EM/Power Side-Channel Attack: White-Box Modeling and Signature Attenuation Countermeasures

Debayan Das
School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA

Arijit Raychowdhury
School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA

Santosh Ghosh
Intel Labs, Intel Corporation, Hillsboro, OR 97124 USA

Shreyas Sen
School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA

Editor's notes:
This article presents analysis methods to pin-point the cause of side-channel leakage in integrated circuits and proposes a number of techniques for leakage attenuation.

—Rosario Cammarota, Intel Labs
—Francesco Regazzoni, University of Amsterdam and Università della Svizzera Italiana

The growth of the low-cost resource-constrained Internet-connected (Internet of Things—IoT) devices is of immense interest from a security perspective. As the systems become increasingly complex, more potentially exploitable attack vectors emerge, leading to higher chances of security vulnerabilities. Hence, most of today's embedded devices are equipped with cryptographic algorithms to provide confidentiality and authenticity of data. However, these algorithms are implemented on a physical substrate, which leaks critical correlated information in the form of electromagnetic (EM) radiation, power consumption, timing of the crypto operations, cache hits and misses, and so on, leading to side-channel analysis (SCA) attacks. An attacker can utilize this side-channel leakage information to extract the secret key.

Many real-world exploitations utilizing the power and EM SCA have already been demonstrated. Recently, the smart lighting system Philips Hue was hacked by exploiting the underlying operating system, utilizing what is known as power SCA [1], allowing the attacker to perform over-the-air firmware updates.

As multiple devices remain interconnected within an IoT network, a small vulnerability on one of the edge devices could prove extremely costly to the security of the entire large-scale network. Hence, security considerations, including power and EM side-channel leakage analysis, should form a necessary part of the design life-cycle of all the embedded devices, even if it is not a critical node of the IoT network.

Despite these requirements, even today, many existing embedded devices do not employ SCA protection. This could be because of two main reasons: *the time to market and the cost*. First, the time to market

Digital Object Identifier 10.1109/MDAT.2021.3065189
Date of publication: 15 March 2021; date of current version: 20 May 2021.

is extremely important for industry, and hence SCA attack protection schemes need to be scalable across technologies and should be generic for all algorithms. Moreover, it is desirable to have a countermeasure as a wrapper around the entire crypto core without any changes to the existing algorithms, thereby also ensuring legacy protection. Second, the cost is related to the area, power, and throughput overheads of the countermeasure. Hence, a low-overhead energy-efficient generic synthesizable countermeasure is necessary which can provide protection against both EM as well as power SCA attacks. In this article, we discuss a white-box analysis of the EM leakage to root cause the source of the EM radiation from a crypto IC, leading to the design of a current domain signature attenuation (CDSA) hardware with local lower-level metal routing to protect against both EM as well as power SCA attacks.

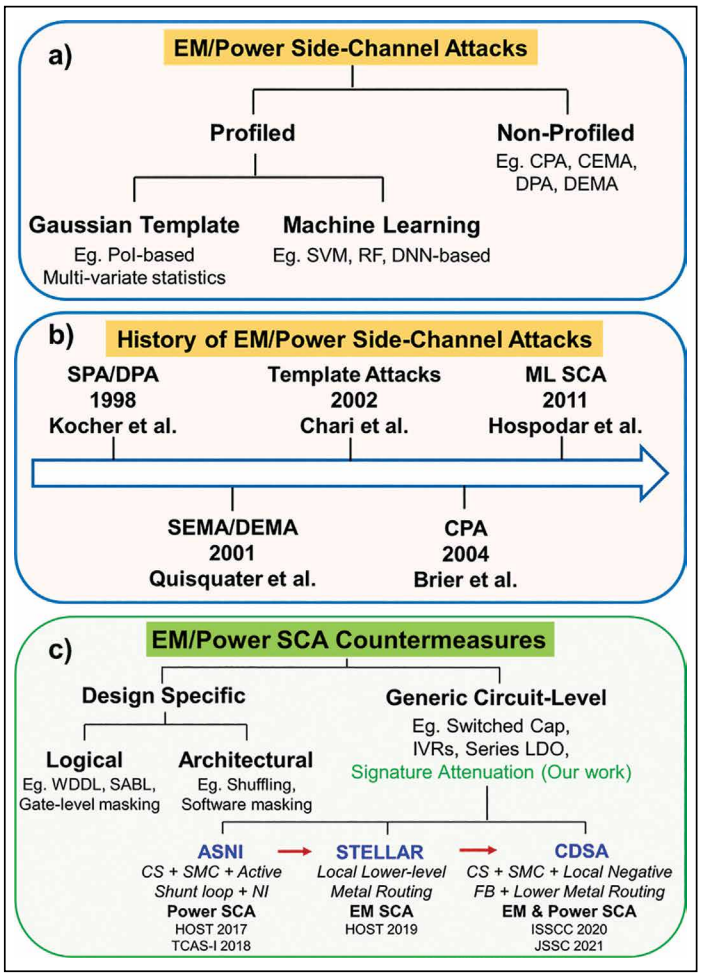

Figure 1. (a) and (b) Types and history of EM/power SCA attacks and (c) types of EM/power SCA countermeasures.

EM and power SCA attacks

Power/EM SCA attacks can be classified as nonprofiled and profiled attacks (Figure 1a).

Nonprofiled SCA attacks

In 1998, Kocher et al. [2] showed the first nonprofiled power SCA attack in the form of simple power analysis (SPA) and differential power analysis (DPA). Several attack vectors have emerged since then, making it an active research domain even today. Nonprofiled side-channel attack is a direct attack on the target device using hamming weight (HW) or hamming distance (HD) leakage model. It includes the conventional correlational/differential power/EM (CPA/CEMA/DPA/DEMA) attacks.

The timeline of the EM/power SCA attacks is shown in Figure 1b. Following the advent of power SCA, the noninvasive EM attack was studied extensively by Quisquater and Samyde [3] in 2001. In 2002, statistical template-based profiling attacks were developed by Chari et al. [4], which will be discussed in the following subsection. In 2004, correlational SCA attack was introduced by Brier et al. [5]. Recently, in 2011, machine learning (ML)-based SCA was introduced by Hospodar et al. [6].

Profiled SCA attacks

The traditional nonprofiled SCA attack requires thousands of traces against an efficient hardware implementation. On the other hand, profiling attacks are performed in two phases—the training phase, which is also known as profiling, and the attack phase. During the training/profiling phase, which happens prior to an attack, an offline template is built using an identical device. The entire heavy-lifting is thus offloaded to the training phase which happens offline prior to the actual attack. During the attack phase, unseen traces are fed to the trained model which then predicts the correct key byte with as low as a single trace. Profiled attacks can be classified into statistical template-based attacks (TAs) and ML or deep-learning-based SCA attacks.

- *Statistical TA:* These statistical TA utilize a multivariate Gaussian distribution of the points of interest (PoIs). PoIs are the maximum leaky time samples determined based on the difference of means, or the sum of squared differences, or the signal-to-noise ratio (SNR) across multiple traces [4].
- *ML attacks:* The ML-based SCA attacks utilize

supervised techniques like the support vector machine (SVM), self-organizing map (SOM), random forest (RF), and deep neural network (DNN). Recently, DNNs have generated huge interest in the SCA community as they can even defeat SCA-protected implementations. Specifically, convolutional neural networks (CNNs) have been shown to defeat clock misalignment-based countermeasures [7]. Also, masking-based countermeasures have been broken using DNNs [8]. Moreover, DNNs are preferred over statistical TA as they can handle large dimensionality of the data and do not require a precise PoI selection. Recently, in DAC 2019, X-DeepSCA demonstrated the first cross-device deep learning (DL)-based side-channel attack on AES128, showing the feasibility of even a single trace attack [8]. X-DeepSCA showed a ten improvement in the minimum traces to disclosure (MTD) even for low SNR scenarios compared to the traditional CPA attack, increasing the threat surface significantly.

State-of-the-art countermeasures

In this section, we will look into the countermeasures against EM/power SCA attacks. These countermeasures can be classified as logical, architectural, and physical techniques (Figure 1c). Most of the logical and architectural countermeasures are design and algorithm-specific, while the circuit-level countermeasures are generic to any crypto algorithm and can often be used as a wrapper around it. All of these countermeasures operate on the fundamental principle of decreasing the SNR, and thus rely on the combination of the two key techniques: 1) noise injection (NI) and 2) critical correlated signature suppression.

Design-specific countermeasures

Logical countermeasures

Logical countermeasures are mainly based on power balancing which includes the wave dynamic differential logic (WDDL) [9], dual-rail precharge (DRP) circuits, sense amplifier-based logic (SABL), and gate-level masking [7]. Dual-rail logic requires a custom design of the logic gates to equalize the power consumption. In DRP cells, one of the outputs always switches its state (either the original output or its compliment), making the power consumption constant. SABL employs a dynamic and differential logic and requires the complete redesign of the standard cell library to ensure that all the four output transitions (0–0, 0–1, 1–0, 1–1) consume the same amount of power. WDDL appears to be the first protection technique validated in silicon and can be built using the single-rail standard library cells, however, it incurs a 3× area overhead, 4× power overhead, and a 4× performance degradation.

Architectural countermeasures

Architectural countermeasures introduce amplitude or time distortions to obfuscate the power/EM trace. Time distortion is achieved by random insertion of dummy operations or by shuffling the operations. However, it does not provide high levels of protection (MTD) as the number of operations that can be shuffled are limited depending on the specific algorithm and its architecture. Also, clock skipping and dynamic voltage and frequency scaling (DVFS)-based countermeasures have been shown to be defeated using advanced attacks than can realign the clock based on the power supply signatures [10]. Algorithmic masking techniques are commonly used [11], but it incurs > 2× area and power overheads.

Overall, the logical and architectural countermeasures explored to date, including the masking and hiding techniques, suffer from high area/power/throughput overheads (as highlighted in Figure 5) and are specific to a crypto algorithm. Next, we will study the generic countermeasures that are applicable to any crypto algorithms.

Generic countermeasures

Physical circuit-based countermeasures

This class of countermeasures involves physical NI and supply isolation circuits. Although NI has been used extensively in many countermeasures, NI alone suffers from large power and area overheads. Supply isolation techniques include switched capacitor current equalizer [12], integrated voltage regulator (IVR) [13], and series low-dropout (LDO) regulators [14]. Switched capacitor current equalizer based countermeasure is a novel technique and achieves high MTD, but it requires an analog reset and also suffers from multiple tradeoffs leading to a 2× performance degradation. IVRs using buck converters and series LDOs have been explored extensively, however, they suffer from large passives—inductors and

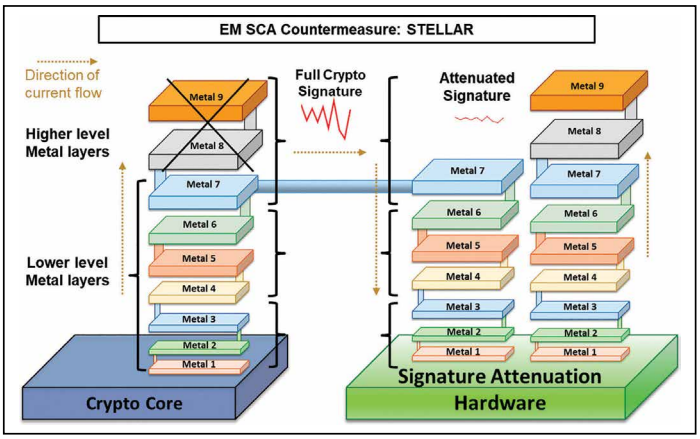

Figure 2. White-box analysis: lower level metal routing of the SAH embedding the crypto core.

on-chip capacitors. As we will discuss later, these on-chip MIM (metal–insulator–metal) capacitors can leak critical side-channel information through the higher-level metal layers in the form of EM leakage [15], [16]. Also, a series LDO-based implementation inherently leaks critical correlated information [17], as it instantaneously tracks the voltage fluctuations across the crypto core and regulates the current accordingly.

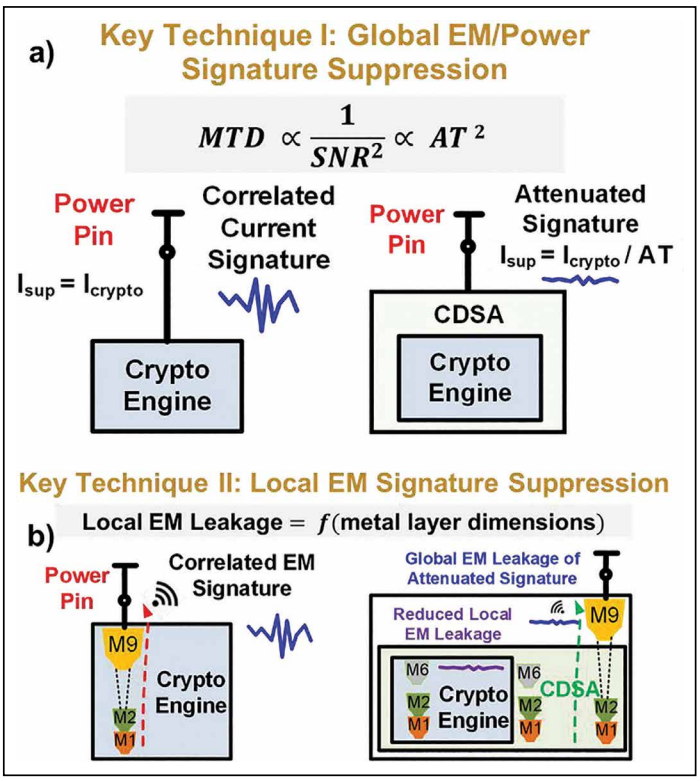

Figure 3. (a) and (b) Overview of CDSA hardware with local low-level metal routing.

Limitations of the existing countermeasures

Most of the countermeasures proposed till now suffer from a high area, performance, and power overheads (> 2×). Although the circuit-level techniques discussed above are generic, they treat the crypto engine as a black box and hence incur high overheads. Our goal is to develop a white-box understanding of the EM leakage (Figure 2, details in the "Root-cause analysis of the EM leakage" section) from a crypto IC leading toward a low-overhead generic countermeasure. Additionally, we also want to design a synthesis-friendly countermeasure so that it can be integrated seamlessly into different technology nodes without much design effort.

Toward the above-mentioned goals, we proposed the concept of signature attenuation to prevent both power as well as EM SCA attacks [16]–[18]. In the sections that follow, we will present the CDSA hardware along with low-level metal routing (inspired from the white-box analysis) to provide a low-overhead generic countermeasure, validated in 65-nm CMOS technology against a parallel AES256 implementation [15]. Figure 3 shows the key techniques behind the proposed CDSA design. As seen from Figure 3a, the MTD is proportional to the square of the attenuation factor (AT) providing resilience against both power as well as global EM SCA. Hence, our goal is to provide a very high signature attenuation with extremely low overheads. Figure 3b shows the key technique of local low-level metal routing to suppress the EM signature at its origin within the lower metal layers.

Rootcause analysis of the EM leakage

In this section, we will study the white-box analysis of the EM leakage to develop a better understanding of the rootcause of the EM leakage. Most of the existing EM SCA attacks as well as countermeasures treat the crypto engine as a black box. However, to design a low-overhead countermeasure, we need to analyze and understand the rootcause of this EM leakage.

White-box analysis and STELLAR technique

All crypto engines like AES256/SHA256/ECC consist of multiple digital gates. These transistors switch their state creating changing currents leading to the EM radiation according to the Maxwell's equations. However, the main question then arises—what does

this observable EM field depend on? Is it caused by the transistors itself?

Well, the observable EM fields depend on the metal layers carrying the current, and not just the transistors. The transformation of the switching currents through the metal-interconnect stack creates the EM radiation which is then picked up by an external adversary, leading to EM SCA attacks. Higher-metal layers are thicker (Figure 2, metal-interconnect stack) and hence act as more efficient antennas at the operating frequency of the crypto cores, compared to the lower metal layers. Hence, the EM leakage from the top metal layers (M_9 and above for the Intel 32-nm process [16]) has a higher probability of detection using the commercially available EM probes. This is proven using 3D finite element method (FEM) system-level simulations of the Intel 32-nm metal stack [16]. Hence, our goal is not to pass the correlated crypto current through the high-level metal layers. But, it needs to connect to the external power pin. So, we somehow need to restrict the correlated power signatures to the lower-level metal layers, such that the EM leakage is suppressed locally.

This quest led to the development of Signature aTtenuation Embedded CRYPTO with Low-Level metAl Routing (STELLAR) [16]. STELLAR proposes routing the crypto core within the lower-level metal layers and then embed it within a signature attenuation hardware (SAH) locally within the lower metal layers, such that the critical signature is significantly suppressed before it reaches the top-level metal layers which radiate significantly. This concept of signature suppression within the lower-level metal layers is shown in Figure 2. The current from the crypto core (denoted by the blue line) goes through the SAH, which embeds the crypto core locally within the lower metals and is then passed through the higher metal layers (denoted by the green line) to connect to the external power pin.

Long-term impact

Our work on STELLAR led to the first white-box analysis and developed a better understanding of the rootcause of the EM leakage. Now, combined with a SAH with lower-level metal routing, we can develop a highly resilient countermeasure against both EM as well as power SCA attacks. The local routing is extremely critical to minimize the long routing of the critical signals.

Looking into the future, we plan to develop a further understanding of the genesis of the EM leakage so that we can kill it even closer to its source [19]. Next, we will analyze the design of our SAH and combine it with our STELLAR technique to prevent both EM and power SCA attacks.

Signature suppression

Now, let us look into the details of the SAH.

Evolution of the SAH

The progression of the SAH is shown in Figure 1c. In 2017, we proposed the first concept of SAH design in the form of attenuated signature noise injection (ASNI) [17], [20] to prevent power SCA attacks, generic for all cryptographic algorithms, without any performance degradation. In ASNI, the key idea was to embed the crypto engine within a SAH such that the correlated critical crypto signature is highly suppressed at the power supply node which an attacker can access, and then inject a tiny amount of noise to protect against power SCA attacks. Next, STELLAR demonstrated the efficacy of local lower-level metal routing to prevent EM SCA attacks, as discussed in the "Root-cause analysis of the EM leakage" section. Finally, we combine the concepts of signature attenuation from ASNI and the local lower metal routing from STELLAR leading to the CDSA hardware, which was demonstrated in a 65-nm test-chip at the ISSCC 2020 [15]. Note that, NI was not included in the CDSA circuit to demonstrate the efficacy of signature attenuation alone. Recently, in ISSCC 2021, we presented a synthesis-friendly version of CDSA which is generic and also scalable across different process/technology nodes, while maintaining the benefits of the analog-like countermeasure [21].

Attenuated signature noise injection

Let us now understand the design details of the ASNI circuit. ASNI combines a SAH along with a NI circuit (NI is not discussed here). The goal of developing a SAH is to have a constant supply current independent of the variations in the crypto current. The first thing that we can think of is a constant current source (CS). However, a constant CS cannot drive a variable current load (crypto engine). Hence, a load capacitor (C_{Load}) is required to account for the differences in the current, as shown in Figure 4a. Now, as shown in Figure 4b, a high bandwidth (BW) shunt LDO is used which bypasses any excess current through the bleed NMOS whenever

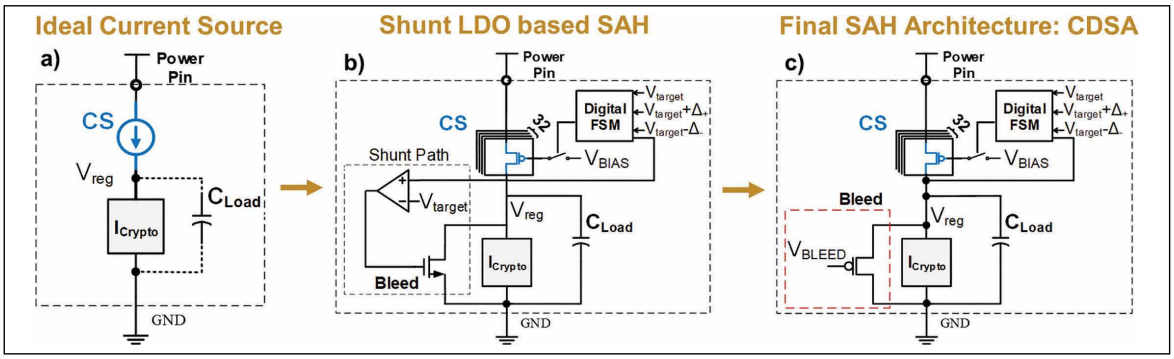

Figure 4. Build-up to the CDSA design: (a) ideal implementation, (b) SAH with SMC and active shunt LDO, and (c) CDSA Design: SAH with SMC and bypass bleed PMOS providing an inherent local negative FB.

the supply current (I_{CS}) is more than the crypto current (I_{Crypto}). A low-BW digital switched mode control (SMC) loop compensates for the process, voltage, and temperature (PVT) variations, and sets the I_{CS} to a quantization level closest to the average crypto current ($I_{Cryptoavg}$) by turning on or off the required number of CS slices, such that $I_{CS} = I_{Cryptoavg} + \Delta$. The quantization error in the supply current Δ is bypassed through the shunt bleed. In steady state, once the top CS current is equal to the average crypto current, the SMC loop is disengaged and the attenuation is thus given by the load capacitance and the output resistance of the CS stage, $AT = \omega C_{Load} r_{ds}$. Now, as discussed previously in Figure 3a, the MTD is proportional to AT^2, which means that a higher output resistance of the CS stage (r_{ds}) can reduce C_{Load}, lowering the area overhead for iso-attenuation (or iso-MTD). Hence, a cascode CS stage with very high output impedance is chosen so that the load capacitance can be significantly reduced.

During steady-state, the SMC loop is only engaged if the V_{reg} node voltage goes below $V_{target} - \Delta_-$ or is above $V_{target} + \Delta_+$, and remains disengaged as long as the voltage remains within the guard band. The low BW of the SMC loop ensures that the voltage fluctuations at the V_{reg} is not reflected instantaneously to the supply current, unlike series LDOs.

Finally, ASNI involves tiny amount of NI in the attenuated signature domain to further enhance the resilience against power SCA attacks [17].

Current domain signature attenuation

CDSA combines the SAH from ASNI and the local lower metal routing from the STELLAR approach to develop the world's most secure SCA countermeasure ($MTD > 1B$) with < 1.5× area and power overheads [15]. The main difference in the SAH design is the replacement of the active shunt LDO loop with a biased PMOS bleed, as shown in Figure 4c. This reduces the power overhead while maintaining the same SCA security enhancement. The bleed PMOS provides the bypass path to drain the extra quantization error (Δ) in the CS current, and also provides an inherent local negative feedback (FB) allowing any average crypto current in between two quantized levels of the CS.

The cascode CS stage is designed such that the unit current per slice is higher than the key-dependent variation in $I_{Crypto_{avg}}$, so that the key-dependent information in the average crypto current is not transferred to the supply current and is leaked by the bleed path, providing information-theoretic security [15].

CDSA does not include NI and has been implemented in TSMC 65-nm technology with local lower-metal routing up to M_6. The parallel AES256 is encapsulated by the CDSA hardware providing both EM as well as power SCA immunity.

Efficacy

Measurements results of the CDSA-AES256 show an active signature attenuation of > 350×. While the unprotected AES256 could be broken with only $8K$ and $12K$ traces, respectively, for CPA and CEMA attacks, the protected CDSA-AES remains secure even after $1B$ encryptions, showing an MTD improvement of 100 over the existing countermeasures [15] (Figure 5). The CPA and CEMA attacks were verified both in the time as well as frequency domain. Finally, to evaluate the effects of the metal

layers on the EM leakage, fixed versus random test vector leakage analysis (TVLA) was performed. With 200M total traces for the TVLA, the unprotected AES showed t-values of 1056 and 961 for power and EM TVLA respectively, while the protected implementation with lower metal routing showed power and EM TVLA of 12 and 5.1 respectively [18]. CDSA-AES256 with high-level metal routing showed an EM TVLA of 8.9, which is much higher than the CDSA implementation with lower metal routing, proving for the first time the effects of metal routing on the EM SCA leakage using on-chip measurements.

The proposed CDSA has also been evaluated against the DNN-based profiling power SCA attacks [22]. While the DNN could be fully trained using only $< 5K$ power traces for the unprotected AES256, the protected CDSA-AES256 could not be trained even after $10M$ traces, demonstrating the efficacy of the proposed countermeasure against DL based SCA attacks. This is also the first countermeasure validated against the DL SCA attacks.

Overall, against the nonprofiled attacks, the CDSA achieved $> 1B$ EM/power SCA MTD with 1.37× area and 1.49× power overhead. It is also a generic countermeasure and can be extended to any crypto algorithm providing both power and EM SCA protections without any performance overheads.

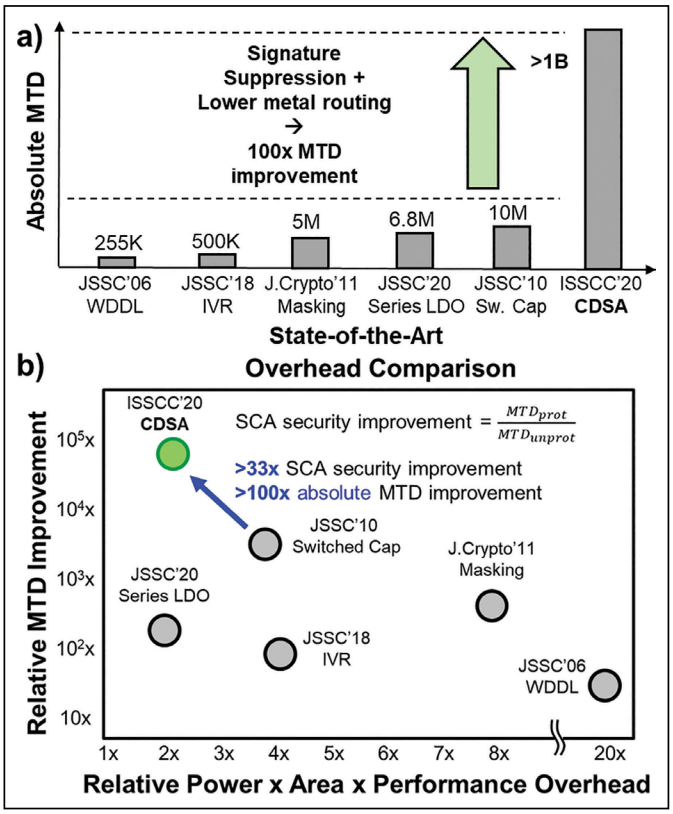

Figure 5. (a) MTD comparison and summary and (b) overhead comparison (power/area/performance/security) with state-of- the-art countermeasures.

Long-term impact and future directions

The proposed CDSA countermeasure can be integrated with both hardware and software crypto implementations and can be used to protect the entire crypto IP (multiple engines—AES/SHA/ECC) within a chip, without any change to the existing architectures. This configurability provides a huge benefit to the industry as they strive to preserve alegacy for their existing crypto implementations.

The proposed CDSA does not degrade the performance of the crypto engine, which is essential for any industry to market the product. In addition, the overheads involved are much lower compared to the most of the existing state-of-the-art countermeasures (which also may not be generic).

Future works can investigate fully digital implementations of the proposed CDSA hardware [18], [21], [23], [24]. This flexibility of such a synthesizable countermeasure would allow the industry to adopt to this circuit without having to put extra manual effort that comes with technology scaling.

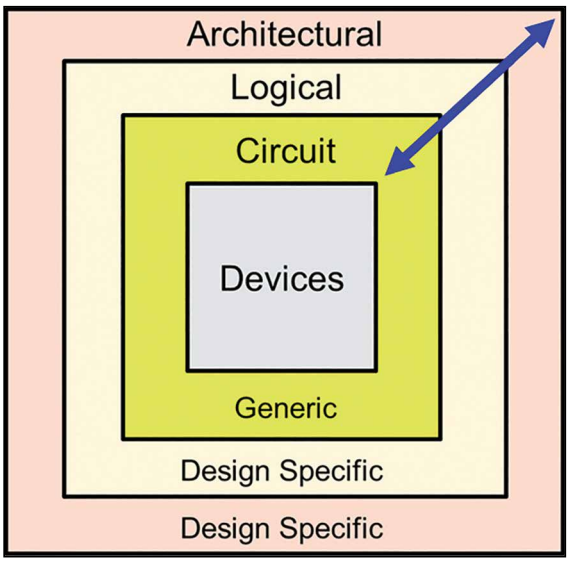

Figure 6. Future direction will involve cross-layer optimization of security, throughput, power, area through a combination of physical fields and its interaction with network and system to enhance system security.

As the number of Internet-connected devices increases, the threat surface for these resource-constrained devices increases significantly. Future research should focus on cross-layer optimization across the physical layers, combining network and system to enhance security while maintaining the throughput, power, and area constraints (Figure 6).

In summary, this article provides a low-overhead solution to the power/EM SCA attacks, while maintaining the legacy of the existing cryptographic algorithms, which are necessary requirements from an industry standpoint. CDSA along with lower-level metal routing demonstrated the highest MTD ($> 1B$) achieved to date with much lower overheads compared to the state-of-the-art countermeasures. Without incurring any performance overhead, this generic solution tries to bridge the gap between the research community and industry demands. ■

Acknowledgments

This work was supported in part by the National Science Foundation (NSF) under Grant CNS 17-19235 and Grant CNS 19-35573 and in part by Intel Corporation.

■ References

[1] E. Ronen et al., "IoT goes nuclear: Creating a ZigBee chain reaction," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 195–212.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. CRYPTO*, vol. 99, Aug. 1999, pp. 388–397.

[3] J.-J. Quisquater and D. Samyde, "Electro magnetic analysis (EMA): Measures and counter-measures for smart cards," in *Proc. Smart Card Program. Secur.*, 2001, pp. 200–210.

[4] S. Chari, J. R. Rao, P. Rohatgi, "Template attacks," in *Proc. CHES*, B. S. Kaliski, K. Koç, and C. Paar, Eds. Berlin, Germany: Springer, 2002, pp. 13–28.

[5] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. CHES*, 2004, pp. 16–29.

[6] G. Hospodar et al., "Machine learning in side-channel analysis: A first study," *J. Cryptograph. Eng.*, vol. 1, no. 4, p. 293, Oct. 2011.

[7] S. Sen and A. Raychowdhury, "Electromagnetic and machine learning side-channel attacks and low-overhead generic countermeasures," presented at the CHES. Accessed: Mar. 19, 2021. [Online]. Available: https://ches.iacr.org/2019/src/tutorials/ches2019 tutorial_Sen.pdf

[8] D. Das et al., "X-DeepSCA: Cross-device deep learning side channel attack," in *Proc. 56th Annu. Design Autom. Conf.*, Jun. 2019, pp. 1–6.

[9] D. D. Hwang et al., "AES-based security coprocessor IC in 0.18-μm CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.

[10] M.-L. Akkar et al., "Power analysis, what is now possible," in *Proc. ASIACRYPT*, 2000, pp. 489–502.

[11] A. Poschmann et al., "Side-channel resistant crypto for less than 2,300 GE," *J. Cryptol.*, vol. 24, no. 2, pp. 322–345, Apr. 2011.

[12] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010.

[13] M. Kar et al., "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," *IEEE J. Solid-State Circuits*, vol. 53, no. 8, pp. 2399–2414, Aug. 2018.

[14] A. Singh et al., "Enhanced power and electromagnetic SCA resistance of encryption engines via a security-aware integrated all-digital LDO," *IEEE J. Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, Feb. 2020.

[15] D. Das et al., "27.3 EM and power SCA-resilient AES-256 in 65 nm CMOS through >350× current-domain signature attenuation," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2020, pp. 424–426.

[16] D. Das et al., "STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2019, pp. 11–20.

[17] D. Das et al., "ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 10, pp. 3300–3311, Oct. 2018.

[18] D. Das et al., "EM and power SCA-resilient AES-256 through >350× current-domain signature attenuation and local lower metal routing," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, Jan. 2021.

[19] D. Das et al., "Killing EM side-channel leakage at its source," in *Proc. IEEE 63rd Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2020, pp. 1108–1111.

[20] D. Das et al., "High efficiency power side-channel attack immunity using noise injection in attenuated

signature domain," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2017, pp. 62–67.

[21] A. Ghosh et al., "An EM/Power SCA-resilient AES-256 with synthesizable signature attenuation using digital-friendly current source and RO-bleed-based integrated local feedback and global switched-mode control," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2021, pp. 499–501.

[22] D. Das et al., "Deep learning side-channel attack resilient AES-256 using current domain signature attenuation in 65nm CMOS," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Mar. 2020, pp. 1–4.

[23] D. Seo et al., "Enhanced detection range for EM side-channel attack probes utilizing co-planar capacitive asymmetry sensing," presented at the IEEE DATE, 2021.

[24] D. Das and S. Sen, "Electromagnetic and power side-channel analysis: Advanced attacks and low-overhead generic countermeasures through white-box approach," *Cryptography*, vol. 4, no. 4, p. 30, Oct. 2020.

Debayan Das is currently pursuing a PhD in electrical and computer engineering with Purdue University, West Lafayette, IN, USA, working with Prof. Shreyas Sen. His research interests include mixed-signal IC design and hardware security. Das has a bachelor's in electronics and telecommunication engineering from Jadavpur University, Kolkata, India (2015). He is a Student Member of IEEE.

Santosh Ghosh is currently a Security Researcher with Intel Corporation, Hillsboro, OR, USA, where he joined in 2012. His research interests includes design and implement cryptographic hardware microarchitecture and RTL with aggressive area, latency, and throughput constraints; multiple of them are already being deployed in high-volume Intel products; investigate and develop timing, power, and EM side-channel countermeasures; collaborate with academic partners; and provide cryptography and security guidance to Intel business units. Ghosh has a PhD and postdoctoral studies in cryptographic hardware and side-channel attacks.

Arijit Raychowdhury is currently a Professor with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA, where he joined in January 2013. His research interests include low power digital and mixed-signal circuit design, design of power converters, sensors, and exploring interactions of circuits with device technologies. Raychowdhury has a BE in electrical and telecommunication engineering from Jadavpur University, Kolkata, India (2001) and a PhD in electrical and computer engineering from Purdue University, West Lafayette, IN, USA (2007). He is a Senior Member of IEEE.

Shreyas Sen is currently an Associate Professor in electrical and computer engineering with Purdue University, West Lafayette, IN, USA. His current research interests span mixed-signal circuits/systems and electromagnetics for the Internet of Things (IoT), biomedical, and security. Sen has a PhD in electrical and computer engineering from Georgia Tech, Atlanta, GA, USA. He is a Senior Member of IEEE.

■ Direct questions and comments about this article to Shreyas Sen, School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA; shreyas@purdue.edu.