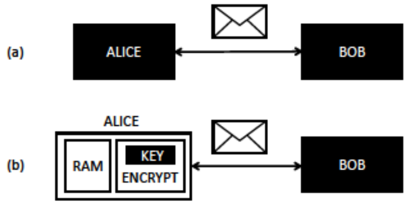
2022 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI) | 978-1-6654-0929-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/EMCSI39492.2022.9889394



The Technological Arm

Shahin Tajik
Worcester
{stajik, ps

Abstract—For many years there has been an arms
between designers and adversaries of secure hardware. Impr
ments in the strategies for attack spur new defense technic
and better defenses lead to improved attacks. In this contribu
first, we examine the technological dimensions of this a
race. While defenders benefit from increased circuit der
and decreasing feature size, attackers benefit from novel s
channel attack vectors based on optical and electromag
interactions with their target. Second, we analyze the feasil
and applicability of various side-channel attacks on primary u
of cryptographic hardware. We also discuss the required t
cost, and expertise to mount these attacks. We then examine
well modern defense methods are capable of thwarting mo
attack methods.

Index Terms—Hardware Security, Physical Security, S
Channel Attacks;

I. Introduction

Hardware security is a general term to describe the use of hardware components to preserve the security properties of an overall design. These security properties may relate to the information processed by the hardware design as well as to the hardware implementation itself. These properties are not absolute, and they can be undone by determined hackers or adversaries. Encryption keys may be stolen and a hardware root-of-trust may be impersonated, thereby rendering the secure hardware useless. The goal of the secure hardware designer is therefore twofold. First, the designer must create a secure hardware design at a desired performance point. Second, the designer must make sure that the security properties of the design can be enforced against a knowledgeable adversary who observes or tampers the secure hardware design.

To establish a baseline, a secure design is commonly evaluated under an *attacker model*, a summary of the assumed capabilities of an attacker. The attacker model thus describes what an adversary can and cannot do. A classic attacker model from the world of information security is the *black-box model* shown in Fig. 1a. Alice and Bob can exchange secure messages because they are working in a black box that perfectly hides the encoding and decoding of secure messages.

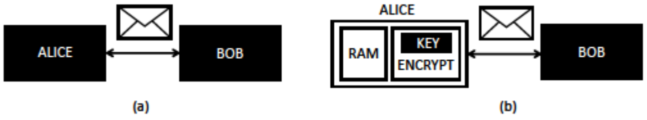


Fig. 1. (a) Traditional Black-box Model (b) Vanishing Black-box Model

However, the black-box model does not translate very well to the world of hardware. Alice clearly makes use of interconnected hardware subsystems, modules, components, and transistors to create secure messages, and these hardware subsystems are observable by the adversary. Over the past few decades, those adversaries have developed a wide array of hardware measurement techniques using power-based, electromagnetic, and optical side-effects. They are able to uncover the lid of Alice's black box, module by module, down to a single transistor.

In response, Alice has improved her abilities to uphold the black-box model. In the example of Fig. 1b, the secure hardware designer used a shielded, tamper-resistant storage module to store a secure key, while other components, such as the RAM storage and encryption logic, remained unprotected. A shielded key storage module may thwart an attacker who aims to probe the key value directly from the chip. However, it is only a partial solution, and it may not prevent side-channel leakage from the encryption module, or fault injection into the encryption module, both of which can indirectly reveal the key value. The challenge of the secure hardware designer is therefore as follows. Given that the black-box model of Alice cannot be supported at the system level, how should the black-box model be realized such that the system-level security properties are preserved?

We call this the *Vanishing Black-box Model*. Given a knowledgeable adversary who is able to observe and manipulate secure hardware components at various abstraction levels, the secure hardware designer builds the physical equivalent of a black box to hide the secure-sensitive parts of a design. The *vanishing* aspect of the black-box reflects that the secure designer wishes to minimize the cost, complexity and physical size of the black box in the realization. In essence, the black-box partitions the hardware design between the security-sensitive part that must be defended using dedicated hardware countermeasures, and the generic part that does not need such countermeasures. The secure hardware designer has a broad range of techniques available to build a black box, such as physical and electromagnetic shielding, buffering and leveling of energy, isolation and restructuring of hardware elements, and monitoring of signal levels and physical events.

In this paper, we will focus on side-channel attacks, which is a class of attacks that bypasses the black-box model by observing the physical behavior of a secure hardware module. In the next section, we investigate the technological progress that has been made in side-channel measurements of secure hardware. In section III, we review recent progress in the countermeasures against these attacks. Finally, we summarize the open challenges for both the adversary and the defender, and conclude the paper.

II. Side-Channel Attacks

Side-channel leakage covers any data-dependent behavior that can be observed by an external adversary. In the context of dedicated hardware implementations, the data-dependent transition or even static state of transistors can be exploited by, for instance, power consumption [1], Electromagnetic (EM) emanation [2], temperature [3], photon emission [4], and electrical probing [5]. In this section, first, we review the known *physical* SCA attacks. Afterward, we compare them in terms of cost, resolution, and effectiveness against different parts of cryptographic hardware.

A. Power Analysis

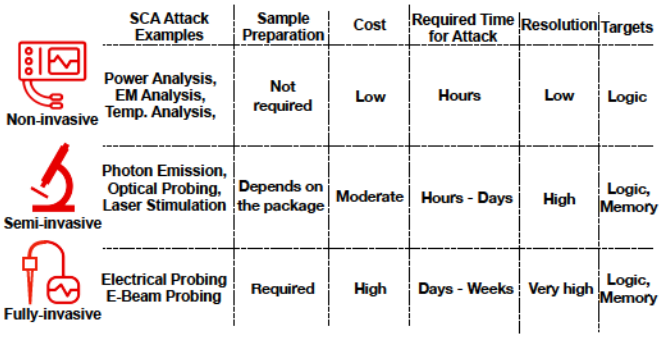
Power analysis is one of the first discovered and most researched non-invasive SCA attack methods in the literature [1]. An integrated circuit's power consumption reflects the combined activity of its individual primitives. The state and activity of some transistors are determined by the data that the circuit is processing, and hence, measuring the dynamic and static power consumption contains information about a circuit's computation on the data. While in power analysis attacks, only one physical probe is usually available to capture the entire circuit's power consumption, the effects of a single transistor appear as weak correlations in power measurements, even though they are not immediately observable. When a cryptographic device processes secrets, its data-dependent power consumption can make them vulnerable to power analysis attacks.

B. Electromagnetic Analysis

Electromagnetic (EM) analysis is another powerful non-invasive SCA attack technique. The switching of transistors inside an IC causes changing currents, which flow through the metal layers of the IC. In this case, the metal interconnects behave like antennas and emanate electromagnetic waves due to the presence of the time-varying current. The induced EM emission from some of the transistors and gates of a circuit depends on the calculated data by the circuit [2]. Therefore, the calculation in cryptographic hardware can result in secret dependent EM emissions, which might reveal the secret data. The primary advantage of the EM analysis attack compared to power analysis is its higher resolution, which makes capturing emissions from various locations of the chip feasible.

C. Temperature Analysis

The power consumption of transistors inside a chip gives rise to the temperature. Therefore, if an adversary can measure the changes in the temperature during a cryptographic operation, attacks similar to simple power and EM analysis are conceivable. However, the rate of data-dependent temperature variation is much lower than that of power consumption [3]. Consequently, temperature side-channel is feasible if the target device can be operated with a slower clock frequency.



	SCA Attack Examples	Sample Preparation	Cost	Required Time for Attack	Resolution	Targets
Non-invasive	Power Analysis, EM Analysis, Temp. Analysis,	Not required	Low	Hours	Low	Logic
Semi-invasive	Photon Emission, Optical Probing, Laser Stimulation	Depends on the package	Moderate	Hours - Days	High	Logic, Memory
Fully-invasive	Electrical Probing E-Beam Probing	Required	High	Days - Weeks	Very high	Logic, Memory

Fig. 2. Side-channel attack (SCA) spectrum, requirements, and capabilities.

D. Photon Emission Analysis

To capture leakage from an integrated circuit at the scale of a single or a handful of transistors, semi-invasive optical techniques, known from failure analysis (FA), have been considered as attack methods. Photon emission (PE) analysis was one of the first optical techniques deployed for SCA. During switching events, transistors pass through saturation for a short period. In saturation, MOS transistors emit photons due to carriers traveling through the space charge region near the drain diffusion. The emission intensity depends on the applied voltages, conducted current, and time spent in saturation. PE can be used to capture weak photon emissions of the switching transistors from the IC backside and link them to the running software or circuit [4] on the chip.

E. Laser Stimulation

A number of techniques have been developed in FA, which use laser radiation to influence the device under test (DUT). These techniques are referred to as laser stimulation techniques and measure changes in device parameters in response to the incident of laser radiation [6]. This is usually performed by scanning a region of interest with a laser beam and monitoring the device parameters. The monitored parameters are often simply voltage or current at a specific device pin. Laser stimulation can be deployed to localize and read the state of the memory cells [7].

F. Optical Probing

Optical probing is another optical FA method that can measure the on-die signals in a contactless manner. For optical probing, a laser beam irradiates the transistors from the IC backside, and the reflected light is evaluated to detect data dependencies. The electrical properties of the device affect the refractive index and absorption coefficient of silicon, and thus, the transistors, based on their states, partially absorb and partially reflect the laser beam. Optical probing is one of the most powerful and threatening side-channel attacks, which can localize points of interest and recover confidential signals from any parts of the hardware, including logic and memory [8], [9].

G. Electrical Probing

Electrical probing is a fully-invasive contact-based method for direct probing of signals from metal interconnects or

transistors [5]. In this case, special thin needles are
to contact the point of interest to sense voltage/curr
trical probing is usually used in conjunction with
Ion Beam (FIB) editing [5]. FIB is deployed t
the materials as well as deposit materials to make
Such a measurement tool can be used to extract co
information from all main blocks of a cryptographi
e.g., logic, metal interconnects, and memory.

H. E-Beam Probing

E-beam probing is one of the less researched
contactless probing techniques, which utilizes electr
to probe on-die signals [10]. Similar to photons, ele
affected by the electric field of various transistors. T
measuring the backscattered electrons can reveal
of the transistors. More research needs to be ca
to understand the potentials of this technique. In
to optical probing, e-beam probing can achieve
resolutions, which is relevant for technologies below

I. Comparison of Attacks

Here, we briefly compare the SCA attacks regar
cost, resolution, and targets, see Fig. 2..

1) Resolution: The effectiveness of non-invasive
limited due to their susceptibility to noise and low re
In other words, they cannot directly distinguish the a
individual transistors in a large and complex circuit. On the contrary, fully-invasive attacks provide the highest resolution. For example, electrical and e-beam probing attacks enable the adversary to probe different wires and transistors with a resolution of a few nanometers. Semi-invasive attacks, which are largely based on near-infrared optical tools, also have much higher resolutions than non-invasive attacks. However, their resolution is limited due to the wavelength of the photons. The resolution of optical methods can be improved significantly using solid immersion lenses (SILs) or visible light wavelengths to obtain resolutions in the order of tens of nanometers at the cost of becoming more invasive.

2) Target: Non-invasive SCA attacks usually provide a single probe to capture the information leakage of all switching transistors of a circuit during the computation. However, due to their low resolution, they cannot be deployed to directly read out individual memory cells (e.g., SRAM and flash cells) or output of key generation primitives, such as Physically Unclonable Functions (PUFs) or True Random Number Generators (TRNGs). Semi- and Fully-invasive attacks, on the other hand, are capable of directly probing individual memory cells as long as their resolution suffices. Certain invasive techniques, such as optical and electrical probing, can even recover data from circuits and memories in steady states.

3) Cost: Some SCA attacks can be mounted non-invasively, i.e., the package of the IC under attack is not required to be removed. These attacks are inexpensive, and they usually need a few hours to succeed. Power, EM, and temperature analysis are examples of non-invasive SCAs. On the contrary, the fully-invasive attacks are partially destructive, i.e., the package of the IC as well as the metal layers on the IC frontside or part of the silicon substrate on the IC backside need to be removed. Hence, such attacks are costly and time-consuming, and in some cases, they might even destroy the assets under attack. Naturally, more samples might be needed for a successful attack. Such attacks usually require days to weeks to get accomplished. Semi-invasive optical attacks are in the middle of the spectrum in terms of cost. If the target IC is available flip-chip packages, these attacks can be launched even in a non-invasive fashion as the backside silicon of the IC is already exposed for near-infrared wavelengths, and hence, no package removal is required. Consequently, these attacks are advantageous in scenarios where only one sample is available.

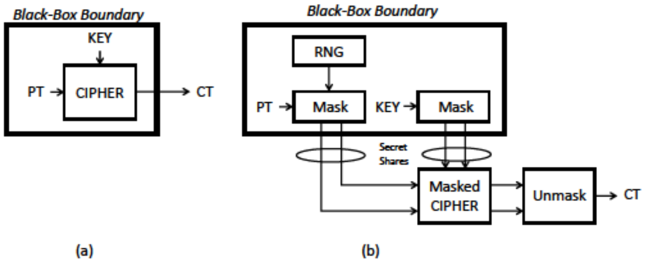


Fig. 3. (a) Unprotected Cipher (b) Masking-protected Cipher requires a random number generator and protected masking operations

III. Side-Channel Countermeasures

Side-channel countermeasures aim at reducing or eliminating the observation of data-dependent circuit behavior in any form – electrical current, electromagnetic radiation, or photon emission. The Vanishing Blackbox principle aims to encapsulate any transistor or wire that carries data-dependent charges in such a way that residual side-channel leakage no longer allows successful side-channel analysis. The black-box defense in VLSI circuits is a physical artifact.

In our summary, we only consider holistic countermeasures, meaning that we only consider complete black-box implementations. Indeed, the implementation of a countermeasure may inject additional security requirements into the design. An example is the use of so-called masking-based countermeasures, which have been extensively investigated in the past decade [11]. In a masking-based countermeasure, secure data is partitioned into two or more secret shares using a masking operation and a random number generator (Figure 3b). The security of the masking scheme relies on the secrecy of the random number stream. Therefore, masking introduces a secure random number generation requirement which must be included in the black-box model of the design. The transformation of unmasked secret variables into masked tuples of secret shares is a black-box operation as well.

In the following analysis, we focus on countermeasures that can be used at the lowest abstraction level of digital hardware design, at circuit-level, or below. Table II describes five different countermeasures (different from masking) which are commonly used at the lowest level of hardware design,

TABLE I
HARDWARE COUNTERMEASURE TECHNIQUES

Countermeasure	Description	Examples
Shielding	Physical Covering of Sensitive Areas	[12]–[15]
Flattening/ Leveling	Hiding of Circuit Activity	[16]–[22]
Restructuring	Isolation of Sensitive Areas	[23]
Sensing	On-chip Detection Circuit	[24]–[28]
Pre-silicon	Design Analysis Technique	[29]–[32]

and which apply to the entirety of the design netlist. These countermeasures are application-agnostic, and in most cases can be expressed as simple transformations on the overall hardware design netlist.

A. Shielding

In a shielding countermeasure, the sensitive area of a chip is physically covered using a physical shield made from a mesh of metal wires. Fig. 4 demonstrates that both the front-side of a chip as well as the backside are susceptible to attacks. Depending on the packaging and die mounting, a frontside shield is used to prevent probing, while a backside shield is used to prevent access to the silicon substrate.

Frontside shields can be implemented using the top-level metal layers of a chip, routed into a dense mesh pattern. Because Focused Ion Beam (FIB) probing techniques are invasive, the integrity of the front-side shield is actively monitored by transmitting a cryptographic pseudo-noise test-pattern from one side of the mesh to the other side [12]. However, such a dedicated shield causes overhead. In a sample application, the shield consumes the top-layer of metal, and adds test circuitry, resulting in 48% area overhead and 164% power overhead to protect an AES cipher. The overhead of front-side shielding can be reduced by re-using existing non-critical nets of the design as shield wires, and migrating sensitive wires to the lower layers of the chip [13].

Backside shielding covers the substrate, and additional silicon processing steps are needed to coat the chip backside with metal. The backside shield prevents measurement of substrate noise for side-channel measurement as well as laser injection through the substrate. Backside Burried Metal (BBM) enables patterning of a mesh pattern on the backside of the chip [14]. Using Through-Silicon Via (TSV), the wire can be monitored by on-chip logic for continuity. As with frontside shields, the backside shield must be actively monitored for tamper.

Backside shielding and frontside shielding can potentially be removed through micro-milling. To prevent this, additional TSVs are added to weaken the chip. This would cause physical breakage of the chip under mechanical milling stress [15].

B. Flattening and Leveling

The idea behind flattening is to reduce side-channel leakage by removing power variations in hardware activity. This technique was originally developed as a secure logic style with constant-power behavior [33]. At chip-level, redundant direct - and complementary logic can ensure near-constant dynamic power consumption [16]. Furthermore, complementary logic can also reduce EM provided that routing is carefully controlled.

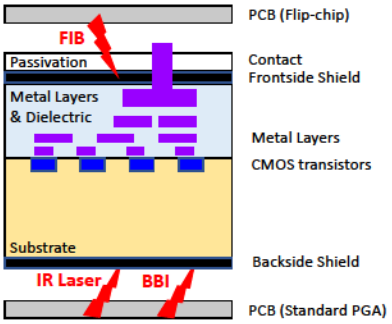


Fig. 4. Chip cross-section showing location of frontside and backside shielding

More recently, several variations of flattening have been developed that optimize the chip power conversion and power distribution network. Figure 5 illustrates a current equalizer circuit [17] which works in three phases. Initially, the *Charge* switch closes and fully charges a capacitor. Next, the *Charge* switch opens and the *Buffer* switches closes. The secure load then performs a sensitive operation which does not fully discharge the capacitor. Finally, the *Discharge* switch closes and the *Buffer* switch opens, which clears the remaining charge on the capacitor. This completes a full cycle. The outside power source delivers the same amount of charge per charge cycle, and therefore the secure load appears to have no power-based side-channel leakage. In a sample 130nm design, this technique introduces 33% power overhead and 100% performance overhead [17]. Current equalization has also been proposed as a cell-level countermeasure [18].

An alternate implementation of the energy buffer technique of Figure 5 is to use a current source that feeds a secure load in parallel with a current bypass path [19]. Current control can be combined with controlled routing that routes the secure-sensitive current path along multiple parallel connections on lower-layer metal. The resulting countermeasure then eliminates both power-based and EM-based side-channel leakage.

Another approach to flattening is to move the power regulator on-chip. The power regulator acts as a low-pass filter for power variations, thereby reducing side-channel leakage. In one recent design, a low drop-out regulator (LDO) is combined with power randomization (Voltage/Frequency Modulation) to both reduce the side-channel leakage and increase the power measurement noise [20]. A sample 130nm design has a 38% power overhead and 10% performance overhead, and offers both power-based and EM-based side-channel leakage reduction. Integrated voltage regulators based on switched-capacitor design offer a similar integration-with-randomization advantage [21]. A sample 28nm design has 15% power overhead and no performance overhead.

Finally, leveling of side-channel leakage can also be achieved at register-transfer level (RTL). By unrolling a sequential design over multiple rounds of a cipher, the side-channel leakage of multiple rounds is mixed in a single clock cycle [22]. This significantly increases the algorithmic noise

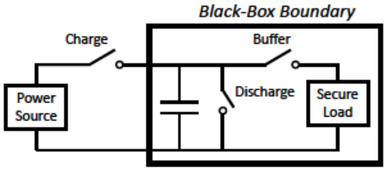


Fig. 5. Current Equalizer Diagram to reduce power-based side channel leakage

in the side-channel leakage.

C. Restructuring

A third class of techniques works on transformations of the design, with the objective of isolating or hiding sensitive areas of a chip. Attacks are limited by the physical dimensions of their measurement technique. For example, the 0.5mm radius of a high-resolution EM probe is still relatively large compared to the feature size on a 65nm chip (a ratio of 770K). It is worthwhile to exploit this difference as a countermeasure. Figure 6 describes several recently proposed techniques applicable to integrated circuits [23]. First, redistributing the most active modules spatially over a design reduces the peak-current draw in the local power grid that would cause EM leakage. Next, standard-cell based decoupling capacitors reduce the peak switching current in the power grid, further reducing EM. Finally, a wide grounded shield reduce EM emissions. A sample design in 40nm with these three features installed reduces the side-channel resistance (MTD) by 2.71 times [23].

D. Sensing

On-chip sensors are used to detect external side-channel measurement probes. In addition, on-chip sensors monitor the generation of on-chip side-channel leakage.

EM side-channel measurements require a sensing coil in the proximity of the side-channel leakage. By measuring the mutual inductance between a sensing coil and an on-chip sensing coil using a test EM field, the EM sensor can be detected [24]. Furthermore, thanks to a differential technique which measures frequency deviation of the EM field rather than the absolute frequency, system calibration is considerably simplified. On-chip detection of power-based side-channel measurement requires monitoring of the integrity of a chip's Power Delivery Network (PDN) [25]. Careful measurement of the impedance of the PDN on-chip using on-chip Vector Network Analysis technology can reveal anomalies such as shunt resistors, loading from capacitive probes, or changes in the power source [26].

A related challenge is the use of on-chip sensors to measure and assess side-channel leakage. This is especially relevant for cases where the application is not known beforehand, e.g., when using programmable components and processors. An on-chip noise measurement (OCM) sensor on a 180nm testchip consumes around 6400 μm^2 (around 240 GE) [27]. This sensor measures power variations and does not include digitization. On the other hand, its proximity to the source of side-channel leakage shows that only half the number of traces are needed compared to side-channel analysis using a targeted off-chip EM probe. The use of OCM also has applications in monitoring of power integrity under laser fault injection. A laser pulse to the junction node of a transistor creates electron-hole pairs, which causes a substrate current that is detected as a voltage peak on the power grid. A sample implementation shows a grid of 338 OCM sensors protecting a 128-bit AES [28].

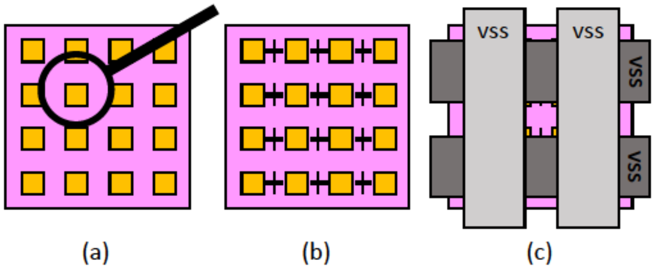


Fig. 6. Protection against fine-grained EM attacks on chips by (a) distributing information-leaky modules evenly over a layout (b) adding extra decoupling capacitors on the power grid (c) adding a top-layer grounded shield

E. Pre-silicon Techniques

Recently, the need for pre-silicon techniques to handle side-channel leakage issues has become apparent. On the one hand, security assessment of side-channel leakage needs to be done as early as possible in the design cycle, in order to detect and mitigate design errors early. On the other hand, commonly used side-channel leakage assessment techniques are based on post-silicon, black-box assessments. In the Vanishing Black Box model, we need to be able to pinpoint the source of side-channel leakage with a better precision, before we can shrink the black box. One aspect of pre-silicon side-channel leakage assessment relates to accurate simulation of power or electromagnetic radiation with sufficient performance and precision. One example of improved simulation techniques at the layout level is to characterize the side-channel leakage of library cells beforehand, and compose the side-channel leakage of the chip from the cells. This leads to a 110x speedup in the case of an AES-128 design [29]. Also, simulation of EM emissions can be specialized towards the side-channel leakage problem [30]. The next step after accurate simulation of side-channel leakage is its mitigation. While traditional mitigation techniques are formulated in terms of countermeasures (such as design transformations, injection of redundancy or randomness, etc), a design flow can also be constrained toward a given objective. For example, the position of side-channel leakage critical nets in a layout can be adjusted by controlling placement and routing [31], [32].

IV. Conclusion

Table II compares the attack vectors discussed in this paper to the countermeasures. It is clear that there is no single countermeasure that addresses all attack vectors, and practical designs need a range of defenses commensurate with the expected risk of the chip in the field. The composition of

TABLE II
COUNTERMEASURE EFFICIENCY

Vector	Shield	Flatten	Restructure	Sense	Pre-silicon
Power	o	+	+	o	+
EM	o	+	+	+	+
Temperature	o	+	o	+	o
Photon Emission	+	o	o	o	o
Laser Stim	+	o	o	+	o
Opt Probe	+	o	o	+	o
Electr Probe	+	o	+	+	+
E-Beam Probe	+	o	o	+	o

+ = countermeasure may be effective
o = countermeasure does not help (or effect unknown)

countermeasures is an open research challenge, although the majority of side-channel countermeasures in Table II can be independently deployed. The Vanishing Black Box model supports secure design refinement and keeps track of the reason for the countermeasures applied to a design.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual International Cryptology Conference*. Springer, 1999, pp. 388–397.

[2] D. Agrawal, B. Archambeault *et al.*, "The em side—channel (s)," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2002, pp. 29–45.

[3] M. Hutter and J.-M. Schmidt, "The temperature side channel and heating fault attacks," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2013, pp. 219–235.

[4] S. Tajik, D. Nedospasov *et al.*, "Emission analysis of hardware implementations," in *2014 17th Euromicro Conference on Digital System Design*. IEEE, 2014, pp. 528–534.

[5] C. Helfmeier, D. Nedospasov *et al.*, "Breaking and entering through the silicon," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 733–744.

[6] H. Lohrke, S. Tajik *et al.*, "Key extraction using thermal laser stimulation," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 573–595, 2018.

[7] T. Krachenfels, T. Kiyan *et al.*, "Automatic extraction of secrets from the transistor jungle using laser-assisted side-channel attacks," in *30th {USENIX} Security Symposium ({USENIX} Security 21)*, 2021.

[8] S. Tajik, H. Lohrke *et al.*, "On the power of optical contactless probing: Attacking bitstream encryption of fpgas," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1661–1674.

[9] T. Krachenfels, F. Ganji *et al.*, "Real-world snapshots vs. theory: Questioning the t-probing security model," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 1955–1971.

[10] R. Schlangen, R. Leihkauf *et al.*, "Backside e-beam probing on nano scale devices," in *2007 IEEE International Test Conference*. IEEE, 2007, pp. 1–9.

[11] A. Covic, F. Ganji, and D. Forte, "Circuit masking: From theory to standardization, A comprehensive survey for hardware security researchers and practitioners," *CoRR*, vol. abs/2106.12714, 2021. [Online]. Available: https://arxiv.org/abs/2106.12714

[12] J. Cioranesco, J. Danger *et al.*, "Cryptographically secure shields," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2014, Arlington, VA, USA, May 6-7, 2014*. IEEE Computer Society, 2014, pp. 25–31.

[13] H. Wang, Q. Shi *et al.*, "A physical design flow against front-side probing attacks by internal shielding," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 39, no. 10, pp. 2152–2165, 2020. [Online]. Available: https://doi.org/10.1109/TCAD.2019.2952133

[14] T. Miki, M. Nagata *et al.*, "Si-backside protection circuits against physical security attacks on flip-chip devices," *IEEE J. Solid State Circuits*, vol. 55, no. 10, pp. 2747–2755, 2020.

[15] S. Borel, L. Duperrex *et al.*, "A novel structure for backside protection against physical attacks on secure chips or sip," in *2018 IEEE 68th Electronic Components and Technology Conference (ECTC)*, 2018, pp. 515–520.

[16] M. Doulcier-Verdier, J.-M. Dutertre *et al.*, "A side-channel and fault-attack resistant aes circuit working on duplicated complemented values," in *2011 IEEE International Solid-State Circuits Conference*, 2011, pp. 274–276.

[17] C. Tokunaga and D. Blaauw, "Secure aes engine with a local switched-capacitor current equalizer," in *2009 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, 2009, pp. 64–65,65a.

[18] A. Gornik, A. Moradi *et al.*, "A hardware-based countermeasure to reduce side-channel leakage: Design, implementation, and evaluation," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 8, pp. 1308–1319, 2015.

[19] D. Das, J. Danial *et al.*, "Em and power sca-resilient aes-256 through gt;350× current-domain signature attenuation and local lower metal routing," *IEEE Journal of Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, 2021.

[20] A. Singh, M. Kar *et al.*, "Enhanced power and electromagnetic sca resistance of encryption engines via a security-aware integrated all-digital ldo," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, 2020.

[21] R. Jevtic, M. Ylitolva *et al.*, "Em side-channel countermeasure for switched-capacitor dc–dc converters based on amplitude modulation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 6, pp. 1061–1072, 2021.

[22] A. Singh, N. Chawla *et al.*, "Energy efficient and side-channel secure cryptographic hardware for iot-edge nodes," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 421–434, 2019.

[23] M. Wang, V. V. Iyer *et al.*, "Physical design strategies for mitigating fine-grained electromagnetic side-channel attacks," in *2021 IEEE Custom Integrated Circuits Conference (CICC)*, 2021, pp. 1–2.

[24] N. Homma, Y. Hayashi *et al.*, "EM attack is non-invasive? - design methodology and validity verification of EM attack sensor," in *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, ser. Lecture Notes in Computer Science, L. Batina and M. Robshaw, Eds., vol. 8731. Springer, 2014, pp. 1–16. [Online]. Available: https://doi.org/10.1007/978-3-662-44709-3_1

[25] N. Gattu, M. N. Imtiaz Khan *et al.*, "Power side channel attack analysis and detection," in *2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, 2020, pp. 1–7.

[26] C. Iorga, "Solve power integrity problems in fpga systems using an embedded vector network analyzer," Signal Integrity Journal, January 2018. [Online]. Available: http://shorturl.at/lnwJ0

[27] D. Fujimoto, M. Nagata *et al.*, "A novel methodology for testing hardware security and trust exploiting on-chip power noise measurement," in *The 20th Asia and South Pacific Design Automation Conference*, 2015, pp. 749–754.

[28] M. Nagata, T. Miki, and N. Miura, "On-chip physical attack protection circuits for hardware security : Invited paper," in *IEEE Custom Integrated Circuits Conference, CICC 2019, Austin, TX, USA, April 14-17, 2019*. IEEE, 2019, pp. 1–6.

[29] L. Lin, D. Selvakumaran *et al.*, "Fast and comprehensive simulation methodology for layout-based power-noise side-channel leakage analysis," in *2020 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*, 2020, pp. 133–138.

[30] D. Poggi, P. Maurine *et al.*, "Protecting secure ics against side-channel attacks by identifying and quantifying potential EM and leakage hotspots at simulation stage," in *Constructive Side-Channel Analysis and Secure Design - 12th International Workshop, COSADE 2021, Lugano, Switzerland, October 25-27, 2021, Proceedings*, ser. Lecture Notes in Computer Science, S. Bhasin and F. D. Santis, Eds., vol. 12910. Springer, 2021, pp. 129–147.

[31] H. Ma, J. He *et al.*, "Security-driven placement and routing tools for electromagnetic side-channel protection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 6, pp. 1077–1089, 2021.

[32] J. Knechtel, J. Gopinath *et al.*, "Security closure of physical layouts ICCAD special session paper," in *IEEE/ACM International Conference On Computer Aided Design, ICCAD 2021, Munich, Germany, November 1-4, 2021*. IEEE, 2021, pp. 1–9.

[33] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *2004 Design, Automation and Test in Europe Conference and Exposition (DATE 2004), 16-20 February 2004, Paris, France*. IEEE Computer Society, 2004, pp. 246–251.