all materials. The figure shows the first two statistical moments T-values (one on the top figures-row and two in the bottom figures-row), from left to right we evaluate Kiel+30, Nora Dell CR and Nantes materials, and from purple curves (no shield) through blue, yellow, and red curves we increase the number of layers. Again Nora Dell CR stands out because of the low surface resistance (Tab. 1). This is already quite exquisite as clearly increase in required number of traces is exponential indeed from experimentation.

Simulation versus Measurements experimentation: comparing the results from Sections 5.1 and 5.2, we can safely say that there is direct causation between SE values and SCA security metrics, and we give concrete transfer- relation from experiments for the first time. In the next section we dive into this point a bit in more details. Incorporating EMI shields into IC package designs and PCB cases is of great value in EM SCA security,

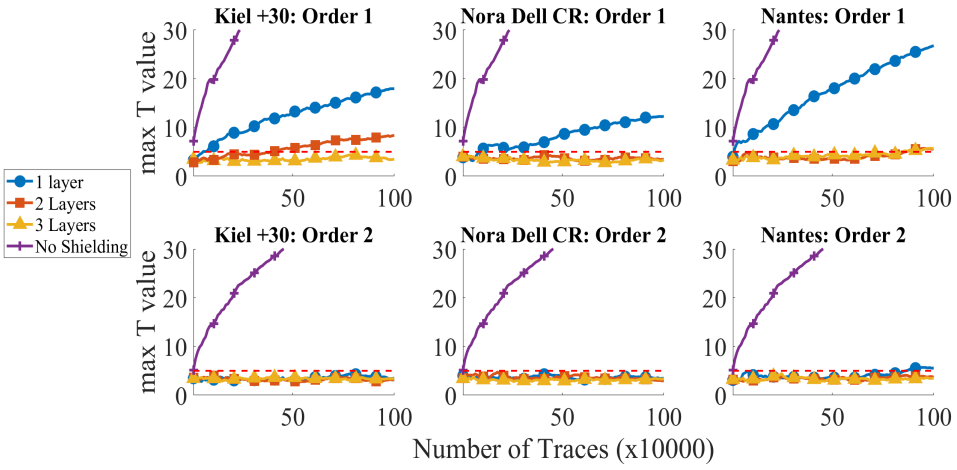

Fig. 13. Convergence of T-value, for a single layer of different materials.

good designs may include tamper sensing capabilities in low cost enclosures relying on the conductive nature of some shields. An important point of discussion to expand upon is the great performance of conductive shields (both fabrics and papers) in our measurements, as seen in Fig. 3 these shields should perform better in our system because of the clock frequency so this comes as no surprise. Designers and engineers should consider operating clock speeds when choosing a suitable shield for SCA security appropriate material justified in accordance with our simulative (deduced and explainable) and experimented framework for their given application space.

6 EASY RULE-OF-THUMB CONNECTION BETWEEN RELIABILITY SE AND (E.G.,) SNR SECURITY EVALUATION:

In this section we aim to give a general rule of thumb and to formulate the connection between SE, to the measured voltage in the electrical probe and finally tie them to observed SNR values. It is important to note that the formulas developed in this sections are approximate (due to very lenient assumptions), but show quite useful and true to experimental evidence and rationalization. An electrical field interacting with a shield can be described by, $\mathbf{E}_{\text{Transmit}} = \mathbf{E}_{\text{Incident}} \cdot 10^{-\frac{\text{SE}}{20}}$. Substituting into the relation between voltage end electric field allows us to take out the term dependent on the SE, which we will define $\alpha = 10^{-\frac{SE}{20}}$:

$$V = \int \mathbf{E}_{Transmit} \cdot d\mathbf{z} = \alpha \cdot \int \mathbf{E}_{Incident} \cdot d\mathbf{z} \tag{13}$$

assuming the measurement probe is in the z direction, without the loss of generality. As the leakage in Eq. 7 is measured in volts, amperes or field strength but not in dB, it is also multiplied by this α term. Assuming for simplicity that the main elements of noise behaves linearly and are additive, defining two types of independent noise sources, N_{int} is the computation systems inherent noise, resulting from but not limited to: power management, switching noise, internal reflections, non-negligible current leakages, thermal noise, etc. and N_{ext} resulting from similar effects in the environment and measuring equipment. From here it is easy to accept that the internal noise is also affected by α, while the external noise isn't. Using these definitions and assumptions we can rewrite Eq. 7 in the following form:

$$\mathrm{SNR_{Sh}(t)} = \frac{\mathrm{Var}_{x_i,k}(\mathrm{E}[\alpha(l^t_{x_i,k} + N_{int}) + N_{ext}])}{\mathrm{E}_{x_i,k}(\mathrm{Var}_i[\alpha(l^t_{x_i,k} + N_{int}) + N_{ext}])} \tag{14}$$

For comfort we define $* = \alpha(l^t_{x_i,k} + N_{int})$ and we split into cases

$$\sigma^2_* << \sigma^2_{\mathrm{N_{ext}}}, \quad \mathrm{SNR_{Sh}} \approx \alpha^2 \cdot \mathrm{SNR_{NoSh}} \tag{15}$$

$$\sigma^2_* >> \sigma^2_{\mathrm{N_{ext}}}, \quad \mathrm{SNR_{Sh}} = \frac{\mathrm{Var}_{x_i,k}(\mathrm{E}[*])}{\mathrm{E}_{x_i,k}(\mathrm{Var}_i[*])} \tag{16}$$

In our case, higher SE leads to lower levels of leakage and internal noises measured by the sensor, which

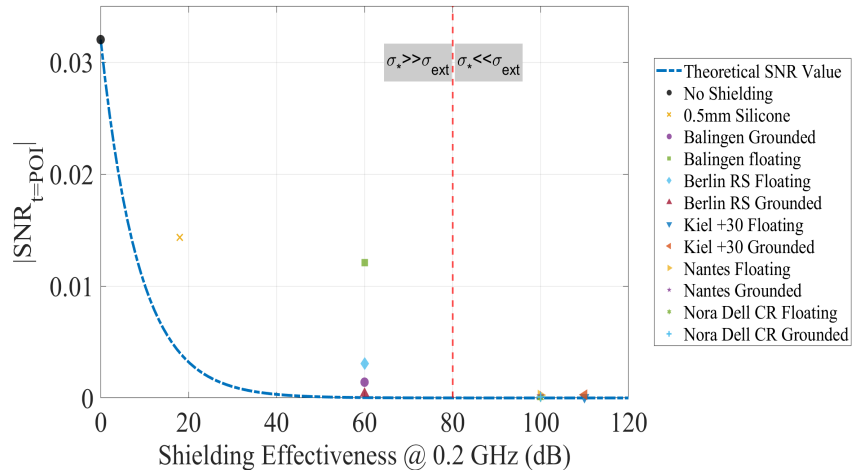

Fig. 14. Comparison of Eqn. 16 to actual measured values. The SE of 0.5mm silicone @ 0.2 GHz is estimated using the ANSYS simulation similar to Fig. 3

in term leads to the dominance of external noise sources in the sampled trace. This significantly hurts the 'rogue' undesirable communication channel between the probe and the target IC, and reduces the success rate of both passive and active Side-Channel Analysis attacks. Our attack scenario can be modeled after near field communication between the Riscure EM probe and Spartan 6 target, it is not a massive leap to accept that SNR in the communication sense should be affected similarly with some form of the de-numerator α. As demonstrated in Fig. 14 which shows the measured asymptotic SNR values of various materials (in red) and the calculated SNR trend versus SE from the approximation above (dashed blue curve), starting from the SE=0 point which is the unprotected design measurable value (in black point). Clearly, for high SE levels for various materials we get very good correspondence of this model, whereas for low SE values, which is anyway not the interesting operating-point for such security applications, some error is observed.

7 REAL WORLD USE CASES AND LIMITATIONS

Real world EMC design take into consideration a variety of factors, ranging from operating temperature to mechanical properties and space limitations. **Architectural considerations:** it has to be mentioned that in some cases (i.e., RF embedded SoCs') the use of a shield should be designed correctly, in the layout and architecture

of a device, in addition to other non radiating sources such as galvanic connection which need protection [14]. Various solutions and ready to use methodologies exist for such scenarios for example by selective covering, vertical coatings etc. **Far-lower price tag:** As a general discussion, various EM-SCA countermeasures in all abstraction layers exist. Increasing hardware security comes at high cost, whether it be performance, power, silicon area, design and verification time etc. Cost can be sub-linear, linear [23, 24] or exponential [10, 31] with the desired security-level, but always non-negligible, if high assurance and minimal security assumptions are taken. Clearly, with the proposed Shielding mechanisms various assumptions are taken which can be dealt with on the application level, but undoubtedly EM security price tag is far lower with negligible cost, and materials which are already standardized and present in devices already. **Application perspective:** The shields covered in this study can be used in various design processes, from integrating in packages to full size Printed Circuit Board (PCB) and chip enclosures, or data center protection. Of high concern are various IoT devices available on the market for purchase, allowing both well-minded hobbyists and nefarious parties with sufficient knowledge to perform extensive tests. **Tamper evidence:** Combining a shield with tamper protection on sensitive parts of a product is the ideal use case for the knowledge offered by this study. Though in [20, 28, 34, 35] authors mainly evaluated the ability of an active shield to detect penetration or probing attacks, indeed understanding and providing insights on connecting sensors on wire/mesh shields is an important future direction for such materials.

8 CONCLUSIONS AND FUTURE RESEARCH

To conclude our paper, the rich literature from the field of EMI shielding has a lot to contribute to the field of EM SCA, both in terms of standardized knowledge and in terms of available shields offered by different manufacturers. Using and embedding shields in their various forms helps achieve better security performance in all forms of computational devices ranging from small IoT devices to PC and data centers. We perform concrete analysis on various materials with various security oriented tools, a task not practiced so far though such materials are standardized and approved for EMI protection. We demonstrate and support by theory and in a full EM-solver simulation environment including actual measurements that significant security levels are possible to achieve with such a technique, with negligible cost. Future research of interest includes: **(1)** Performing measurements on faster devices in the *GHz* range, testing polymers and carbon foams in similar fashion. **(2)** Expanding upon the possibility of using fibers as Frequency Selective surfaces [11] to demodulate antennas for defence against RF attacks [9] and direct read-outs [14]. **(3)** Stress testing conductive shields under varying temperature conditions validating viability in different real world scenarios.

ACKNOWLEDGMENTS

Itamar Levi was partially Funded by the Pazy Foundation Research Grant ID377 and Israel Science Foundation (ISF) grant 2569/21. Daniel Dobkin and Itamar Levi received partial funding for parts of this project from the Israel Innovation Authority (IIA), Bio-Chip Consortium Grant file No. 75696, Israel.

REFERENCES

[1] Ec 61000. https://webstore.iec.ch/publication/24517.
[2] Ieee 1848-2020. https://standards.ieee.org/ieee/1848/7221/.
[3] Ieee 2665-2022. https://standards.ieee.org/ieee/2665/7185/.
[4] Intel processor families – quick reference guide. https://www.intel.com/pressroom/kits/quickreffam.htm. Accessed: 14/04/2024.
[5] Rf interference control. https://www.hexcel.com/Products/Interference-Control/RFInterferenceControl, 2024. Accessed: 2024-04-08.
[6] Shieldex. https://www.shieldex.de/en/, 2024. Accessed: 2024-04-08.
[7] Brier, E., Clavier, C., and Olivier, F. Correlation power analysis with a leakage model. In *Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings 6* (2004), Springer, pp. 16–29.

[8] Bruder, J., Carlo, J., Gurney, J., and Gorman, J. Ieee standard for letter designations for radar-frequency bands. *IEEE Aerospace & Electronic Systems Society* (2003), 1–3.

[9] Camurati, G., Poeplau, S., Muench, M., Hayes, T., and Francillon, A. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (2018), pp. 163–177.

[10] Cassiers, G., Grégoire, B., Levi, I., and Standaert, F.-X. Hardware private circuits: From trivial composition to full verification. *IEEE Transactions on Computers 70*, 10 (2020), 1677–1690.

[11] Celozzi, S., Araneo, R., Burghignoli, P., and Lovat, G. *Electromagnetic Shielding: Theory and Applications*. John Wiley & Sons, 2023.

[12] Cooper, J., Mulder, E. D., Goodwill, G., Jaffe, J., Kenworthy, G., and Rohatgi, P. Test vector leakage assessment (TVLA) methodology in practice (extended abstract). ICMC 2013.

[13] Danial, J., Das, D., Ghosh, S., Raychowdhury, A., and Sen, S. Scniffer: Low-cost, automated, efficient electromagnetic side-channel sniffing. *IEEE Access 8* (2020), 173414–173427.

[14] Danieli, E., Goldzweig, M., Avital, M., and Levi, I. Revealing the secrets of radio embedded systems: Extraction of raw information via rf. *IEEE Transactions on Information Forensics and Security 19* (2024), 2066–2081.

[15] Elibol, F., Sarac, U., and Erer, I. Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In *2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO)* (2012), IEEE, pp. 1767–1771.

[16] Guri, M. Air-gap electromagnetic covert channel. *IEEE Transactions on Dependable and Secure Computing* (2023).

[17] Guri, M., Zadov, B., and Elovici, Y. Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields. *IEEE Transactions on Information Forensics and Security 15* (2019), 1190–1203.

[18] Jagatheesan, K., Ramasamy, A., Das, A., Basu, A., et al. Electromagnetic shielding behaviour of conductive filler composites and conductive fabrics–a review. *Indian Journal of Fibre & Textile Research (IJFTR) 39*, 3 (2014), 329–342.

[19] Jia, X., Shen, B., Zhang, L., and Zheng, W. Construction of shape-memory carbon foam composites for adjustable emi shielding under self-fixable mechanical deformation. *Chemical Engineering Journal 405* (2021), 126927.

[20] Katz, E., Avital, M., and Levi, I. Refined analytical em model of ic-internal shielding for hardware-security and intra-device simulative framework. *IEEE Access* (2024).

[21] Kim, B., Koncar, V., Devaux, E., Dufour, C., and Viallier, P. Electrical and morphological properties of pp and pet conductive polymer fibers. *Synthetic Metals 146*, 2 (2004), 167–174.

[22] Kocher, P., Jaffe, J., and Jun, B. Differential power analysis. In *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19* (1999), Springer, pp. 388–397.

[23] Levi, I., Bellizia, D., Bol, D., and Standaert, F.-X. Ask less, get more: Side-channel signal hiding, revisited. *IEEE Transactions on Circuits and Systems I: Regular Papers 67*, 12 (2020), 4904–4917.

[24] Levi, I., Bellizia, D., and Standaert, F.-X. Beyond algorithmic noise or how to shuffle parallel implementations? *International Journal of Circuit Theory and Applications 48*, 5 (2020), 674–695.

[25] Li, Y., Shen, B., Pei, X., Zhang, Y., Yi, D., Zhai, W., Zhang, L., Wei, X., and Zheng, W. Ultrathin carbon foams for effective electromagnetic interference shielding. *Carbon 100* (2016), 375–385.

[26] Longo, J., De Mulder, E., Page, D., and Tunstall, M. Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip. In *Cryptographic Hardware and Embedded Systems–CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings 17* (2015), Springer, pp. 620–640.

[27] Mangard, S. Hardware countermeasures against dpa–a statistical analysis of their effectiveness. In *Topics in Cryptology–CT-RSA 2004: The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings* (2004), Springer, pp. 222–235.

[28] Miki, T., Nagata, M., Sonoda, H., Miura, N., Okidono, T., Araga, Y., Watanabe, N., Shimamoto, H., and Kikuchi, K. A si-backside protection circuits against physical security attacks on flip-chip devices. In *2019 IEEE Asian Solid-State Circuits Conference (A-SSCC)* (2019), IEEE, pp. 25–28.

[29] Plos, T., Hutter, M., and Herbst, C. Enhancing side-channel analysis with low-cost shielding techniques. In *Proceedings of Austrochip* (2008), pp. 90–95.

[30] Quisquater, J.-J., and Samyde, D. Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In *Smart Card Programming and Security: International Conference on Research in Smart Cards, E-smart 2001 Cannes, France, September 19–21, 2001 Proceedings* (2001), Springer, pp. 200–210.

[31] Salomon, D., and Levi, I. Masksimd-lib: on the performance gap of a generic c optimized assembly and wide vector extensions for masked software with an ascon-p test case. *Journal of Cryptographic Engineering 13*, 3 (2023), 325–342.

[32] Sayakkara, A., Le-Khac, N.-A., and Scanlon, M. A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digital Investigation 29* (2019), 43–54.

[33] Shinagawa, S., Kumagai, Y., Umehara, H., and Jenvanitpanjakul, P. Conductive papers for electromagnetic shielding. In *Proceedings of the international conference on electromagnetic interference and compatibility* (1999), IEEE, pp. 372–375.

[34] Wang, H., Shi, Q., Nahiyan, A., Forte, D., and Tehranipoor, M. M. A physical design flow against front-side probing attacks by internal shielding. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 39*, 10 (2019), 2152–2165.

[35] Wang, K., Gu, Y., Zhou, T., and Chen, H. Multi-pair active shielding for security ic protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 38*, 12 (2018), 2321–2329.

[36] Zhang, J., Liang, B., Zhang, H., Zhang, W., Ling, Z., and Yang, M. Mobile applications identification using autoencoder based electromagnetic side channel analysis. *Journal of Information Security and Applications 75* (2023), 103481.

[37] Zhang, L., Liu, M., Roy, S., Chu, E. K., See, K. Y., and Hu, X. Phthalonitrile-based carbon foam with high specific mechanical strength and superior electromagnetic interference shielding performance. *ACS Applied Materials & Interfaces 8*, 11 (2016), 7422–7430.