3-2024

Analysis of Countermeasures Against Remote and Local Power Side Channel Attacks using Correlation Power Analysis

Aurelien Tchoupou Mozipo
Portland State University, mozipo@hotmail.com

John M. Acken
Portland State University, john.acken@pdx.edu

Citation Details

Published as: Mozipo, A. T., & Acken, J. M. (2024). Analysis of Countermeasures Against Remote and Local Power Side Channel Attacks using Correlation Power Analysis. IEEE Transactions on Dependable and Secure Computing.

Analysis of Countermeasures Against Remote and Local Power Side Channel Attacks using Correlation Power Analysis.

Aurelien T. Mozipo, John M. Acken, *Member, IEEE*

Abstract*— Countermeasures and deterrents to power side-channel attacks targeting the alteration or scrambling of the power delivery network have been shown to be effective against local attacks where the malicious agent has physical access to the target system. However, remote attacks that capture the leaked information from within the IC power grid are shown herein to be nonetheless effective at uncovering the secret key in the presence of these countermeasures/deterrents. Theoretical studies and experimental analysis are carried out to define and quantify the impact of integrated voltage regulators, voltage noise injection, and integration of on-package decoupling capacitors for both remote and local attacks. An outcome yielded by the studies is that the use of an integrated voltage regulator as a countermeasure is effective for a local attack. However, remote attacks are still effective and hence break the integrated voltage regulator countermeasure. From the experimental analysis, it is observed that within the range of designs' practical values, the adoption of on-package decoupling capacitors provides only a 1.3x increase in the minimum number of traces required to discover the secret key. However, the injection of noise in the IC power delivery network yields a 37x increase in the minimum number of traces to discover. Thus, increasing the number of on-package decoupling capacitors or the impedance between locally measured power and the IC power grid should not be relied on as countermeasures to power side-channel attacks, for remote attack schemes. Noise injection should be considered as it is more effective at scrambling the leaked signal to eliminate sensitive identifying information.

***Index Terms*—Integrated voltage regulator, noise injection, power delivery network, on-package decoupling capacitors, side channel attacks, countermeasures, remote attacks, local attacks**

I. INTRODUCTION

POWER-side channel attacks (SCAs) exploit the sensitive identifying information present in the leaked power of the internal operation of a cryptographic engine. For this reason, some techniques published in the literature have attempted to change the signature of the leaked information to reduce or eliminate its correlation with the encryption algorithm by altering the IC power delivery network (PDN). One method uses an integrated voltage regulator (IVR) within the IC [1][2], which scrambles or filters the cryptographic engine current and delivers the regulator input current to the external world, which should now be only loosely correlated to the regulator output current, which is the IC operating current. Another method of scrambling the power delivery network is by injecting noise with either the integrated regulator or clocking circuitry into the IC grid PDN to reduce the correlation between the intrinsic IC power signature and the signal leaked to the outside world at the circuit board level [3][4].

One common practice for keeping IC power grid noise from propagating into external portions of the design is adopting on-package decoupling capacitors (OPDs). Filtering the signal generated by the cryptographic compute core is typically performed with the placement of decoupling capacitors close to the device pins to limit the voltage droop created by PDN impedance. Modern circuit designs move the decoupling caps on the package substrate closer to the IC bumps. However, given their functions, these OPDs can intuitively serve as a countermeasure against power SCA. The filtering performed by these OPDs has the unplanned but desirable effect of reducing the relationship between the encryption engine power trace and the trace captured at the board level by the malicious agent in a local attack scenario. However, how effective can they be, and how can their implementation be optimized to become an effective power SCA countermeasure? This novel approach is analyzed herein to quantify its effectiveness within a reasonable

This paragraph of the first footnote will contain the date on which you submitted your paper for review, which is populated by IEEE. It is IEEE style to display support information, including sponsor and financial support acknowledgment, here and not in an acknowledgment section at the end of the article. For example, "This work was supported in part by the U.S. Department of Commerce under Grant BS123456." The name of the corresponding author appears after the financial information, e.g. *(Corresponding author: M. Smith).* Here you may also indicate if authors contributed equally or if there are co-first authors.

The next few paragraphs should contain the authors' current affiliations, including current address and e-mail. For example, First A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@ boulder.nist.gov).

Second B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

Third C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba 305-0047, Japan (e-mail: author@nrim.go.jp).

Mentions of supplemental materials and animal/human rights statements can be included here.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org

and implementable design space.

II. Background

The theoretical success rate of a local power SCA scenario depends on the ability of the agent to closely correlate the leaked measurements with an estimated power model using non-profiled attacks, with distinguisher such as differential (DPA) [8] and correlation power analysis (CPA) [9], or profiled attacks such as template-based attacks [12], machine learning (ML) side channel attacks [13], and deep learning side channel attacks (DL-SCA) [21].

A. Power Side Channel Attacks Techniques

The distinguishers such as SPA, DPA, and CPA are classified as non-profiled attacks. As opposed to a non-profiled attack, a profiled attack emulates the behavior of the target victim on a similar device/environment to create a leaking template (profiling phase), then compared the correlated power traces of the victim with the template to uncover the secret key (extraction phase).

1) - Correlation power analysis

The basic hypothesis of DPA and CPA is that an estimation of the power consumed by an FPGA at time t is given by the number of bits that change values in the registers. However, the correlation can be significantly reduced or eliminated with the injection of noise into the captured traces by scrambling the encryption IC power grid [3][4].

Likewise, the result of a local attack can be impacted by the impedance of the subcircuit network between the source of the leakage at the IC's bumps and the location of the measurements by the agent on the system circuit board. Such a network presents a loop impedance and a path resistance that contribute to filtering the signal and thus impact the success rate of a local attack.

However, the PDN techniques described above fail to address the threat model of remote power SCA, where the malicious does not require physical access to the victim to orchestrate a successful attack.

Do remote power SCA (where the trace is captured by a trojan logic running inside the device) constitute a residual vulnerability for the PDN scrambling techniques described herein? To evaluate the effectiveness of the proposed countermeasures, the minimum traces to discover (MTD) are computed based on the correlation coefficient between the measurements (remote and local) and the estimated power of each key guess.

2) - Profiled attacks

The most popular profiled attacks in literature are template-based attacks [10][11][12], machine learning side channel attacks [13][14], and deep learning side channel attacks (DL-SCA) [15][16][17][18][19][20][21].

Template-based attacks, which are based on the Gaussian assumption (i.e., observed traces are well described by a Gaussian distribution) use the multivariate normal distribution to create a profile, which consists of the traces' specific covariance matrices and mean vectors [12][22].

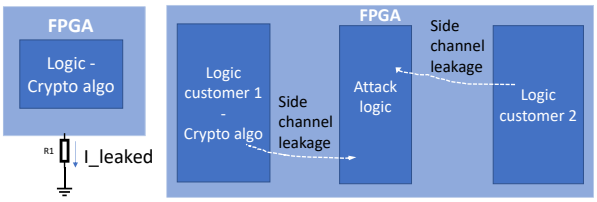


Fig.1: Side channel leaked information of an FPGA running a cryptographic algorithm. *Left:* power leaked for measured for a local attack. *Right:* malicious IP running in an FPGA to monitor local information and sending back to the malicious agent.

Another example of profiled attack is a machine learning (ML) based attack. In ML-based attacks, an ML technique replaces the multivariate normal distribution used in template-based attacks [13][22]. The binary classifier Support Vector Machine (SVM) can be used to first reduce the length of the power trace (feature selection), and then to learn the features of the power traces (classifier phase). SVM has been demonstrated as being effective to attack symmetric algorithms [23].

DL-SCA are very effective against not only single countermeasures such as masking, jitter, and random delay insertion but also on multiple countermeasures combined in implementations [21][22]. [20] has demonstrated a DL-based template attack technique named similarity learning used to derive relatively low-dimensional space data that are then fed into a template attack to improve its success rate.

B. Local vs. *remote attacks*

FPGA side channel attacks can be classified as local vs. remote. Local or direct side channel attacks are implemented when the agent has physical access to the targeted device (FPGA in our case) by observing the current consumed by the device [24]. Such current constitutes leaked information that can be exploited by the malicious agent to guess the algorithm encryption key. Fig. 1 depicts an example of a local attack vs. a remote attack.

With the emergence of the cloud computing field, such as FPGA as a service (FPGAaaS) and CPU/FPGA co-packaged chiplet architectures [25][26], more cryptographic algorithms are implemented in an FPGA located in a data center, where the compute fabric is shared with unknown workloads from unknown customers. Such co-implementation of multiple algorithms on the same FPGA fabric allows a malicious agent to launch an attack against a cryptographic algorithm implemented nearby to decipher the encryption key. The malicious agent who is renting partial sectors in the FPGA will be running a snooping IP that monitors vital FPGA information, such as the local voltage and temperature. The feasibility of such an attack was demonstrated by [27], where a malicious program consisting of a ring oscillator (RO) delivers a clock frequency depending on the IC local voltage. Time-to-digital converters (TDC) have also been demonstrated as an effective method for monitoring nanosecond scale transient voltage fluctuations [28][29][30] in an FPGA[31]. For both the RO and the TDC voltage monitoring scheme, the digital information returned is a representation of the local voltage, i.e., where the

malicious agent logic is implemented within the fabric. The voltage information is then used to run a power analysis to attempt to guess the encryption key of a cryptographic algorithm implemented nearby.

Besides PDN based countermeasures, masking is an effective method of protecting the implementations of crypto algorithms against power SCA. Some masking and PDN-based countermeasures are effective in fully preventing the successful power SCA, but others only increase the number of plaintexts or ciphertexts necessary to successfully attack the system.

C. Masking and Threshold Implementations Countermeasures

Masking undoubtedly constitutes the most effective countermeasure against the SCA under practical and rational leakage assumptions. Masking provides security against power and electromagnetic SCAs under a first-order DPA distinguisher. It consists of the technique of splitting sensitive information and variables inside a cryptographic algorithm into parts called shares so that each share analyzed on its own contains sensitive information. Therefore, only the combinations of all shares will contain information needed to uncover the sensitive information of interest.

At the application level, masking consists of modifying the execution of the algorithm implementation to ensure that the power or the leaked EMI is modified in a way that will not correlate to the power consumption of the unmasked algorithm implementation [32]. It has been proven that masking the AES by fake key addition reveals the fake key instead of the candidate's secret key. To some extent, this type of countermeasure is resistant to power SCA methods, such as CPA, the difference of means (DPA by Kocher), and the t-test. Masking has thus far been thought to be one of the most efficient countermeasures against power SCA [29][33].

Three-share threshold implementations (TIs) are also used as masking countermeasures in cryptography. The authors in [34] apply TI to lightweight ciphers and the AES in the Internet of Things (IoT) applications and use the DPA to verify improved protection against SCA. TI is a change in the cryptographic algorithm implementation to protect against the SCA. With TI, transactions from a single party in the communication cannot be used to uncover secret information.

TI is an improvement on Boolean masking because it provides security in the presence of glitches.

D. Threat models and vulnerability hypothesis

The models of the threats analyzed in this section assume the insertion of a voltage measuring logic circuit as a trojan RTL inside an FPGA or the insertion of a voltage monitoring circuit inside an ASIC by a contracting third-party house, unbeknown to the design owner. With the trojan RTL measuring the local IC PDN grid voltage, will the PDN-based countermeasures be effective in preventing remote SCA? Or will they only increase the number of plaintexts or ciphertexts necessary to successfully attack the system?

E. Our contribution

This research studies four PDN-related topics that by design are used as countermeasures to protect a cryptographic system against power SCA. Specifically, the study characterizes and evaluates the effectiveness of these PDN practices in improving the side channel leakage ability to reveal secret information. The practices analyzed in-depth herein are (i) the integration of an on-die voltage regulator, (ii) noise injection to scramble the IC PDN, (iii) the impedance of the subcircuit from the local capture point to the IC power grid, and (iv) the adoption of on-package decoupling capacitors. The current literature demonstrates the effectiveness of noise injection and integrated voltage regulators (IVRs) for local attacks; however, the effectiveness of those measures has not been studied in the case of remote attacks, which is one of this study's main focuses.

The goal is to generate methods for evaluating the PDN of a cryptographic system before fabrication to assess the ability of countermeasures to eliminate or lessen the exposure to malicious attacks for local attacks. Then, the study analyzes and characterizes the residual vulnerability threats of remote attacks. These vulnerabilities are still present in the system even after implementing a countermeasure.

A fast PDN simulation method for an IC is proposed and implemented. The method is applied on an FPGA running an AES256 cryptographic algorithm, followed by the implementation of the CPA distinguisher to successfully attack the device. The method is based on end-to-end system-level modeling that includes the chip power grid model, the package organic substrate PDN model, and the active elements representing the IC dynamic current. The simulations also focus on remote attack scenarios to contrast and compare the results against local attack schemes published in the prior art.

F. Organization of the paper

The paper starts with a summary analysis of PDN-based countermeasures' strengths, and a deduction of the residual vulnerabilities a cryptographic system still displays after the countermeasures have been implemented is given in Chapter III. Then, chapter IV expands the analysis with an in-depth theoretical analysis of the PDN-based deterrents to power SCA considered herein: IVR integration, voltage noise injection, on-package decoupling capacitors addition, and IC bumps-to-circuit board loop impedance. Chapter V focuses on the experimental studies that derive the results of local vs. remote attack scenarios, the impact of PDN noise injection, and OPD integration. The tail end of chapter V summarizes the impact of these power SCA countermeasures and deterrents while exposing their shortcomings in protecting against remote attacks.

III. Introduction to Residual Vulnerabilities on PDN-based Countermeasures

Since power side-channel attacks target the device power consumption signature, various prior studies have focused on altering the power delivery network (PDN) to scramble the device power signature to eliminate or reduce device vulnerabilities. Various PDN-based techniques have been proposed as countermeasures. Table I summarizes the categories and their strengths (the SCA techniques they are

TABLE I
PDN BASED COUNTERMEASURES STRENGTHS AND RESIDUAL VULNERABILITIES

PDN Countermeasure Schemes	Type of Power SCA analysis or distinguisher protected Against	Residual vulnerabilities
On-Chip Voltage Regulators as a Countermeasure [1][2]	• DPA • CPA	• SCA by remote power measurement • DPA with higher number of traces
Security-Aware Integrated Buck Voltage Regulator [5] [6]	• TVLA • CPA	• SCA by remote power measurement
Fully Integrated Inductive Voltage Regulator [7]	• TVLA • CPA	• SCA by remote power measurement
Noise Injection [3]	• DPA • CPA	• SCA by remote power measurement • CPA with an increased number of traces
Clock noise and voltage noise combination [4]	• Protection against SCA when noise is injected, and a clock randomizer (CR) is utilized. • Noise injection alone or CR alone performs efficiently against CPA	• Vulnerable to CPA/DPA SCA with remote measurement if the trojan logic is adequately located

protecting). A deduction of the residual countermeasure vulnerabilities is also proposed in the 3rd column. Most techniques involve the use of an IVR to scramble the current leaked to the external world[1][2][5][6][7]. However, voltage noise injection is also shown to be effective in reducing the vulnerability of the implementation against power SCA in local attack scenarios [35][36][37]. Decoupling capacitors are also used to decouple the crypto engine's current consumption from the current leaked outside the device. They are introduced on the Si power delivery grid or the power delivery network to reduce coupling among hardware shares [38][39][40][41][42].
The on-chip voltage regulator topologies used are multiphase, interleaved, buck converters, and multiphase switched capacitor converters. Conventional interleaved buck converters or switched capacitor converters have limited effectiveness in reducing the correlation factors used in CPAs. However, introducing random phase ordering or loop randomizing further reduces the correlation coefficients and thus renders the device less vulnerable [5][6]. However, those techniques are demonstrated only with local attacks. The side channel information is the power measured outside of the device power grid, with physical access to the victim. In the next subsections, the study attempts to show that remote attacks are still possible in the presence of PDN-based countermeasures. Remote attacks are the opposite of local attacks, as they require the attacker to be neither physically in proximity nor in the vicinity of the target device. Remote power measurement with a DPA distinguisher and with a higher number of traces is theorized to be a common weakness that these new techniques exhibit.

IV. Analysis of Power Delivery Network-based Deterrents to Power Side-Channel Attacks

A. Integrated voltage regulator as a countermeasure

The concept of using an IVR as a countermeasure works on the premise that the attacker measures the leaked power information locally by sensing the device's power pins or somewhere between the power pins and the external voltage regulator.

1) - Impact of an integrated voltage regulator against local attacks

The IVR aims to scramble the device's input current to reduce or remove the correlation with the internal operation. In Fig. 2a, the voltage or current measured at the local sensing point (which is representative of the IC power consumption) is a linear transformation of the current at the AES engine and thus will show a good correlation to this internal current of the AES engine. However, with the IVR integration, Fig. 2b, the transformation is active nonlinear and, therefore, there will be a poor correlation between the internal AES engine current and the leaked current measured by the attacker [7]. The impact of IVR as a countermeasure for local attack schemes has been studied in [1][2][5][6][7], therefore we'll refer the readers to this prior literature.

2) - Analytical formulation of correlation power analysis for remote attacks

For applications where the encryption is implemented in FPGA softcore logic, the attacker can implement a trojan logic that measures the voltage locally at the power grid and sends it to an offline processing center to run DPA or CPA [27][43]. In Fig. 2c, the voltage measured by the malicious agent remotely is tightly coupled to the cryptographic engine current and thus will exhibit a good correlation to this current.
Let us quantify the correlation impact for the various scenarios outlined in Fig. 2. Let us use the voltage at the node as a representative of the current through the node. This is a valid assumption because there is a linear relationship between both quantities and hence, a strong correlation exists between the two.
For a local attack scenario, the leaked measured voltage and the voltage at the engine are linked as follows:

$$V_1 = G_s V_1' \quad (1)$$

$$cov(V_1, H) = E[V_1 H] - E[V_1]E[H] = E[G_s V_1' H] - E[G_s V_1']E[H] = G_s cov(V_1', H) \quad (2)$$

$$\sigma_{V_1} = G_s \sigma_{V_1'} \quad (3)$$

where:

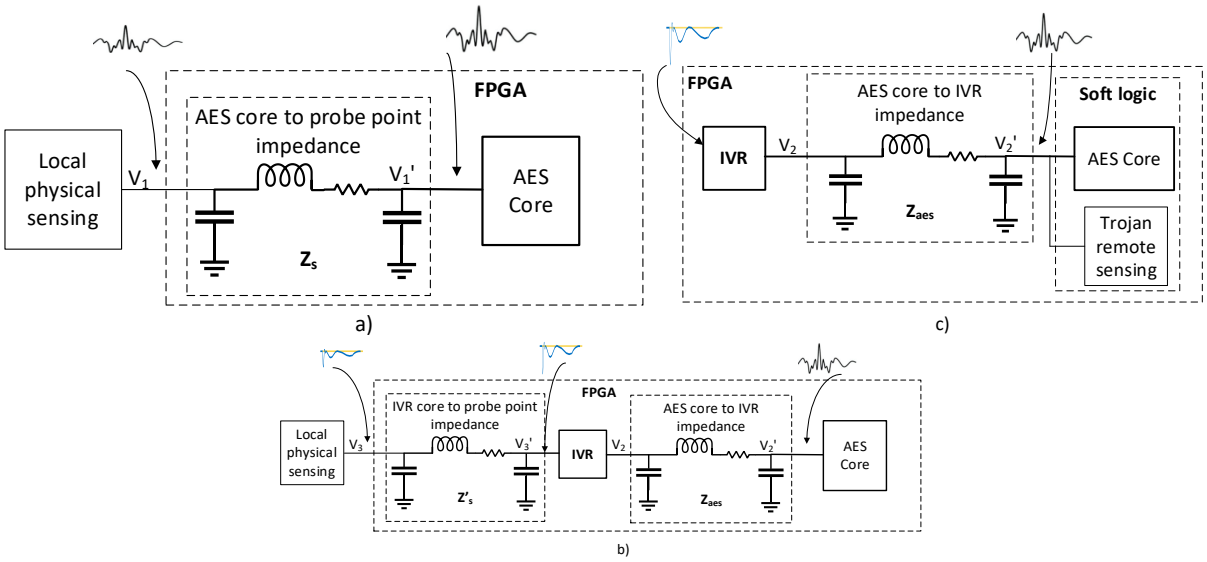


Fig. 2: Modeling of: a) - Local attack without IVR; b) - Local attack with IVR; c) - Remote attack with a trojan IP, in presence of IVR

G_s is the power delivery network impedance gain from the encryption engine to the local onboard measurement point,

H is the power estimation made by the attacker for CPA,

σ_{V_1} and $\sigma_{V_1'}$ are the standard deviations of the random quantities V_1 and V_1', respectively.

Similarly, the correlation coefficients are linked by the following relationships:

$$\rho_{V_1H} = \frac{cov(V_1,H)}{\sigma_{V_1}\sigma_H} = \frac{cov(V_1',H)}{\sigma_{V_1'}\sigma_H} = \rho_{V_1'H} \quad 4$$

$$V_2' = V_1' + G_{aes}V_2 \quad 5$$

$$cov(V_2',H) = cov(V_1' + G_{aes}V_2, H) = E[(V_1' + G_{aes}V_2)H] - E[V_1' + G_{aes}V_2]E[H] = E[V_1'H] - E[V_1']E[H] + G_{aes}(E[V_2H] - E[V_2]E[H]) = cov(V_1',H) + G_{aes}cov(V_2,H) \quad 6$$

$$\sigma_{V_2'}^2 = \sigma_{V_1'}^2 + |G_{aes}|^2\sigma_{V_2}^2 \quad 7$$

$$\rho_{V_2'H} = \frac{cov(V_2',H)}{\sigma_{V_2'}\sigma_H} = \frac{cov(V_1',H)+G_{aes}cov(V_2,H)}{\sigma_H\sqrt{\sigma_{V_1'}^2+|G_{aes}|^2\sigma_{V_2}^2}} \quad 8$$

ρ_{V_1H} and $\rho_{V_2'H}$ are the correlation coefficients between the locally onboard measured voltage and the estimated device power and between the remotely measured voltage and the estimated device power, respectively.

G_{aes} is the gain of the power delivery network impedance from the encryption engine to the IVR output.

σ_{V_2}, $\sigma_{V_2'}$, and σ_H are the standard deviations of the random quantities V_2, V_2' and H, respectively.

The IVR is designed to generate a voltage containing signature patterns that can scramble the encryption engine signature to protect against power SCA. It is an independent random variable and uncorrelated to the device's estimated power consumption. Hence, the correlation factor between the crypto device voltage and the estimated power consumption is written as:

$$\rho_{V_2'H} = \frac{cov(V_2',H)}{\sigma_{V_2'}\sigma_H} = \frac{cov(V_1',H)}{\sigma_H\sqrt{\sigma_{V_1'}^2+|G_{aes}|^2\sigma_{V_2}^2}} = \frac{\rho_{V_1H}}{\sqrt{1+|G_{aes}G_s|^2\left(\frac{\sigma_{V_2}}{\sigma_{V_1}}\right)^2}} \quad 9$$

3)- Impact of an integrated voltage regulator as a countermeasure on FPGA remote attacks

The relationship between the correlation coefficients in the remote measurement scheme in the presence of the IVR and the local measurement derived in Equation (9) above yields the following conclusions:

- Introducing the IVR reduces the magnitude of the correlation coefficients in the remote attack scenario and thus reduces the probability of uncovering the secret key.
- It shows how the new correlation factor can reject even the right key candidate. For example, if the IVR noise level is 1000x higher than the noise level at the local measurement point, the correlation factors are 100 to 1,000 times smaller. Hence, the number of plaintexts/ciphers required to successfully attack the implementation is significantly increased.
- The impedance of the power delivery network between the IVR and the remote sense location (i.e., the physical location of the encryption device) impacts the correlation coefficients and the probability of uncovering the secret key. As the gain G_{aes} approaches 1, i.e., the impedance Z_{aes} approaches zero, the correlation coefficients increase, signaling the increased effectiveness of the IVR in scrambling the voltage at the output of the crypto engine and thus reducing the probability of recovering the secret key.

Let us assume the following notations:

- The IVR random voltage source standard deviation normalized to the local sense voltage standard deviation, $\sigma = \frac{\sigma_{V_2}}{\sigma_{V_1}}$,
- The product of the gain of the impedance networks is called:

$$G = G_{aes}G_s \quad 10$$

TABLE II
COMPARISON OF CORRELATION FACTOR REDUCTION BETWEEN AN IVR IMPLEMENTATION ON A LOCAL ATTACK, TO POTENTIAL IVR IMPLEMENTATION WITH REMOTE ATTACK

	IVR and local attack [7]	**IVR with Loop Randomizer and local attack [7]**	**IVR with remote attack** ***IVR rel. noise: 10 PDN att: 0.1***	**IVR with remote attack** ***IVR rel. noise: 10 PDN att.: 0.9***	**IVR with remote attack** ***IVR rel. noise: 100 PDN att.: 0.1***	**IVR with remote attack** ***IVR rel. noise: 100 PDN att.: 0.9***
Correlation coefficients reduction ratio	1/5	1/30	1/1.4	1/9.1	1/10.1	1/90.1

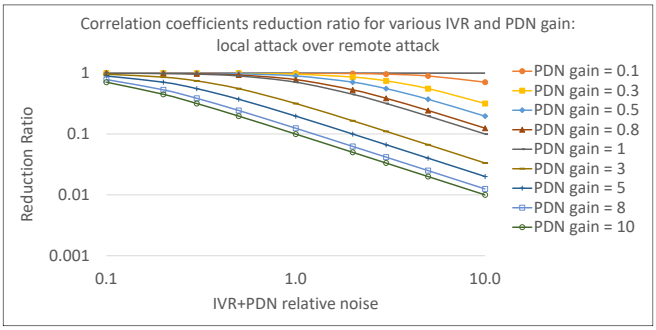


Fig. 3: Correlation factors reduction ratio as a function of the IVR (or other noise sources) relative noise, for various PDN impedance attenuations.

- The ratio of the correlation coefficients is denoted $\rho = \frac{\rho_{V'_2 H}}{\rho_{V_1 H}}$

Equation (9) above can be written as:

$$\rho = \frac{1}{\sqrt{1+|G|^2\sigma^2}} \qquad 11$$

Let us illustrate the impact of the IVR as a countermeasure with Fig. 3. The figure shows the plot of the IVR normalized correlation factor ρ vs. the IVR voltage standard deviation, normalized to that of the voltage noise of a local attack, parametrized by the product of network impedance attenuations. This shows that the IVR can reject the correlation factors used by the attacker in a remote scheme by attenuating them. The higher the IVR voltage spread (standard deviation) is, the higher the rejection. However, lower PDN attenuation renders IVR integration ineffective. As seen on the chart, the higher the gain G is, the lower the correlation coefficients. As an example, for an IVR relative noise level of 10 (10x higher than the voltage at the sense point of a local attack scheme), a reduction in impedance network attenuation from 0.9 to 0.1 (9x) results in an increase in the correlation coefficients from 0.11 to 0.7 (6.4x). Therefore, the use of IVR as a countermeasure is not an effective method, as the device PDN network may still allow the correlation coefficients to yield the secret key in a cryptanalysis case.

However, even in the presence of high attenuation, the IVR correlation coefficients, although reduced, may only increase the number of plaintexts or ciphertexts necessary to attack the system. Therefore, the effectiveness of the countermeasure hinges on the ability of the attacker to successfully mount an attack with an increased quantity of captured data.

4)- Comparison of theoretical correlation coefficients with prior art

[7] has demonstrated that with the integration of an IVR as a countermeasure, the reduction in the correlation factors is between 5x and 30x, resulting in increases in the minimum traces to discover (MTD) from ~5,000 to more than 500,000. Let us reiterate that the attack in their analysis is a local attack, i.e., the traces are now measured at the input of the IVR after it has scrambled the AES block signature.

Table II summarizes the correlation factor reduction obtained in the prior art by [7] with IVR used as a countermeasure against cryptanalysis of the implementation of the AES128 algorithm. In addition to a standard IVR, they also introduce the concept of a loop randomizer to randomize all transformations through the IVR. Thus, the IVR input current signature has an increased noise level, as seen by the local attacker, because there is no constant relationship between the captured measurements. The standard IVR produces a correlation factor reduction of 5x, whereas the introduction of a loop randomizer improves the reduction to 30x. However, as in our analysis, a remote attack on an IVR implementation has a reduction of ~1.4x - 9.1x when the relative IVR noise is 10 and 10.1x – 90.1x when the relative IVR noise is 100. A relative IVR noise of 100 amounts to an IVR feature with an efficiency higher than the loop randomizer. To our knowledge, such a feature does not yet exist in the current literature.

In conclusion, an IVR with a remote attack only results in increasing the minimum trace to detection but still leaves it vulnerable to power side-channel attacks with correlation power analysis (CPA). The use of an IVR as a countermeasure is effective for a local attack, as shown in [7], but remote attacks can still be very effective and hence break the IVR countermeasure.

B. Voltage noise injection

Adding noise to a system to counter power side-channel attacks can be modeled as shown in Fig. 4. If v_n denotes the noise injected, Z_n denotes the impedance of the subcircuit from the noise injection point to the local measurement point, and Z_{aes} denotes the impedance of the subcircuit from the AES core location to the local measurement point, then the voltages are related by the equation below:

$$V'_1 = \frac{Z_{aes}+Z_n}{Z_n} V_1 - \frac{Z_{aes}}{Z_n} v_n \qquad 12$$

Assuming that the estimated power and the injected noise are uncorrelated, the correlation coefficients of the remotely measured voltage and the estimated power are:

content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3370711

$$\rho_{V_1'H} = \frac{cov(V_1',H)}{\sigma_{V_1'}\sigma_H} = \frac{cov\left(\frac{Z_{aes}+Z_n}{Z_n}V_1,H\right)-cov\left(\frac{Z_{aes}}{Z_n}v_n,H\right)}{\sigma_H\sqrt{\sigma_{V_1}^2+\sigma_{v_n}^2}} = \frac{\rho_{V_1H}}{\sqrt{1+G'^2\left(\frac{\sigma_{v_n}}{\sigma_{V_1}}\right)^2}} \quad 13$$

Denoting ρ as the correlation coefficient reduction ratio between the local board-level measurement and the remote silicon-level measurement:

$$\rho = \frac{\rho_{V_1'H}}{\rho_{V_1H}} = \frac{1}{\sqrt{1+G'^2\sigma^2}} \quad 14$$

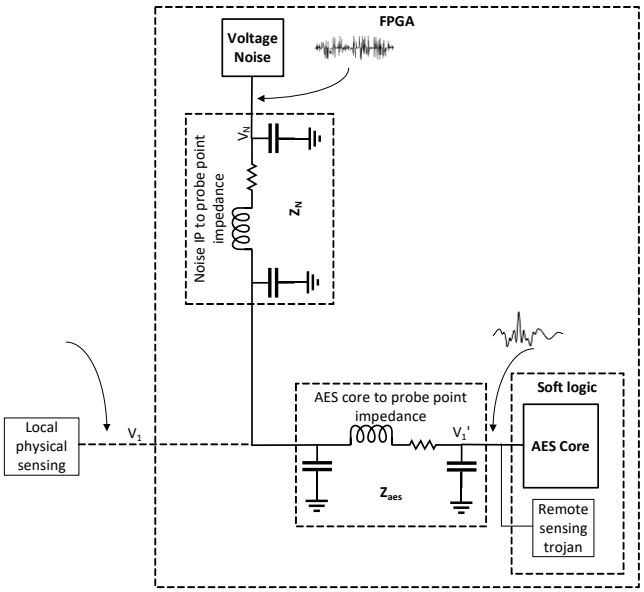


Fig. 4: Model of a noise injection as a power SCA countermeasure

where $\sigma = \frac{\sigma_{v_n}}{\sigma_{V_1}}$ is the relative noise standard deviation, i.e., normalized to the locally measured voltage standard deviation, and $G' = \left|\frac{Z_{aes}}{Z_{aes}+Z_n}\right|$ 15

This result is similar to that of the IVR integration presented above when the gain of the impedance is equal to G, (Fig. 3) and G=G'.

An observation can be made by analyzing the comparative data in Table III: for a sample noise level of 2.38, a local attack scenario achieves a reduction ratio of 1/22.5 with noise injection only [4], and a remote attack scenario, assuming G'= 0.5 (equal impedance between the AES path and the noise injection path), achieves a correlation coefficient reduction of 1/1.6. Stretching the impedance gain ratio to 1 improves this reduction to 1/2.6. In the next chapter, the practical experiments of this research focus on analyzing the impact of such a reduction on the minimum number of traces required to discover the secret key in a remote attack scenario.

C. Effect of on-package decoupling capacitors as side channel attack countermeasures

This section studies the impact that the integration of on-package decoupling capacitors (OPDs) has on the success of power SCAs for local attacks (onboard trace capture) and remote attacks (on-die trace capture). OPDs are incorporated into system designs to reduce the voltage droop from high-frequency switching activities.

Fig. 5 illustrates OPDs on a package soldered on a motherboard with an onboard voltage regulator. The transient response to a step load is illustrated for measurements made at the power grid and the board voltage regulator decoupling capacitors. The

TABLE III

COMPARISON OF CORRELATION FACTOR REDUCTION BETWEEN NOISE INJECTION AND LOCAL ATTACK AGAINST NOISE INJECTION WITH REMOTE ATTACK

	Noise Addition Only, local attack [4]			**Noise Addition w/Attenuated Signature, local attack [4]**			**Noise addition and remote attack, G'=0.5**				**Noise addition and remote attack, G'=1**			
Relative noise power	0.317	2.38	3.7	0.006	0.013	0.053	0.1	1	2.38	3.7	0.1	1	2.38	3.7
Reduction ratio	1/4.5	1/22.5	<1/36	1/7.5	1/12	<1/45	1	1/1.1	1/1.6	1/2.1	1/1	1/1.4	1/2.6	1/3.8

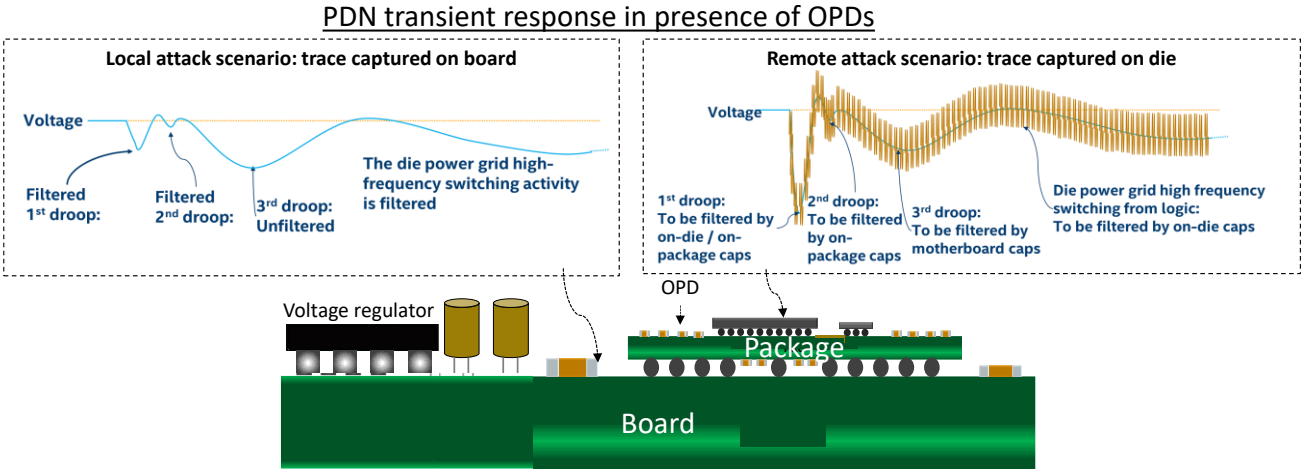


Fig. 5: On-board and on-die traces of system PDN transient response.

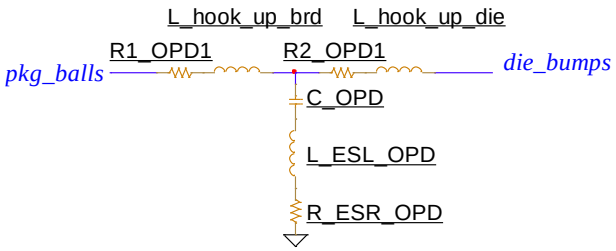


Fig. 6: Equivalent circuit modeling of the OPD with hook-up impedances.

transient response of the PDN is divided into four parts. The 1st droop is the initial response to the current step provided by the on-die decoupling capacitors and sometimes the OPDs because of their low impedance path to the die. The frequency range is typically in the 10s or 100s of MHz. The 2nd droop is the response provided by the OPDs after the charge from the on-die caps has been depleted. The 2nd droop frequency is in the single digit MHz range. Similarly, once the OPD charge is depleted, the onboard regulator capacitors kick in, which creates the 3rd droop [44]. Here, the frequency ranges from KHz to single digit MHz. The high-frequency noise riding on the average waveform is from the logic switching activities. Its frequency ranges from 100 s MHz to multiple GHz.

The system model of on-package decoupling capacitors integration is similar to that of Fig. 4, with the noise source removed and the impedance Z_{aes} replaced with the capacitor equivalent circuit of Fig. 6. The correlation coefficients in a remote attack scenario are defined by:

$$\rho_{V_1 H} = \frac{cov(V_1,H)}{\sigma_{V_1}\sigma_H} = \frac{cov\left(\frac{V_1'}{G_{OPD}},H\right)}{\frac{\sigma_{V_1'}}{G_{OPD}}\sigma_H} = \rho_{V_1' H} \qquad 16$$

With:

$$V_1' = G_{OPD} V_1$$

and G_{OPD} is the gain of the OPD circuit in Fig. 6.

It is derived from the analysis that the linear effect of decoupling filtering has no impact on the correlation coefficients and thus the power side-channel resistance. This is because filtered versions of the 1st and 2nd droop are propagated to the board level and are thus captured by the malicious agent in a local attack scenario. Furthermore, the 3rd droop signal that is seen at the board level by the malicious agent has a magnitude independent of the OPD scheme. Thus, the 3rd droop magnitude is the main carrier of sensitive distinguishing information in a local attack scenario.

V. Experimental Assessment of the Impact of Remote Attacks, Noise Injection and Decoupling Capacitors on Power Side-Channel Attacks Success

The experiments to ascertain the impact of a remote attack on the correlation coefficients are carried out in three steps: (i) generating the current profile of an AES algorithm; this is performed by measuring the current of an Artix 7 FPGA while running an AES256 algorithm implemented with the ChipWhisperer side channel attack environment; (ii) applying the current profile to a generic FPGA platform SPICE model, then running simulations with target victim and malicious agent models attached to the FPGA die; (iii) CPA run, then computing the correlation coefficients for local attacks and remote attack scenarios.

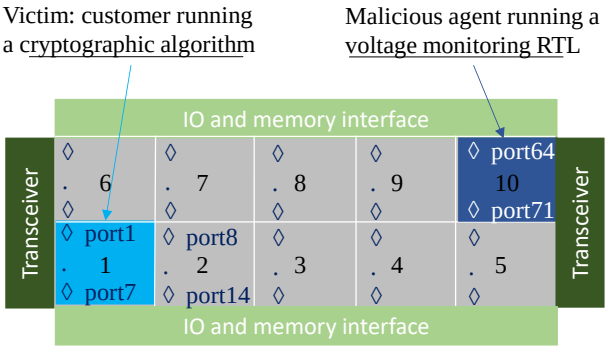


Fig. 7: Representative floorplan of the FPGA partition with two independent applications

A. FPGA remote attack modeling framework

In a remote attack scenario, a malicious agent remotely uploads its trojan program into the FPGA to attempt to monitor the IC power grid voltage. The ability of the on-die silicon power grid to act as a filter for a high-frequency signal crossing over from the victim's location to the attacker's trojan logic location determines how successful the malicious agent will be in guessing the victim's secret information.

Fig. 7 highlights the silicon layout of an FPGA used in datacenter cloud applications, modeled based on the FPGA architecture shared in [45]. The FPGA is divided into its core, a 2x5 sector array, two transceivers, and two IO and embedded external memory interfaces (EMIFs). The malicious agent logic and the victim logic are physically placed as far away as possible around sectors 10 and 1, respectively.

B. Power delivery network modeling

The device PDN modeling consists of three parts: the die+metal-insulator-metal (MiM) capacitors, the package substrate, and the voltage regulator. The die, on-chip MiM, and package substrate are extracted as a distributed model with 71 ports each. The equivalent circuit model of the FPGA on-chip MiM is represented by the simplified RC model, derived from the equivalent model of [46] but with the parasitic elements (the series inductance L_s and the oxide capacitance C_{ox}) neglected. For each distributed port x (x=1,2,…,71), the MiM capacitor is thus represented with $R_{mimx}/C_{mimx,}$ as shown in Fig. 8. The vertical contact to other layers is represented by the resistance R_{vert}. Similar to the MiM, the die is extracted as an RC model, as shown in the figure. Table IV summarizes the values of the components, which are also included in the SPICE models.

Each sector of the FPGA and the corresponding power grid is distributed into seven ports. The traces are probed in the SPICE model at the load locations to illustrate the attacker's remote sensing of the victim's actual voltage. For the local attack scenario, the voltage is measured on the PCB, which corresponds to where the adversary measures the voltage when they have physical access to the device.

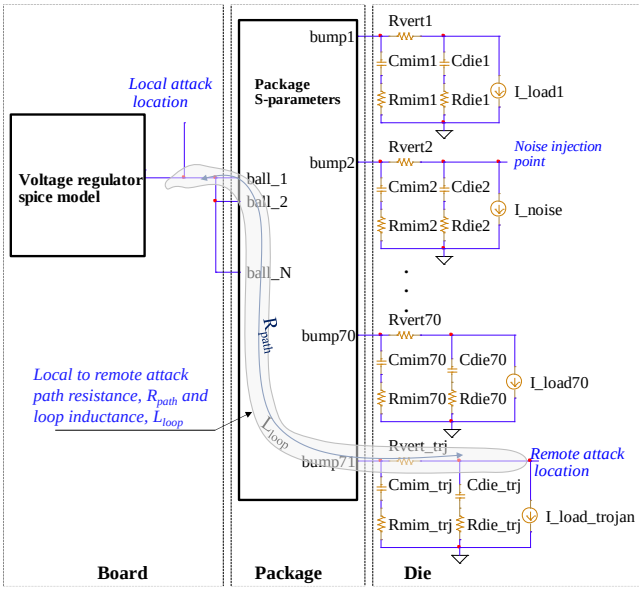


Fig. 8: Distributed PDN modeling of local and remote side channel attack

TABLE IV
DIE AND MIM CAPS SPICE MODEL PARAMETERS

	C_{min}	R_{min}	C_{die}	R_{die}	R_{vert}
Value	5.2nF	142mΩ	35.3nF	3.6mΩ	0.003mΩ

C. Simulation setup

In practical applications, the malicious agent implements trojan logic such as a ring oscillator or a time-to-digital converter in the vicinity of the victim's logic to measure the voltage that serves as a trace for the differential power analysis. However, the effectiveness of such a circuit depends on the algorithm topology and the accuracy of the instrumentation portion of the circuit. We removed this complexity from the scope of this research and instead measured the voltages directly at the FPGA power grid and package balls in the SPICE simulations.

As shown in Fig. 9, the side channel attack (AES current capture on Artix 7 and correlation coefficient computations) on the FPGA is carried out in the ChipWhisperer environment [47]. The environment provides certain APIs for random plaintexts and random key generation. The traces captured during the AES256 core encryption are passed to the Hspice simulator via text files. The Hspice simulator is embedded within the time domain traces capture subblock and invoked within the Python notebook framework. The simulator is invoked in a loop for each trace captured. The outputs of the simulator are the traces captured at various locations: at the die bumps closest to the malicious agent trojan logic (remote attack scenario) and at the board level (local attack scenario). The correlation power analysis (CPA) and the computation of the correlation coefficients are carried out according to methods and principles developed in [48][49]. The attack on the AES256 algorithm is performed in the last round using the side channel attack leak functions and the corresponding Hamming distance shared in [49].

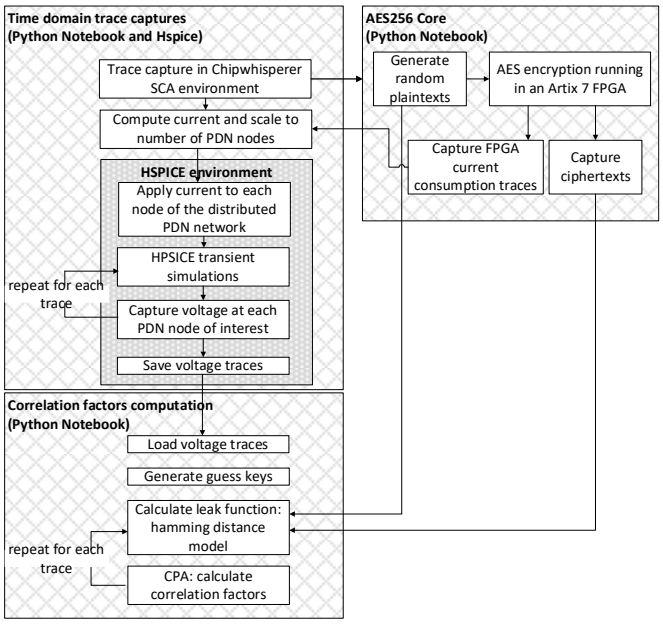


Fig. 9: Remote power side-channel attack experiment framework

D. *Local* vs. *remote attack simulation results*

The nature of FPGAs provides malicious agents opportunities to remotely configure or reconfigure a portion of the fabric with a trojan IP that serves as a telemetry agent, monitoring the IC power grid voltage fluctuations in its vicinity.

The path between the power grid and the physical onboard attack point is characterized by the package's physical dimensions and the substrate stack-up. These physical characteristics present a loop inductance between the Si power grid and the onboard measurement location. In addition, the package substrate stack-up composition, such as the number of CU layers and the CU layer thicknesses, defines the path resistance. The impedance parameters of various package sizes and stack-up compositions were extracted, and each of them was characterized by loop inductance and path resistance. For the same resistance packages (R_{path} = 0.5 mΩ), a remotely carried attack requires only 25 traces to discover the secret encryption key, whereas 36, 46, 38, 45, and 82 traces are required for loop inductances L_{loop} of 0.5 nH, 1.0 nH, 1.5 nH, 2.0 nH, and 2.5 nH, respectively. However, the package resistance has little effect on the MTD, as shown in Fig. 10.

The experiment carried out reveals that at constant loop inductance, package resistance does not impact the MTD, but the MTD increases with the inductance (irrespective of resistance), as shown in Fig. 11. Hence, with larger packages (higher loop inductance), it takes more captures to uncover the secret key, as evidenced by the surface tilted upward on the inductance axis. In summary, the extra PDN impedance between the IC power grid and the external local attack measurement point acts as a countermeasure against local power SCA. Thus, remote attacks are more effective than local attacks, assuming that the attacker can maximize the trojan IP telemetry accuracy.

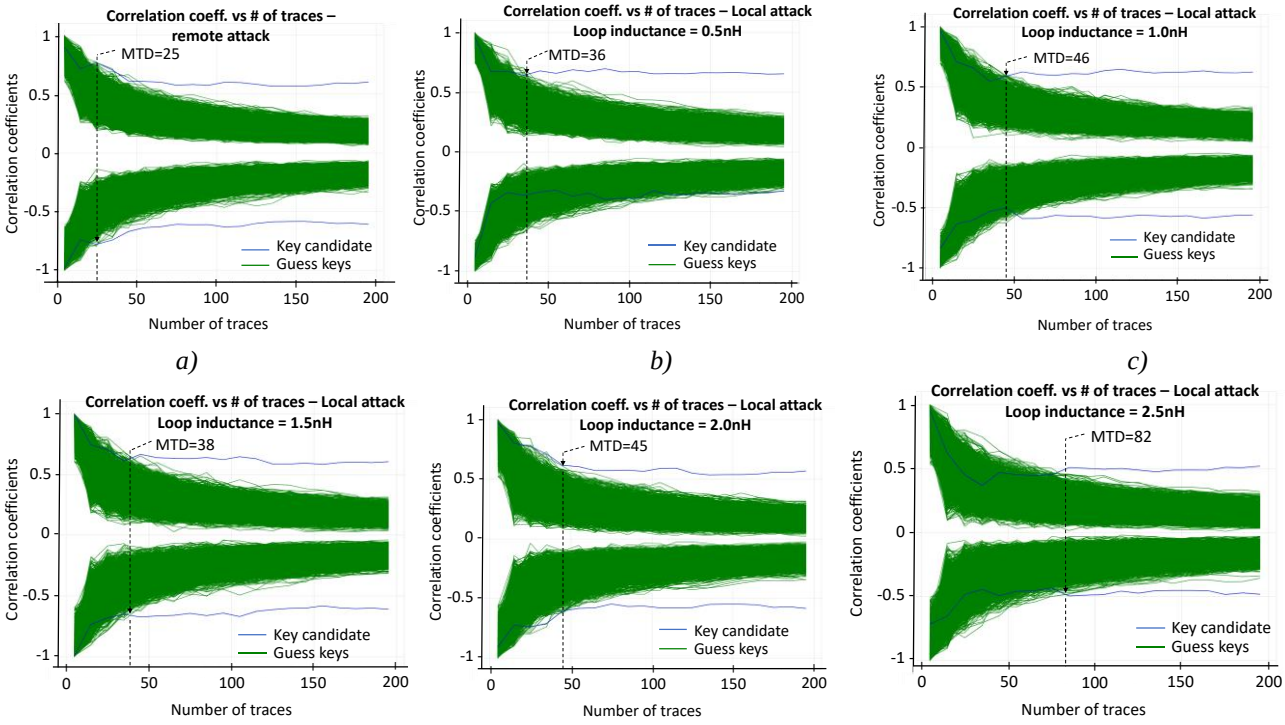


Fig. 10: Impact of package inductance on local attack success. Constant resistance R_{path}=0.5m: a)–Remote attack; Local attack with various package loop inductances: b)–L_{loop}=0.5n; c)–L_{loop}=1.0n; d) – L_{loop}=1.5n; e)–L_{loop}=2.0n; f)–L_{loop}=2.5n.

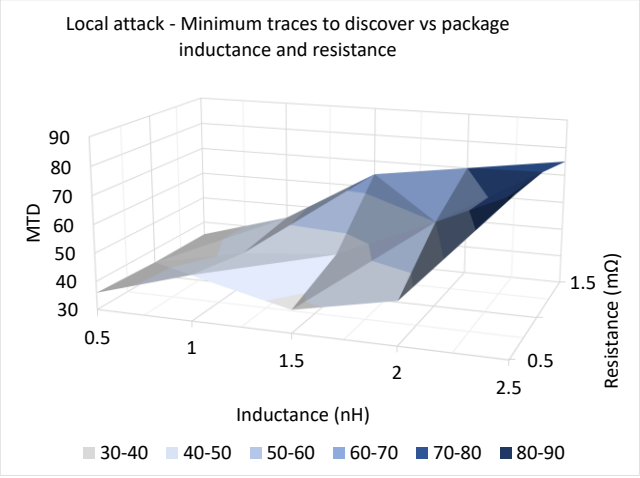


Fig. 11: MTD vs. package impedance in a local attack.

E. Impact of PDN noise injection on the power side-channel attack success rate

For power SCA experiments, the signal-to-noise ratio (SNR) is introduced as [50][51]:

$$SNR = \frac{\sigma_{trace}}{\sigma_{noise}} \qquad 17$$

where σ_{trace} and σ_{noise} represent the standard deviation of the IC power consumption and the injected noise, respectively.

Noise is injected into the system at the injection point shown in Fig. 9. In practical applications, voltage traces are a collection of signals from various IPs running concurrently with the victim IP. Hence, for real-life applications with multiple IPs, the traces from other IPs constitute the noise that provides SCA countermeasures.

To quantify the impact of a noise source on SCA success, a Gaussian noise source is injected into the extracted model. Then, the simulation is run, and the measurements taken at the C4 bumps closest to the attacker trojan IP emulate a remote attack. A statistical analysis (CPA) is then performed to compute the correlation coefficients and the MTD for various SNR levels. Based on the results of the previous section, attacks carried out remotely are far more effective than local attacks; thus, it is predicted that with noise injected into the PDN network, a local attack will still require more traces to uncover the secret key.

The MTD for the baseline without noise injection is computed and plotted for five SNR levels: 10, 5, 3, 2, and 1 (Fig. 12). Note from the figure that the MTD increases gradually as we go from no noise to noise injection of SNR = 10 and 5. Then, there is an exponential increase as the SNR decreases from 5 to 1. We could not mount a successful attack with 1,000 traces when the SNR is equal to 1.

Fig. 13 summarizes the impact of the noise injection by plotting the maximum correlation coefficients, the experimental and theoretical correlation coefficient reduction ratio, and the MTD versus the noise relative magnitude (which is the inverse of the SNR). The plot also shows a linear interpolation of the MTD. The maximum correlation is attained for each trace where the estimated leak function correlates with the measurements, which is during the last round of encryption. The correlation coefficient reduction represents the ratio of the max correlation coefficients for the noise level over the baseline max coefficient

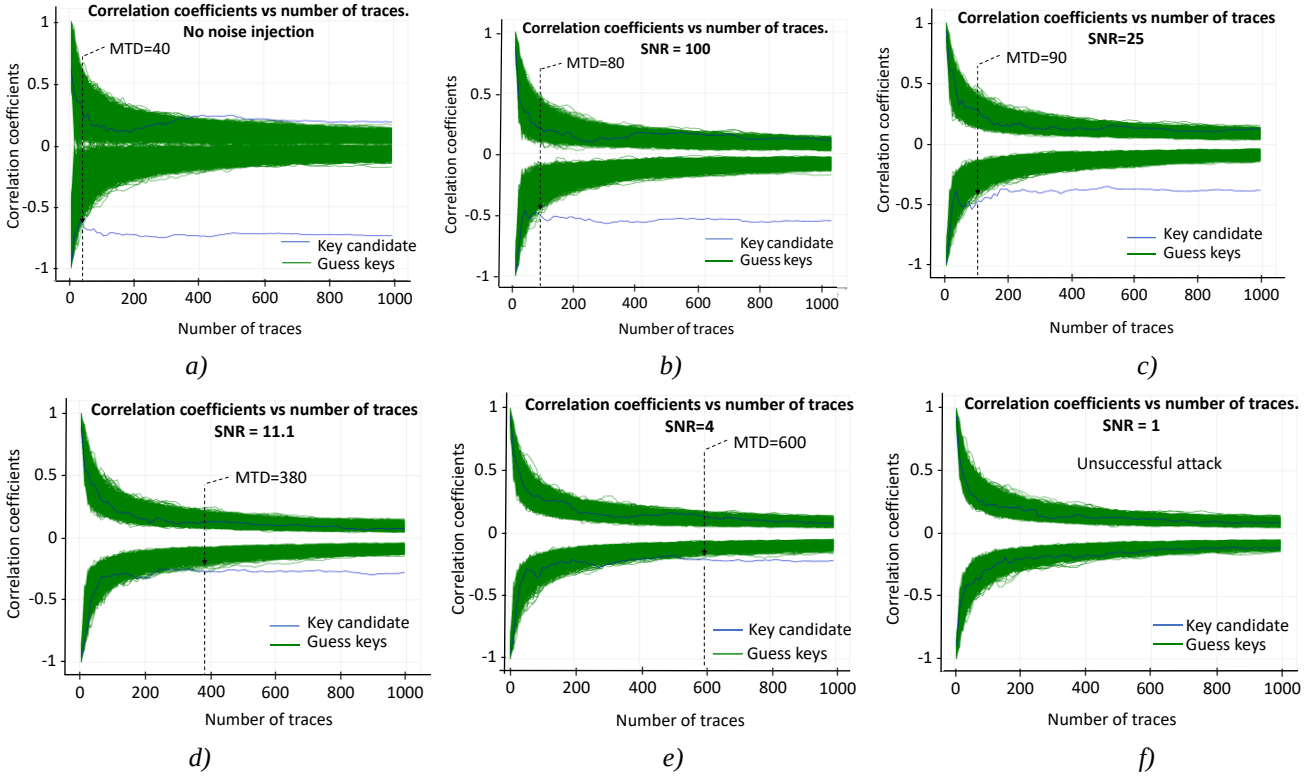


Fig. 12: MTD with and without PDN noise injection: a) – Baseline, no noise injection; b) – Noise injection: SNR=100; c) – Noise injection: SNR=25; d) – Noise injection: SNR=11.1; e) – Noise injection: SNR=4; f) – Noise injection: SNR=1.

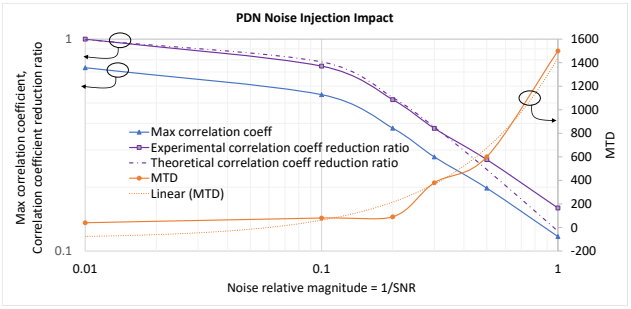


Fig. 13: Impact of noise injection on power side-channel attack success.

without noise injection. As expected, the max correlation coefficient decreases as the noise magnitude increases, as does the reduction ratio. A comparison between the theoretical reduction ratio for a system impedance with gain G=8, as defined in equation (10), shows a close match with the experimental results. Therefore, an empirical deduction is made that our system PDN network has a gain of G=8. Likewise, the MTD shows a similar trend, with a marked exponential increase above a relative noise magnitude of 0.3. In summary, the experimental results show that the presence of noise in the PDN is an effective countermeasure to power SCA.

F. Impact of on-package decoupling capacitors on side channel attack success

The OPD filters the 1st and 2nd droop signals seen at the die level. With OPDs modeled as shown in Fig. 14, simulations of the AES256 cryptosystem are run, and on-die and onboard waveforms are captured with OPD scenarios. Comparing the

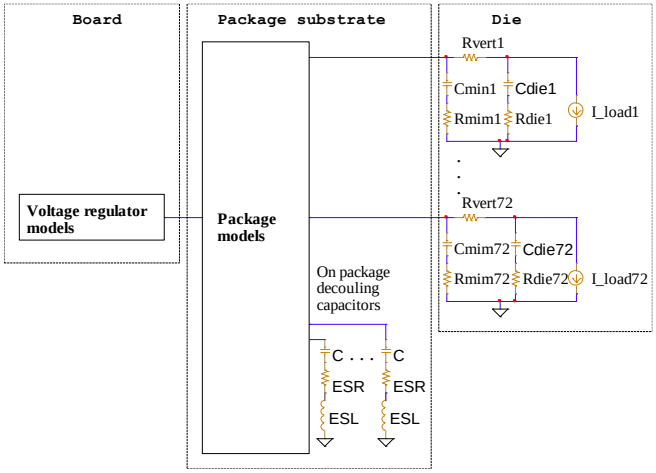


Fig. 14: System modeling with on-package decoupling capacitors

voltages with no OPD and with 20 OPDs, in Fig. 15, it is apparent that the OPDs significantly reduced the magnitude of the voltage measurement at the board level, from 14 mVpp to 1.6 mVpp (8.75x). They have also impacted the magnitude of the on-die voltage, albeit with a lower ratio, reducing it from 2 mVpp to 0.6 mVpp (3.33x).

Simulations were run with multiple settings of OPDs to gauge their impact on the success rate or the probability of an attacker uncovering the secret key while mounting either a local attack (capturing traces onboard with physical presence at the scene) or a remote attack (capturing the voltage at the die level with a trojan IP). With no OPDs, 39 and 29 traces are required

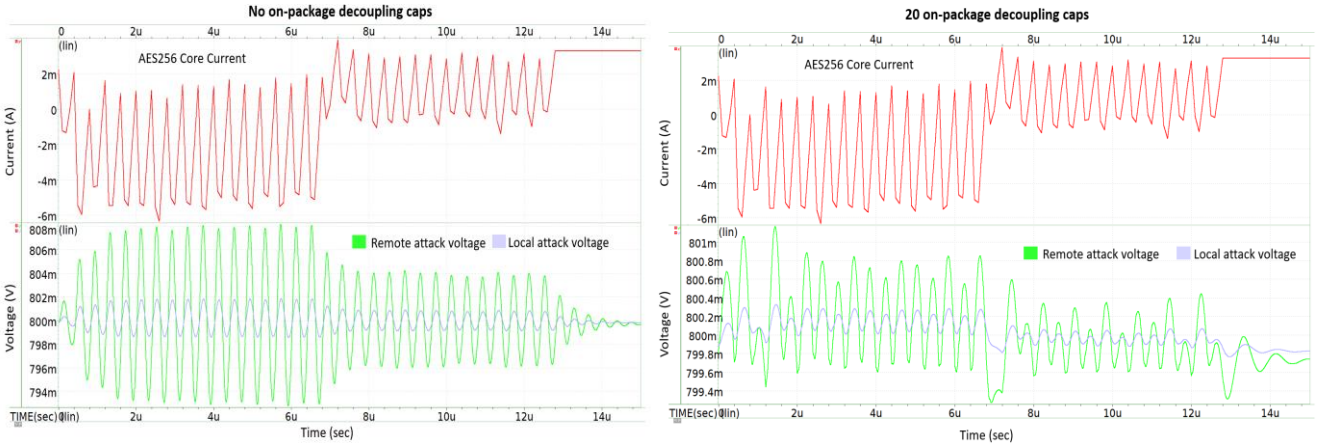
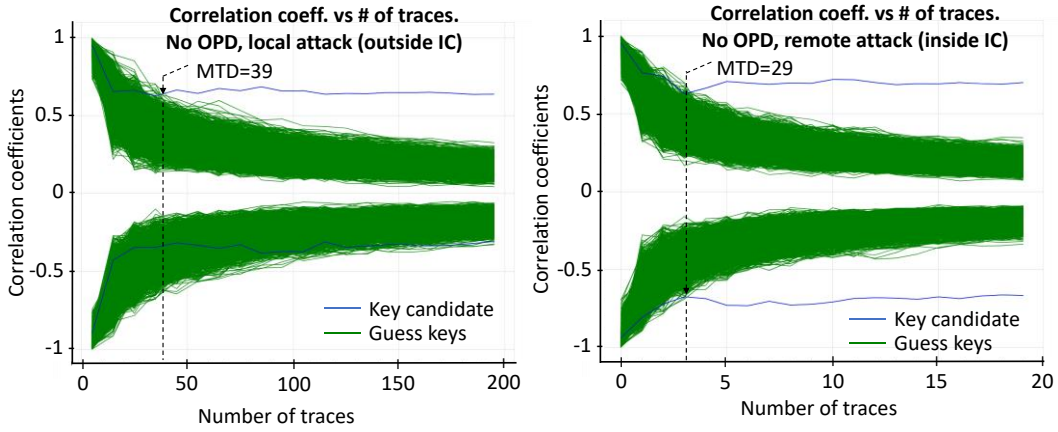


Fig. 15: Simulated waveforms of AES256 engine. Left: No OPD; trace measured at the die (green) and at the board (blue), vs. AES256 engine current (red). Right: 20 OPDs, trace measured at the die (green) and at the board (blue), vs. AES256 engine current (red).



a) *b)*

Fig. 16: Correlation coefficients vs. number of traces: MTD with no OPD for local attack (a) and remote attack (b).

to mount a successful local and remote attack, respectively. This is a reduction of 25.6% from local to remote attack scenarios (Fig. 16a, and Fig. 16b). With 5, 10, 15, 20, 30, and 40 OPDs, the MTDs for a local attack are 38, 39, 42, 48, 49, and 49, respectively, as shown in Fig. 17. Although the locally measured waveforms in the presence of OPDs show a gain attenuation, it should be observed that there is little distortion present on those waveforms compared to the waveforms without OPDs. This explains the CPA results that show only a small increase in the MTD: 39 to 48. The gain attenuation is a linear transformation that has no impact on the correlation coefficients. This is rooted in the principle of Pearson correlations, which constitute the basis for CPA [52][9]. When the estimated power accurately models the measured power, a deviation in the magnitude of the measured power, in the same direction as the no-OPD scenario, will lead to similar correlation coefficients as the no-OPD case. However, for remote attacks, the MTD remains constant at 29-30, regardless of the number of OPDs.

A summary of the impact of the OPDs on the MTD is presented in Fig. 18. The local attack MTD increases from 39 to 49 (or ~25%) from no OPD to 40 OPDs but remains constant for remote attacks.

G. Summary of PDN countermeasures experimental findings

For the practical system considered herein, the design space is defined by the acceptable values of the design parameters that can be practically implemented to keep the product viable and realistic. The range of realistic values for the number of OPDs is 0 to 40, and the max implementable package size yielded a loop inductance of 2.5 nH and path resistance of 1.5 mΩ after extraction with broadband spice. Additionally, the maximum magnitude of the noise that can be injected into the design is set to be equal to the signal magnitude, hence a relative noise magnitude of 1. Therefore, the design space is defined as the trivariate (relative noise magnitude, number of OPDs, package impedance):

Design space
- Relative noise magnitude: [0,1]
- Number of OPDs: [0,40]
- Package impedance:
  - Loop inductance: [0.5nH, 2.5nH]
  - Path resistance: [0.5mΩ, 1.5mΩ]

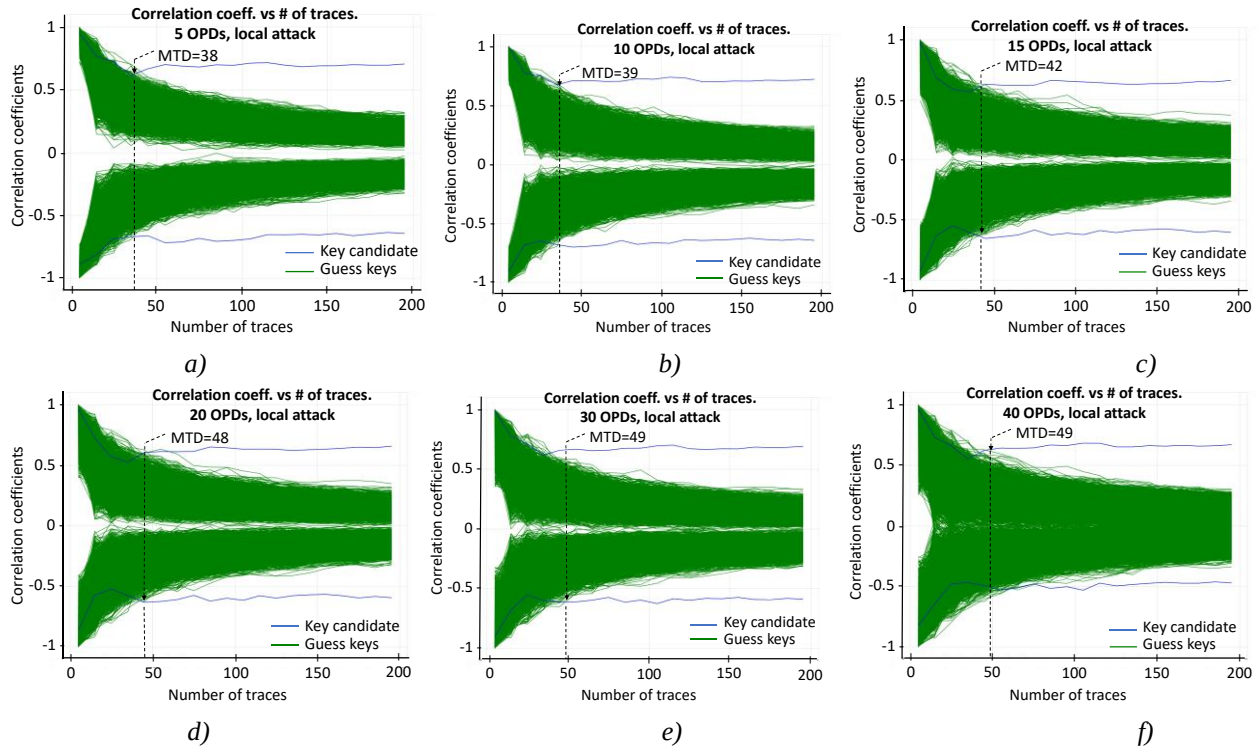


Fig. 17: Correlation vs. number traces for various OPD settings: a) – 5 OPD; b) – 10 OPDs; c) 15 OPDs; d) 20 OPDs; e) - 30 OPDs; f) - 40 OPDs.

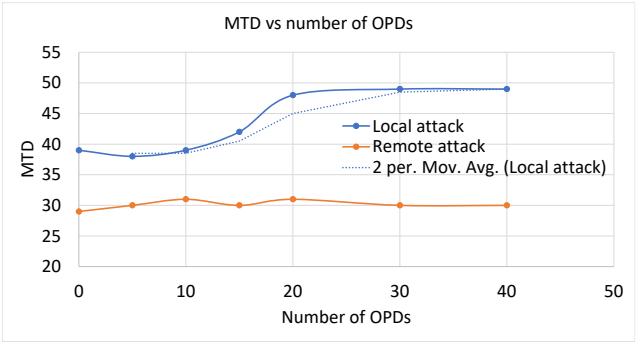


Fig. 18: MTD vs. number of OPDs.

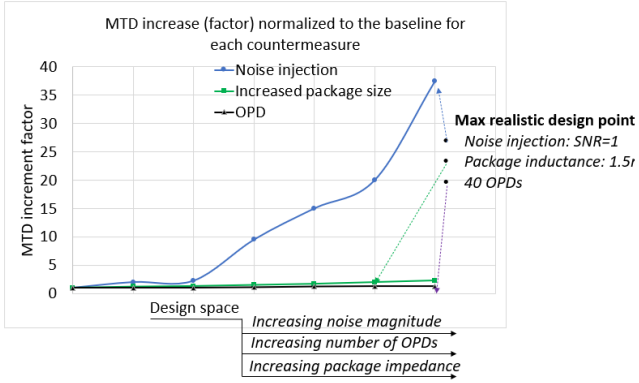


Fig. 19: Relative MTD increase compared to the baseline, for each PDN-based countermeasure

The normalized MTD versus each of the design space variables is plotted in Fig. 19. The MTD is normalized to the following minimum value for each parameter: no noise injection (noise magnitude), no OPD (number of OPDs), and 0.5 nH, 0.5 mΩ (impedance). The Y-axis shows the relative increase in MTDs, and the X-axis shows increasing design parameter values. It can be observed that in the range of practical values, OPDs and larger packages provide only 1.3x and 2.3x increases in the MTD. However, the noise injection in the PDN yields a 37x increase in the MTD. In summary, one should not rely on increasing the number of OPDs or the distance between locally measured power and die location afforded by a larger package size as efficient power SCA countermeasures. Noise injection is by far the best countermeasure mechanism.

VI. Conclusion

This paper analyzed the impact of IVR, noise injection, OPDs, and circuit impedance on the ability of a cryptographic system PDN to reduce the amount of leaked identifiable information in a remote side channel attack scheme. The prior art narrowly focused on IVR and noise injection to local attacks with a physical presence, whereas this study shows that remote attacks with traces captured at the IC power grid are significantly less impacted by IVR and OPD. The proximity and low impedance of the remote trojan IP to the victim are great security vulnerabilities, as it is shown that it requires fewer traces to uncover the secret key than a locally carried attack that captures the traces farther away on the system board. However, it was demonstrated that noise injection constitutes an effective countermeasure to remote SCA as it increases the MTD by 37x, compared to 1.3x for OPDs increase. Additionally, a local attack requires 2.3x fewer traces to discover the secret key than a remote attack. Considering circuit

loop impedance as a factor for remote vs. local attack analysis, which is a novel art, circuit impedance alterations, including IVR, are not effective at reducing the correlation between the measured traces and the encryption key.

REFERENCES

[1] W. Yu, O. A. Uzun, and S. Köse. "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks." In Proceedings of the 52nd Annual Design Automation Conference, pp. 1-6. 2015.

[2] W. Yu, and S. Köse. "Exploiting voltage regulators to enhance various power attack countermeasures." IEEE Transactions on emerging topics in Computing 6, no. 2 (2016): 244-257.

[3] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017, pp. 62-67, doi: 10.1109/HST.2017.7951799.

[4] J. Lagasse, C. Bartoli, and W. Burleson, "Combining Clock and Voltage Noise Countermeasures Against Power Side-Channel Analysis," 2019 IEEE 30th International Conference on Application-specific Systems, Architectures and Processors (ASAP), 2019, pp. 214-217, doi: 10.1109/ASAP.2019.00009.

[5] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay. "8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator." In 2017 IEEE International Solid-State Circuits Conference (ISSCC), pp. 142-143. IEEE, 2017.

[6] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay. "Improved power/EM side-channel attack resistance of 128-bit aes engines with random fast voltage dithering." IEEE Journal of Solid-State Circuits 54, no. 2 (2018): 569-583.

[7] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator," in IEEE Journal of Solid-State Circuits, vol. 53, no. 8, pp. 2399-2414, Aug. 2018, doi: 10.1109/JSSC.2018.2822691.

[8] P. Kocher, J. Jaffe, and B. Jun. "Differential power analysis." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1999.

[9] E. Brier, C. Clavier, and F. Olivier. "Correlation power analysis with a leakage model." *International workshop on cryptographic hardware and embedded systems*. Springer, Berlin, Heidelberg, 2004.

[10] FX. Standaer, F. Koeun, W. Schindler, (2009). *"How to Compare Profiled Side-Channel Attacks?"*. In: Abdalla, M., Pointcheval, D., Fouque, PA., Vergnaud, D. (eds) Applied Cryptography and Network Security. ACNS 2009. Lecture Notes in Computer Science, vol 5536. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-01957-9_30

[11] L. Lerman, R. Poussier, O. Markowitch, FX. Standaert. "*Template attacks versus machine learning revisited and the curse of dimensionality in side-channel analysis: extended version."* Journal of Cryptographic Engineering. 2018 Nov;8:301-13.

[12] S. Chari, J. R. Rao, P. Rohatgi. *"Template attacks."* In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 13-28. Springer, Berlin, Heidelberg, 2002.

[13] L. Lerman, G. Bontempi, O. Markowitch. "*Power analysis attack: an approach based on machine learning.*" International Journal of Applied Cryptography 3, no. 2 (2014): 97-115.

[14] B. Hettwer, S. Gehrer, T. Güneysu. *"Applications of machine learning techniques in side-channel attacks: a survey."* J Cryptogr Eng 10, 135–162 (2020). https://doi.org/10.1007/s13389-019-00212-8

[15] F. Hu, H. Wang, J. Wang. *"Multi-leak deep-learning side-channel analysis."* IEEE Access. 2022 Feb 18;10:22610-21.

[16] R. Benadjila, E. Prouff, R. Strullu, E. Cagli, C. Dumas . *"Deep learning for side-channel analysis and introduction to ASCAD database."* Journal of Cryptographic Engineering. 2020 Jun;10(2):163-88.

[17] G. Zaid, L. Bossuet, F. Dassance, A. Habrard, A. Venelli. *"Ranking loss: Maximizing the success rate in deep learning side-channel analysis."* IACR Transactions on Cryptographic Hardware and Embedded Systems. 2021:25-55.

[18] T. Kubota, K. Yoshida, M. Shiozaki, T. Fujino. *"Deep learning side-channel attack against hardware implementations of AES."* Microprocessors and Microsystems. 2021 Nov 1;87:103383.

[19] B. Timon. *"Non-profiled deep learning-based side-channel attacks with sensitivity analysis."* IACR Transactions on Cryptographic Hardware and Embedded Systems. 2019 Feb 28:107-31.

[20] L. Wu, G. Perin, and S. Picek, "*The Best of Two Worlds: Deep Learning-assisted Template Attack*", *TCHES*, vol. 2022, no. 3, pp. 413–437, Jun. 2022.

[21] H. Maghrebi. *"Deep Learning based Side Channel Attacks in Practice."* IACR Cryptol. ePrint Arch. 2019 (2019): 578

[22] M. Taouil, A. Aljuffri and S. Hamdioui, *"Power Side Channel Attacks: Where Are We Standing?,"* 2021 16th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS), 2021, pp. 1-6, doi: 10.1109/DTIS53253.2021.9505075.

[23] G. Hospodar, B. Gierlichs, E. D. Mulder, I. Verbauwhede, and J. Vandewalle. *"Machine learning in side-channel analysis: a first study."* Journal of Cryptographic Engineering 1, no. 4 (2011): 293.

[24] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard. "Systematic classification of side-channel attacks: A case study for mobile devices." *IEEE Communications Surveys & Tutorials* 20, no. 1 (2017): 465-488.

[25] https://www.hpcwire.com/2019/08/19/ayar-labs-to-demo-photonics-chiplet-in-fpga-package-at-hot-chips/

[26] https://blogs.intel.com/psg/intel-releases-royalty-free-high-performance-aib-interconnect-standard-to-spur-industrys-chiplet-adoption-and-grow-the-ecosystem/

[27] M. Zhao, and G. E. Suh. "FPGA-based remote power side-channel attacks." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.

[28] R. Lumbiarres-Lopez, M. López-García, and E. Canto-Navarro. "Hardware architecture implemented on FPGA for protecting cryptographic keys against side-channel attacks." IEEE Transactions on Dependable and Secure Computing 15, no. 5 (2016): 898-905.

[29] Y. Niu, J. Zhang, A. Wang and C. Chen, "An Efficient Collision Power Attack on AES Encryption in Edge Computing," *in IEEE Access*, vol. 7, pp. 18734-18748, 2019, doi: 10.1109/ACCESS.2019.2896256.

[30] A. Moradi, D. Oswald, C. Paar, and P. Swierczynski. "Side-channel attacks on the bitstream encryption mechanism of Altera Stratix II: facilitating black-box analysis using software reverse-engineering." In *Proceedings of the ACM/SIGDA international symposium on Field programmable gate arrays*, pp. 91-100. 2013.

[31] D. Mahmoud, and M. Stojilović. "Timing violation induced faults in multi-tenant FPGAs." In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1745-1750. IEEE, 2019.

[32] N. Pramstaller, E. Oswald, S. Mangard, F. K. Gürkaynak, and S. Häne. A Masked AES ASIC Implementation. na, 2004.

[33] R. Lumbiarres-López, M. López-García and E. Cantó-Navarro, "Hardware Architecture Implemented on FPGA for Protecting Cryptographic Keys against Side-Channel Attacks," *in IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 898-905, 1 Sept.-Oct. 2018, doi: 10.1109/TDSC.2016.2610966.

[34] W. Diehl, A. Abdulgadir, J. P. Kaps, and K. Gaj. "Comparing the cost of protecting selected lightweight block ciphers against differential power analysis in low-cost FPGAs." *Computers 7*, no. 2 (2018): 28.

[35] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2017, pp. 62-67, doi: 10.1109/HST.2017.7951799.

[36] S. Kotipalli, Y.B. Kim, and M. Choi. "Asynchronous advanced encryption standard hardware with random noise injection for improved side-channel attack resistance." *Journal of Electrical and Computer Engineering* 2014 (2014).

[37] M. Zhao and G. E. Suh, "FPGA-Based Remote Power Side-Channel Attacks," *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 229-244, doi: 10.1109/SP.2018.00049.

[38] R. Selvam and A. Tyagi, "Power Distribution Network Capacitive Decoupling for Side-Channel Resistance," 2021 IEEE International Symposium on Smart Electronic Systems (iSES), Jaipur, India, 2021, pp. 183-188, doi: 10.1109/iSES52644.2021.00051.

[39] A. Gornik, A. Moradi, J. Oehm and C. Paar, "A Hardware-Based Countermeasure to Reduce Side-Channel Leakage: Design, Implementation, and Evaluation," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 8, pp. 1308-1319, Aug. 2015, doi: 10.1109/TCAD.2015.2423274.

[40] M. Mayhew and R. Muresan, "On-Chip Nanoscale Capacitor Decoupling Architectures for Hardware Security," in IEEE Transactions on Emerging Topics in Computing, vol. 2, no. 1, pp. 4-15, March 2014, doi: 10.1109/TETC.2014.2303934.

[41] S. Seçkiner, and S. Köse. "Security Implications of Decoupling Capacitors on Leakage Reduction in Hardware Masking." In 2023 IEEE 14th Latin America Symposium on Circuits and Systems (LASCAS), pp. 1-4. IEEE, 2023.

[42] T. Nakai, M. Shiozaki, T. Kubota, and T. Fujino. "Evaluation of on-chip decoupling capacitor's effect on AES cryptographic circuit." Synthesis And System Integration of Mixed Information Technologies 13 (2013).

[43] K. Zick, Kenneth M., M. Srivastav, W. Zhang, and M. French. "Sensing nanosecond-scale voltage attacks and natural transients in FPGAs." In Proceedings of the ACM/SIGDA international symposium on Field programmable gate arrays, pp. 101-104. 2013

[44] P. Pant and J. Zelman, "Understanding Power Supply Droop during At-Speed Scan Testing," 2009 27th IEEE VLSI Test Symposium, 2009, pp. 227-232, doi: 10.1109/VTS.2009.46.

[45] J. Chromczak, M. Wheeler, C. Chiasson, D. How, M. Langhammer, T. Vanderhoek, G. Zgheib, and I. Ganusov. "Architectural enhancements in intel® agilex™ fpgas." In Proceedings of the 2020 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays, pp. 140-149. 2020.

[46] S. S. Song, S. W. Lee, J. Gil, and H. Shin. "Simple wide-band metal-insulator-metal (MIM) capacitor model for RF applications and effect of substrate grounded shields." Japanese journal of applied physics 43, no. 4S (2004): 1746.

[47] NewAE Technology Inc, ChipWhisperer® by, https://wiki.newae.com/Main_Page

[48] E. Brier, C. Clavier, and F. Olivier. "Correlation power analysis with a leakage model." *International workshop on cryptographic hardware and embedded systems*. Springer, Berlin, Heidelberg, 2004.

[49] A. T. Mozipo and J. M. Acken, "Power Side Channel Attack of AES FPGA Implementation with Experimental Results using Full Keys," 2021 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS), 2021, pp. 1-6, doi: 10.1109/DTS52014.2021.9497976.

[50] D. Mahmoud, and M. Stojilović. "Timing violation induced faults in multi-tenant FPGAs." In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1745-1750. IEEE, 2019.

[51] S. Guilley, H. Maghrebi, Y. Souissi, L. Sauvage, and J. L. Danger. "Quantifying the quality of side channel acquisitions." COSADE, February (2011).

[52] E. Brier, C. Clavier, and F. Olivier. "Optimal Statistical Power Analysis." IACR Cryptology ePrint Archive 2003 (2003): 152.

Aurelien T. Mozipo holds a master's in engineering from Polytechnic Institute of Yaounde, Cameroon, and an MSEE from the University of Quebec at Trois Rivieres, Canada, with a concentration in microelectronics and digital signal processing. He has over 20 years of industry experience in power electronics and architecture of FPGA-based SmartNICs. His interests include FPGA power architecture, FPGA power security, side channel attack countermeasures, and power/performance optimizations. He is currently with Intel and Portland State University. Prior to joining Intel, he worked at Delphi Automotive, where he designed DCDC converters.

John M. Acken is a faculty member in the Electrical and Computer Engineering Department, Portland State University, Portland, OR. He received his BS and MS in electrical engineering from Oklahoma State University and his PhD in electrical engineering from Stanford University. Dr. Acken's primary research areas include hardware for information security, digital system testing, and VLSI design. Currently, his primary research is distributed trust models for the energy grid, and his research projects include technology and devices for information security and identity authentication. Dr. Acken taught at Santa Clara University, Oklahoma State University, and PSU. He has been on PhD. Committees at UC Santa Cruz, Carnegie Mellon University, Syracuse University, Oklahoma State University, and PSU. He is a coinventor on a patent titled "Conditional Access and Content Security Method", US Patent Number 6,069,647, granted 30 May 2000. He has worked as an electrical engineer and manager at several companies, including the US Army, Sandia National Labs in Albuquerque, New Mexico and Intel in Santa Clara, CA, Valid logic Systems in Santa Clara, CA, and Crosscheck Technology in San Jose, CA. During his time in the US Army, he was in the Army Security Agency, which was the Army Branch of NSA during the Vietnam War. He is a member of IEEE, Eta Kappa Nu, and Tau Beta Pi.