Reducing a Masked Implementation's Effective Security Order with Setup Manipulations

And an Explanation Based on Externally-Amplified Couplings

Itamar Levi, Davide Bellizia and François-Xavier Standaert

Université catholique de Louvain, ICTEAM/ELEN/Crypto Group, Belgium
{itamar.levi,davide.bellizia,fstandae}@uclouvain.be

Abstract. Couplings are a type of physical default that can violate the independence assumption needed for the secure implementation of the masking countermeasure. Two recent works by De Cnudde et al. put forward qualitatively that couplings can cause information leakages of lower order than theoretically expected. However, the (quantitative) amplitude of these lower-order leakages (e.g., measured as the amplitude of a detection metric such as Welch's T statistic) was usually lower than the one of the (theoretically expected) d^{th} order leakages. So the actual security level of these implementations remained unaffected. In addition, in order to make the couplings visible, the authors sometimes needed to amplify them internally (*e.g.*, by tweaking the placement and routing or iterating linear operations on the shares). In this paper, we first show that the amplitude of low-order leakages in masked implementations can be amplified externally, by tweaking side-channel measurement setups in a way that is under control of a power analysis adversary. Our experiments put forward that the "effective security order" of both hardware (FPGA) and software (ARM-32) implementations can be reduced, leading to concrete reductions of their security level. For this purpose, we move from the detection-based analyzes of previous works to attack-based evaluations, allowing to confirm the exploitability of the lower-order leakages that we amplify. We also provide a tentative explanation for these effects based on couplings, and describe a model that can be used to predict them in function of the measurement setup's external resistor and implementation's supply voltage. We posit that the effective security orders observed are mainly due to "externally-amplified couplings" that can be systematically exploited by actual adversaries.

Keywords: Masking · Side-Channel Analysis · Security Order · Couplings

Introduction

Masking is a theoretically well understood countermeasure against Side-Channel Attacks. It works by splitting any sensitive variable of an implementation into d shares, and performing the computations on those shares only. Under the assumption that the leakages produced during the manipulation of the shares depend on at most one share each or can be written as a linear function of these shares, which is frequently referred to as masking's *independence assumption*, it amplifies the noise in the leakages, and therefore the implementation security. In essence, this amplification is obtained by forcing the adversary to estimate a higher-order statistical moment of the leakage distribution: a task of which the data complexity grows exponentially in the number of shares [CJRR99, PR13, DFS15]. The lowest key-dependent moment of the leakage distribution is usually denoted as the (statistical) *security order*.

Concretely though, it is well known that implementing masking schemes in a way that fulfills this independence assumption is non-trivial. For example, it has been shown that

IACR Transactions on Cryptographic Hardware and Embedded Systems ISSN 2569-2925, Vol. 2019, No. 2, pp. 293–317
DOI:10.13154/tches.v2019.i2.293-317

glitches in hardware implementations can re-combine the leakages of several shares in a non-linear manner, therefore reducing the security order [MPG05]. A similar re-combination can happen in the case of software implementations due to memory transitions [CGP+12]. Yet, it has also been shown that such physical defaults can be kept under control at design (synthesis) time. For example, Threshold Implementations (TIs) prevent glitches thanks to a property of non-completeness [NRS11] (which requires excluding one share from the computation of any combinatorial logic circuit in the implementation), and transition-based leakages can be simply mitigated by doubling the number of shares in an implementation [BGG+14]. This group of hazards is denoted in this manuscript as *logical* recombinations, since they can be formulated as logical conditions which can then be verified and prevented [FGP+18].

In this work, we are concerned with yet another physical default, next denoted as *couplings*, which was recently reported by De Cnudde *et al.*, [CBG+17, CEM18]. In summary, these works show that even when implemented correctly (*i.e.*, in a way that prevents glitches and transitions), masking can suffer from (non-linear) shares re-combinations due to the physical proximity of the shares, with contrasted conclusions.

On the one hand, such re-combinations are worrying since they highly depend on the implementation technology and on the placement and routing, which happen late in the design of a masked implementation, correspond to a lower abstraction level, and are therefore more difficult to model than logical recombinations.

On the other hand, the couplings' re-combinations experimentally exhibited so far were not yet critical for two reasons. First, despite De Cnudde *et al.* demonstrated the presence of information leakages of lower order than the theoretically expected d qualitatively, the (quantitative) amplitude of these lower-order leakages was usually lower than the one of the d^{th} order leakages [CBG+17][1], and were only put forward based on detection tests, leaving the concrete exploitability of these leakages as an open question. Second, in order to make these effects visible, the authors sometimes needed to amplify them internally (*e.g.*, by tweaking the placement and routing or by iterating several linear operations on the shares to increase their contribution to the global power consumption measured by the adversary [CEM18] – while a designer would naturally work in the opposite direction).

In this paper, we pick up some of the challenges initiated by De Cnudde *et al.* and contribute to the issue of shares' recombinations due to setup manipulations and couplings in masked implementations in two main directions.

Our first contribution is to demonstrate experimentally that the amplitude of low-order leakages in masked implementations can be amplified thanks to external manipulations of a power analysis adversary's measurement setup (*e.g.*, the setup's external resistor and implementation's power supply), and reduce its concrete security level for reasonable noise levels (*i.e.,* as typically observed in our setups). Formally, the previous works by De Cnudde exhibited reductions of the security order for such implementations. We extend these results by exhibiting reductions of the *effective security order*, defined as the order of the statistical moment that can be exploited with the smallest number of measurements (which, as per footnote 1, depends on the noise level). For this purpose, we provide experimental results of both a hardware (FPGA) case study based on Domain-Oriented Masking (DOM) [GMK17], and a software (ARM-32) case study based on Barthe *et al.*'s parallel masking scheme [BDF+17]. We also move from the detection-based analyzes of previous works to attack-based evaluations, allowing to confirm the exploitability of the lower-order leakages that we amplify. We use Moradi & Standaert's Moments-Correlation

[1] Concretely, the latter is already problematic though. What it shows is only that for the noise levels considered in the author's target implementations, couplings did not reduce the concrete security level, for example in terms of the number of measurements to disclose the key. But as discussed in [DFS15], Section 4.2, it remains that when increasing the noise (which could typically be done to increase security), lower-order leakages will gradually get closer to d^{th}-order leakages, and become critical at some point.

Profiled DPA (MCP-DPA) to this end, as it allows obtaining simple intuitions about the exploitability of the statistical moments of a leakage distribution [MS16].

Our second contribution is to provide a tentative explanation of these effects based on *externally-amplified couplings*. For this purpose, we provide a model that illustrates how tweaking a side-channel measurement setup in a way that is under control of a power analysis adversary (*e.g.*, by manipulating the setup's external resistor and implementation's power supply, as in our experiments) can lead to significant amplifications of low-order leakages due to couplings. We describe the physical effects which (we assume) are the cause of this external amplification, and confirm that our model is reasonably predictive of our experimental results. As a consequence, we posit that externally-amplified couplings can be systematically exploited by actual adversaries, and therefore are an important risk to consider in side-channel security evaluations.

We conclude the paper by discussing its impact, open problems regarding the generalization of our conclusions to masking schemes with more shares, and possible countermeasures to be investigated in the future.

Cautionary remarks. We note that the physical effects we put forward in this paper could be anticipated from previous works. For example, modifying the measurement setup's external resistor and the supply voltage was already done in [CEM18], but with more limited ranges for these parameters (and not to the point of reducing the effective security order).[2] So our contribution in this respect is to show that these external factors are as (if not more) important for the exploitability of low-order leakages as internal ones (*e.g.*, related to the placement and routing of masked designs).

We also note that even though it is a known fact that the quality of measurement setups may greatly affect the conclusions of a security evaluation, the common understanding is that it mostly plays a role regarding the noise level of the leakages [PS17]. Our results show that it can equally affect the (effective) security order, which may have far more damaging consequences (since potentially reducing the concrete security level by an exponential factor corresponding to the noise level raised to the reduction of the order). In view of the difficulty to accurately model the physical effects observed, these results imply a need of security margins in the expected security orders of masked implementations – the evaluation of which is an important scope for further research.

Paper organization. For readability, we present our contributions starting with our model and an intuitive description of the externally-amplified couplings which we assume are the cause of our results (in Section 2). This provides us with a basis to discuss the experiments of Section 3, where we evaluate externally-amplified reductions of the effective security order for a Domain-Oriented-Masking architecture implemented on an FPGA, and the ones of Section 4, where we evaluate them for the bit-wise parallel masking scheme of Barthe *et al.* (ARM 32-bit software implementation). These sections are complemented with background information on the designs we evaluate, our measurement setups and the tools used in this manuscript in Section 1, and a conclusion in Section 5.

1 Background

In this section, we recall the masking schemes and tools needed for the understanding of our following results. We start with a brief reminder of DOM and the parallel masking scheme of Barthe *et al.*, that we consider in our experiments, followed by a description of our setups. The section is concluded with a brief review of Moment-Correlating Profiled DPA (MCP-DPA) that will be our main statistical tool to demonstrate the exploitability of lower-order side-channel leakages presumably due to externally-amplified couplings, and Welch's T-Test leakage detection which will help us to strengthen our observations.

[2] Typically, values of 0 to 1Ω and differences of 200-300 mV were examined so far.

Notations. In this manuscript, variables are denoted with capital letters, sampled values with lowercase letters, functions with sans serif fonts and vectors with bold letters. We consider masked (aka secret shared) implementations where every sensitive variable s is represented by d-1 random variables $(s_1, s_2, ..., s_{d-1})$ and one more variable s_d, which complies with:

$$s = s_1 \oplus s_2 \oplus \cdots \oplus s_d, \tag{1}$$

where $\oplus$ is a group addition operation in a finite-field (in the case of binary values in GF(2), it represents the XOR operation between bits). If the secret is a vector ($\boldsymbol{s}$) of b bits, the operations are done bit-wise. The secret variable is never processed within the hardware, only its d shares are. For this purpose, and in order to implement a cryptographic primitive (which translates to an architecture), one must be able to perform logic operations securely on the shared values. In general, any logical function can be represented (or synthesized) by multiplications (AND gates/operations) and additions (XOR gates/operations). Implementing linear operations is considered easy and can be performed share by share. For multiplications, it is well known (see for example [ISW03]) that special care should be taken as they *recombine* values of different shares (logically). In this work, we examine two popular architectures to perform secure multiplications that we detail next. We then demonstrate how physical recombinations can take place.

1.1 Domain-Oriented Masking and Barthe *et al.*

Parallel Hardware Implementation - DOM AES. The first architecture which will be examined in this work is the Domain-Oriented-Masking (DOM) architecture. In [GMK17] Gross *et al.* proposed a procedure to implement a masked AND over shared variables. The approach consists in splitting the shares into *domains* corresponding to the shares indices (*e.g*, $\{a_1,b_1\}$ or $\{a_2,b_2\}$ for variables a and b shared in two), and to keep the shares of all domains independent from shares of other domains. This independence ensures d^{th}-order security. The domain separation allows the DOM architecture to minimize the number of random bits needed to perform the refreshing part of the multiplication, compared to the original algorithm by Ishai, Sahai and Wagner.

Important for our later discussions, the full DOM AES architecture is shift-register based. That is, only one byte is processed at a given clock cycle, and the generated values are stored in a shift-register. Each AES round in this architecture takes above 20 clock cycles (we specifically used the 23 cycles per round architecture of the "AES simple" design from [GMK17]). Thus, it is expected that if there exist physical couplings for a specific intermediate value, they will be evident for a long duration in the system.

Parallel Software Implementation - Barthe et. al. The second architecture we consider is software-oriented and utilizes the parallel multiplication (and refreshing) algorithm(s) by Barthe *et al.* [BDF+17], which aim(s) at performing efficient secure computations by storing all the shares of a sensitive variable in a single register. The test case we consider in this manuscript is similar to the one detailed in [JS17]. In the algorithms below, the shares of a are grouped and represented by a vector such that $\boldsymbol{a} = (a_1, a_2, ..., a_d)$ and $\mathsf{rot}(\boldsymbol{r}, m)$ denotes the rotation of vector $\boldsymbol{r}$ by m elements.

It is important to highlight that these algorithms can be processed in parallel since operations on bits of different shares can be executed simultaneously (in the same computation cycle / instruction) over a micro-controller data-path (which is sometimes referred to as a bit-sliced implementations). In this manuscript we utilize the implementation of these algorithms in a bit-sliced fashion as done in [JS17]. The motivation for using such a bit-wise shares-parallel architecture, other than its performance attractiveness, is that it is easier to capture and interpret the leakage distribution (as will be clear in Section 2).

Algorithm 1: Parallel Refreshing [JS17].

0: **Input**: shares of a ($\boldsymbol{a}$) and a uniform randomness vector $\boldsymbol{r}$.
0: **Output**: refreshed shares $\boldsymbol{b}$ of $\boldsymbol{a}$.
1: $\boldsymbol{b} = \boldsymbol{a} \oplus \boldsymbol{r} \oplus \mathsf{rot}(\boldsymbol{r}, 1)$
2: return $\boldsymbol{b}$

Algorithm 2: Parallel Multiplication (illustrated with the case d=4 [JS17]).

0: **Input**: shares of a and b ($\boldsymbol{a}$, $\boldsymbol{b}$) and a uniform randomness vector $\boldsymbol{r}$.
0: **Output**: shares $\boldsymbol{x}$ of x, with $a \cdot b = \bigoplus_{i=1}^{d} x_i$.

1: $\boldsymbol{c}_1 = \boldsymbol{a} \cdot \boldsymbol{b}$
2: $\boldsymbol{c}_2 = \boldsymbol{a} \cdot \mathsf{rot}(\boldsymbol{b}, 1)$
3: $\boldsymbol{c}_3 = \mathsf{rot}(\boldsymbol{a}, 1) \cdot \boldsymbol{b}$
4: $\boldsymbol{d}_1 = \boldsymbol{c}_1 \oplus \boldsymbol{r}$
5: $\boldsymbol{d}_2 = \boldsymbol{d}_1 \oplus \boldsymbol{c}_2$
6: $\boldsymbol{d}_3 = \boldsymbol{d}_2 \oplus \boldsymbol{c}_3$
7: $\boldsymbol{d}_4 = \boldsymbol{d}_3 \oplus \mathsf{rot}(\boldsymbol{r}, 1)$
8: $\boldsymbol{x} = \boldsymbol{d}_4$
9: return $\boldsymbol{x}$

1.2 Measurement Setups

Hardware - FPGA with Single-ended Amplifier Probe. The first evaluation setup which is used throughout this manuscript is composed of a PicoScope oscilloscope and a SAKURA-G board. The SAKURA-G board embeds a Xilinx FPGA (Spartan-6 in 45nm technology) which was utilized to inhabit the evaluated DOM designs. The board is also equipped with a single-ended embedded amplifier which is utilized to sense the power supply voltage. The PicoScope 5244B oscilloscope was used to capture the power supply voltage directly from the amplifier. Sampling rates of 100 MS/s to 1 GS/s were practiced and the device was clocked at 4-to-12 MHz. Inputs were asserted through a UART interface to the FPGA.

Software - μC with Passive Inductive Probe. In the second setup, the target device is a 32-bit ARM Cortex-M4 processor embedded in the Atmel SAM4C-EK evaluation board. In this setup the architecture was clocked with an internal 100 MHz clock frequency. The device was powered from an on-board power regulator and from a stable and low-noise external power supply. The core power supply current was measured with a passive inductive probe (Tektronix-CT1) connected serially to the measurement points after a variable soldered SMD resistor (with varying values of 1-39 ohms on V_{DD}-$CORE$ measurement point, JP6). The inductive probe was connected to a Lecroy WaveRunner HRO 66 oscilloscope. Current traces were collected with between 250 MS/s to 1 GS/s and 12-bit of amplitude resolution. Quite importantly, with this setup, due to the passive inductive probe, no external resistor was needed in practice. However, we added some to amplify the physical couplings.

A Note On the Importance of the Measurement Setup. The measurement setup quality is in general of very high importance in side-channel security evaluations, and not sufficiently studied nor understood yet. As previous works (*e.g.,* [PS17]), we have repeatedly witnessed significantly different levels of noise in different setups. In the context of low-order leakages amplification and couplings, results degradation due to noisy evaluation setups can be even more critical. As the effects demonstrated in this manuscript are amplified externally, if the amplification circuitry is noisy (*e.g.*, by long and dangling routings, noisy resistors selection, or by utilization of a noisy probe or a physically unstable setup), it might lead to quite different results and conclusions. This will in turn have a strong impact on the number of measurements needed to perform an attack. We used a 12-bit Picoscope oscilloscope (with/without a passive CT1 probe), which gave us limited noise. Moreover, in order to improve our setups, we removed unwanted capacitive elements from the measurement boards (*e.g.* capacitors C6 to C10 on the SAM4C-EK board) and we used a very high-resolution and (sometimes) higher sampling rates than mentioned in

previous reports within a highly maintained measurement environment and calibrated device's ADC ranges etc. In this respect, we note the significantly worse results that we obtained before improving our setups (*e.g.,* by directly using two high-end oscilloscopes, a LeCroy and a Keysight, with active-differential probes, we needed to collect $\sim \times 10^2$ more traces than with our optimized setups in order to see the same phenomena as discussed in Subsection 3.1 and shown in Figure 4). So in general, the reduced data complexities that we observe in the following are attributed to the setup quality and to the reduced noise environment. However, we insist that our focus is not on the understanding of all the parameters influencing the quality of side-channel measurements, but on how isolated changes can impact the effective security order of a masked implementation.

1.3 Moments-Correlating Profiled DPA and Welch's T-test

As described in the introduction, in this manuscript we are interested to move from the detection-based analysis of previous works to attack-based evaluations, in order to confirm the exploitability of the lower-order leakages that we amplify (and the corresponding reduction of security level). Moments-Correlating Profiled DPA (MCP-DPA) is used for this purpose. It serves as a natural tool to this end, since it profiles different statistical moments and observes only their respective informativeness [MS16]. We shortly detail on MPC-DPA in this section. In addition, in some places along the manuscript we utilize detection tests (namely, Welch's T-test), which we also recall for completeness.

Let $l_{x,k}$ be a leakage trace measured with the setup discussed in Subsection 1.2. To perform an MCP-DPA, one should choose a target computation to template (in the case of an AES, typically the first round SBOX output). That is, the manipulation of the target intermediate value $\mathsf{f}(x,k)$ associated to a known plaintext (byte) x and secret key (byte) k. A set of $\mathcal{L}_p$ profiling traces of size N_p is first used in order to estimate the d^{th} leakage moments, denoted as $\hat{M}^d_{x,k}$. Next, during the attack (online) phase, a fresh set of new traces $\mathcal{L}_a$ of size N_a is utilized. Finally the secret key (byte) $k*$ which maximizing the following simple univariate correlation is chosen:

$$\tilde{k} = \arg\max_{k*} \quad \hat{\rho}(\hat{M}^d_{x,k*},\ \left({l^t}_{x,k}\right)^d), \tag{2}$$

where $l^t_{x,k}$ is a leakage trace sample ($t \in \{0, ..., \#samples\}$) which corresponds to the manipulation of x and k. For the 1^{st}-order moment, Equation 2 is used as-is with d=1; for d=2, the second-oder central-moment (denoted as CM) is used (instead of the raw M); for higher orders the standardized central moment (denoted as SM) is used. Quite interestingly, since MCP-DPA correlates profiled statistical moments with leakage samples (raised to some power), the correlation values it outputs provide a metric flavor and leads to a rule-of-thumb to quantify the number of measurements needed for key recovery [MS16].

The detection method used is the traditional univariate one, based on Welch's (two-tailed) T-test [Wel47]. It is computed on two input sequences (Set_0 and Set_1). In this work we compare two classes of leakages with so-called non-specific "*fixed* vs. *random*" [CMG+] and "*fixed* vs. *fixed*" [DS16] tests to detect leakages, using the following statistic:

$$T_{value} = (\mu_{Set_0} - \mu_{Set_1}) \Big/ \sqrt{{\sigma_{Set_0}}^2/|Set_0| + {\sigma_{Set_1}}^2/|Set_1|}, \tag{3}$$

where μ and σ are the populations' mean and standard-deviation, respectively. The leakages from the random sequences were recorded with random inputs and fixed key (and tested for multiple keys). The leakages from the fixed sequences were recorded with fixed input and key. Detection was assumed for estimated statistics beyond a certain threshold (we used the 4.5 threshold that is frequently considered in practice). In addition, we use the generalization in [SM16] to analyze higher-order statistical leakages.

2 Externally-Amplified Couplings

In this section, we use a simple case study of a masked implementation with two single-bit shares in order to discuss the physical effects that cause the external amplification of couplings theoretically. We start by providing an intuitive description, and follow with a modeling attempt which, despite overly simplified, allows a quantified prediction of the security order reduction that such couplings may imply. We recall that as any physical model, it is tentative. As will be clear in the following experimental sections, it is plausible in the sense that it reasonably predicts the reductions of the security orders (and the shape of the measurement curves) we observe. But further refinements are certainly possible (especially for higher-order analyzes) which we leave as a scope for further research. For simplicity, from now on we will stop adding cautionary remarks regarding the possible limitations of this physical model, and just use it as our current explanatory tool.

2.1 Intuitive Description

In this subsection, we detail the logical and physical assumptions of masked implementations. We start with a simplified and illustrative example with $d = 2$ shares processed in parallel (simultaneously), as shown in Figure 1a. Let L_i denote the leakage of share i where, the leakage is assumed to follow the Hamming Weight model (denoted as $\mathsf{W}(\cdot)$) with some additive Gaussian noise (denoted as N_i). As briefly detailed in introduction, the basic assumptions of masking designs are that the leakages of the shares are sufficiently noisy and that each leakage sample either depends on a single share or is a linear function of the shares' leakage (*i.e.*, no recombination of the shares is "performed" by the leakage function). For example, the leakage function can be a sum function of the shares' currents ($L = L_1 + L_2$). The illustrative conditional distribution of this leakage function (*i.e.,* $\Pr(L|s)$) is shown on the figure. In this scenario, the conditional means ($\mu_{L|s=i}$, $i \in \{0, 1\}$) are equal and only the conditional variances (or standard-deviations, $\sigma_{L|s=i}$) are informative (*i.e.*, second-order moments must be estimated to recover sensitive information). These intuitions extend to higher orders in the natural way.

This ideal setting is followed by an abstraction of the same system at the physical level (in Figure 1b). We use it to capture physical and design defaults, and situations where the leakage samples do not only depend on a single share or a linear combination of the shares' leakages (*i.e.,* recombinations). Concretely, recombinations can be of two types:

1. *Logical recombinations* denote recombinations which we can prevent logically (in the digital or Boolean representation). As recently formulated in [FGP+18], we denote by *glitches* internal temporary (combinational) values which process jointly more than one share – as illustrated in Figure 1b by $f_i(s_1, s_2)$. By *transitions*, we denote transitions of storage elements (between an *old* to a *new* state) that induce leakages which combine the two values (also represented in Figure 1b). These two risk factors can be prevented by a careful logic representation of the design. The main methods to prevent them is by restricting the number of shares processed jointly, as typically achieved by Threshold Implementations (TI) [NRS11] or DOM [GMK17], and by using a sufficient amount of registers to prevent memory transitions between shares or increasuing the number of shares [BGG+14]. In the following, we assume that the implementations we analyze have been designed with care and following these principles, so that no glitches nor transitions reduce the security order.
2. *Physical recombinations* denote recombinations which are induced by physical factors. We specifically classify them into two dominant factors. The first one is associated with proximity issues of shared values which are recombined due to capacitive parasitic elements (couplings) in electronic devices, as represented in Figure 1b. Interestingly, this type of recombination can be substantially reduced by careful

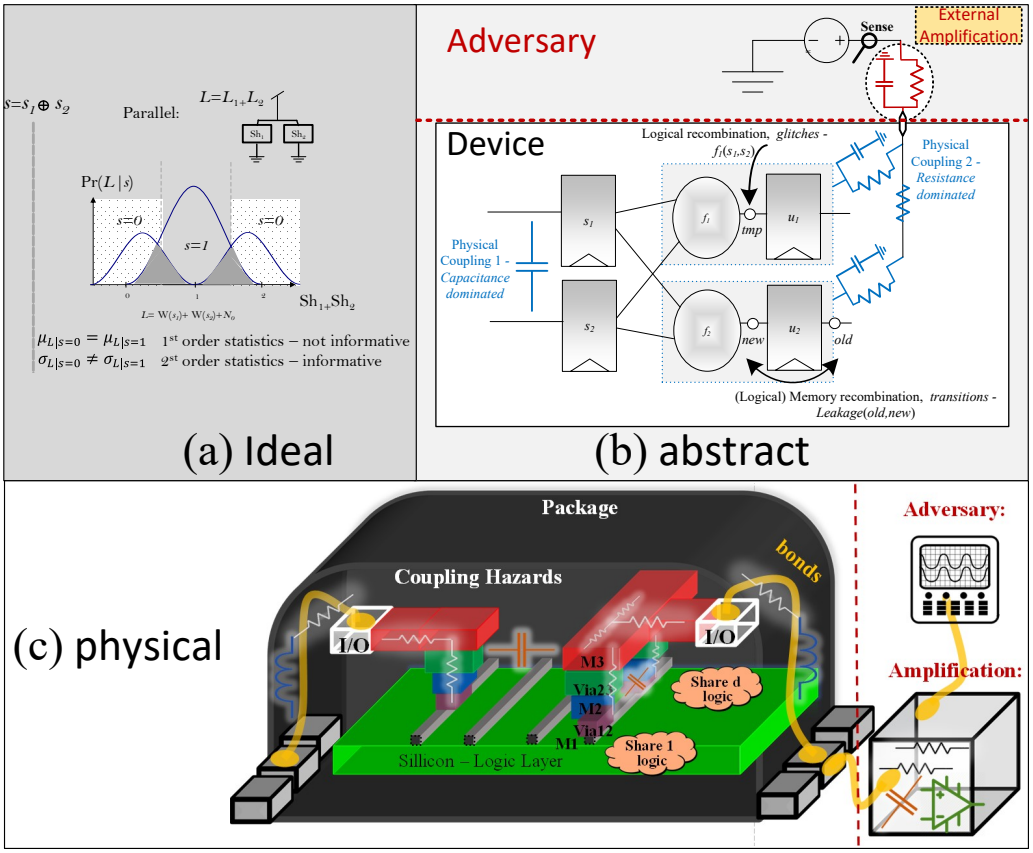

Figure 1: Illustrative example of a d=2 shares masking: (a) ideal parallel computation of the shares; (b) abstraction of the physical system; (c) physical system illustration.

design and by Electronic-Design-Automation (EDA) tools, and the capacitive values of these elements (in integrated circuits) are quite limited. The second one, which is the focus in this manuscript, is associated with electrical properties of the internal and external power-network of the device. As illustrated on the figure, each share is powered independently from one point in the design. However, all of these leakages are then merged to the main power-supply. In essence, the complex power-grid of electronic devices couples these independent leakages. The interesting (and alarming) issue is that the level of this form of resistive-dominated leakage coupling can be amplified externally by an adversary, as illustrated in Figures 1b and 1c; where Figure 1c shows the physical abstraction of the system. Clearly any abstraction of such a system which includes transistors, metal layers, IOs PADs, package, metal-bondings *etc.* will suffer from inaccuracies. From this point this specific form of recombination is denoted as *physical couplings*.

2.2 A Simple Model

We now aim to shed greater light on the physical sources of leakage couplings, and to make a step forward in formulating and modeling them. We start from a simple mathematical model to derive intuition (with two single-bit shares). We then use it to discuss the general intuitions, risks and the adversarial knobs to amplify the coupling phenomena. We note

that despite overly simplified, this model is supported by distribution plots based on measurements (in Subsection 4) and in general, is not falsified by our experiments.

Our mathematical model is based on a toy example with univariate leakages (to connect it to the real world, it implies that no capacitance is considered on nets). Considering Figure 2a, which shows a schematic ideal-world environment (with no external resistor added by an adversary: R_{ext}=0), the current drawn from the power supply is a summation of the shares' current (*i.e.*, $I_{\text{supply}} = I_1 + I_2$). However, assuming an external resistor is present (Figure 2b), the new supply current (denoted with a ') can be derived as a function of the ideal scenario currents (*i.e.*, the independent terms) as:

$$I'_{\text{supply}} = I'_1 + I'_2 = \alpha_1 \cdot I_1 + \alpha_2 \cdot I_2 - \beta \cdot I_1 \cdot I_2, \tag{4}$$

where, the parameters α_1, α_2 and β are as follows:

$$\alpha_1 = \frac{1}{(1+\frac{2\cdot R_{\text{ext}}}{R_{\text{on1}}})}; \quad \alpha_2 = \frac{1}{(1+\frac{2\cdot R_{\text{ext}}}{R_{\text{on2}}})}; \quad \begin{aligned}\beta &= \frac{R_{\text{ext}}}{V_{\text{DD\_ext}}}\left[\frac{R_{\text{on1}}}{2\cdot R_{\text{ext}}+R_{\text{on1}}} + \frac{R_{\text{on2}}}{2\cdot R_{\text{ext}}+R_{\text{on2}}}\right]\Big|_{R_{ext}<<R_{on}} \\ &\cong \frac{2\cdot R_{\text{ext}}}{V_{\text{DD\_ext}}}\end{aligned} \tag{5}$$

For simplicity we assume the transistors operate in the linear mode of operation (R_{on} denotes the *on* resistance of a transistor – in a linear mode of operation, it is defined by $1/(K(V_{GS} - V_T))$ [RCN02]). It is important to emphasize that the coefficients of the non-coupled elements (I_1 and I_2) tend to one as typically the transistor's *on* resistance R_{on} is much larger than the (controlled) R_{ext} which is chosen by the adversary. More importantly, the coupling element (β) tends to $\frac{2\cdot R_{\text{ext}}}{V_{\text{DD\_ext}}}$. This simple analysis reveals a quite alarming scenario (which is supported and better modeled in the following):

1. An adversary can induce and substantially amplify couplings (linearly in R_{ext}).
2. If simultaneously changing the supply V_{DD_ext}, the phenomena can be extended.
3. In the presence of an internal shared resistor, an adversary can utilize the power-supply voltage alone to amplify the internal couplings (as observed in [CBG+17, CEM18]).

Figure 2a-b shows the distributions obtained from the simplified model (Equation 4) under the assumption that each of the shares generates a normal and independent Gaussian noise (*i.e.*, $I_j^{noisy} = I_j + N(0, \sigma_n)$) with zero mean. The noise variance is a parameter in this setting which implies a certain Signal-to-Noise Ratio (SNR) ratio. Several observations can be drawn from the distributions:

1. In the *Ideal* setting ($R_{ext} = 0$), the conditional leakage distributions of the model are symmetric and 1^{st}-order secure (see Figure 1a for the ideal distributions).
2. While increasing R_{ext}, the *physical-coupling* element (β) starts to play a role: when current flows through I_1 and I_2, the right Gaussian element (from the Gaussian mixture) starts to shift left in mean (due to the minus β factor) and its variance is reduced by two (assuming the two normal noise elements in the multiplication have the same variance). In turn, this asymmetry is reflected in the figures. As the statistical set size increases (*i.e.*, more samples are used) the asymmetry becomes clearer.

Next, the simple equation from above is further generalized assuming multiple current consumers on the power-network (which, without the loss of generality, can correspond to multiple shares or multiple bits). For simplicity, let us denote $K' = K(V'_{GS} - V_T)$. Then, a single bit/share/consumer current (i) can be written as:

$$I'_i = K'_i V'_{DS_i} = K'_i(V_{DS_i} - R_{\text{ext}} \cdot I'_{\text{supply}}) = I_i - K_i \cdot R_{\text{ext}} \cdot I'_{\text{supply}}. \tag{6}$$

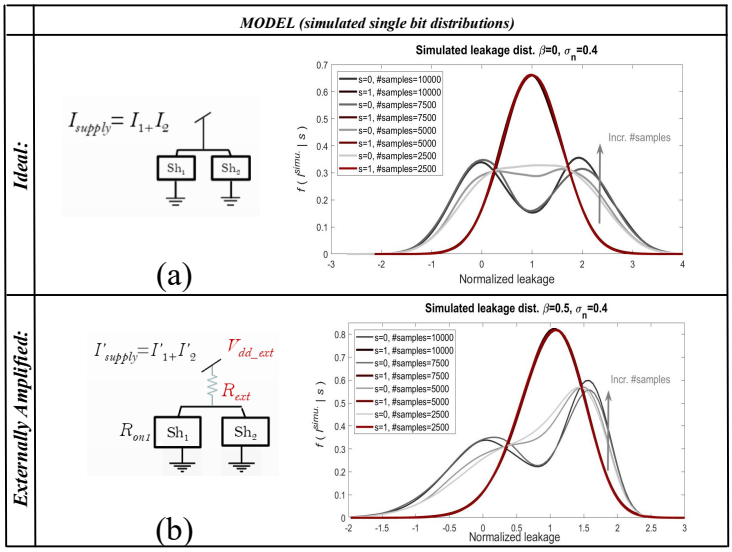

Figure 2: $\mathtt{f}(l^{simu.}|s)$: (a) β=0 (b) β=0.5.

The total current can then be computed as the individual consumers currents' summation:

$$I'_{\text{supply}} = \sum_i I'_i = \sum_i I_i - K_i \cdot R_{\text{ext}} \cdot I'_{\text{supply}} \rightarrow I'_{\text{supply}} = \frac{\sum\limits_i I_i}{1 + R_{\text{ext}} \cdot \sum\limits_i K'_i}. \tag{7}$$

By assuming that $R_{\text{ext}} \cdot \sum\limits_i K'_i << 1$,[3] and expending the *Taylor* series (of $1/(1+x) \approx 1 - x + x^2 - x^3 ...$), the total current can be rewritten by:

$$I'_{\text{supply}} \approx \sum_i I_i - R_{\text{ext}} \cdot \sum_i I_i \left[\sum_j K'_j\right] + {R_{\text{ext}}}^2 \cdot \sum_i I_i \left[\sum_j K'_j\right]^2 + ... \tag{8}$$

Recalling that $I'_i = K'_i V_{DS_i}$, simplifying $V_{DS_i} = V_{DD}$ (of secondary importance) and taking a closer look at the first two elements of the equation, we finally derive:

$$I'_{\text{supply}} \approx \underbrace{\sum_i I_i}_{2^{nd}-order} \underbrace{- \frac{R_{\text{ext}}}{V_{DD\_ext}} \cdot \sum_i \sum_j I_j I'_i}_{1^{st}\ order} + ... \underbrace{\qquad}_{higher\_powers}. \tag{9}$$

Note that, other than constants which tend to one (*e.g.*, α_i), Equation 9 generalizes the simplified Equation 4 for multiple physically-coupled shares and/or multiple physically-coupled bits. An important observation is that R_{ext} generates couplings in all mathematical powers, thus in all statistical moments and for any order of secret-sharing (without the loss of generality R_{ext} can be modeled as a combination of the internal – IR drop – and the external resistances). For example, it is easy to anticipate that for a design with three shares (ideally 2^{nd}-order secure), the first term (powers of 1) will include 3^{rd}-order information, a second term (powers of two) will be amplified by R_{ext}/V_{DD_ext} and contain 2^{nd}-order information, and the third term (powers of three) will be amplified by $(R_{ext}/V_{DD\_ext})^2$ and contain 1^{st}-order information. Quite naturally, the effect of couplings in lower statistical

[3] Which is conservative: in current technologies, transistors' overdrive ranges from 10^4 to 10^6 Siemens.

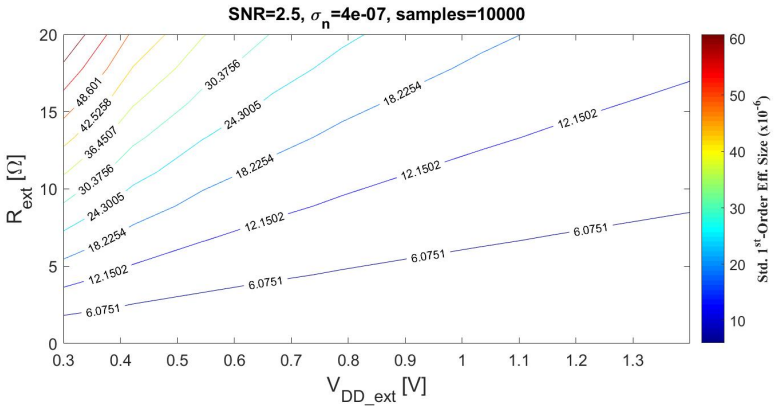

Figure 3: Contour plots of the standardized 1^{st}-order effect size as a function of R_{ext} and V_{DD_ext}. The values on curves represents the actual value of each contour.

orders (*i.e.,* in higher powers of I's in Equation 9) is also reduced as multiplication of d currents, which are typically very small, takes place. So from the adversarial perspective, the important question is whether the external amplification is sufficient so that the couplings reduce the effective security order.

We note that the validity of this model is admittedly limited and we stress that we do not expect that actual leakages in a concrete system will be as simple. However, we believe that it provides important insights on the key factors which affect the physical couplings (whether through the device power-grid or the external physical setup).

We also emphasize that the internal couplings of share's bits do not break the independence assumption and therefore, from Equation 9, we are interested in *inter-* and not *intra-share* couplings. In turn, this implies that we can assume that (*e.g.,*) I_1 and I_2 are multi-bit Hamming weight leakages of full shares, which only couple through (*e.g.*) β.

To conclude this section, and as discussed above, the main knobs of the adversary are the power supply voltage and the external resistance. We used a leakage simulator approach to simulate the physically-coupled leakages with additive and independent Gaussian noise (per share). Our goal was to assess the first-order detectable signal as a function of β. To do so, we define the 1^{st}-order effect size as:

$$Eff.\ Size^{1^{st}Order}(V_{DD\_ext}, R_{ext}) = \mathsf{E}(L|s=1) - \mathsf{E}(L|s=0). \tag{10}$$

Figure 3 plots the standardized 1^{st}-order effect size as defined by:

$$\frac{Eff.\ Size^{1^{st}Order}(V_{DD\_ext}, R_{ext}) - Eff.\ Size^{1^{st}Order}(V^{\min}_{DD\_ext}, R_{ext}=0)}{\mathsf{E}(L|s=0)}. \tag{11}$$

As shown in the figure, the external voltage and resistance have concrete first-order security implications. The next sections will demonstrate experimentally that externally-amplified low-order leakages can be observed in practice with a 2-share masked design. We leave the investigation of a larger number of shares (together with model refinements possibly needed to better capture such complex cases) as an interesting open problem.

3 Hardware (FPGA) Experiments

In this section, we evaluate amplified coupling effects over the Domain-Oriented-Masking (DOM) architecture implementation (see Subsection 1.1). We deal with the practical exploitability of the (coupled) leakages. More concretely we have two objectives:

1. To show that the phenomena of amplifying the leakage of sensitive information externally is concrete and paves the way to relatively easy attacks (or more informativeness of the leakage probability distributions). That is, concurrent changes of external resistances and power supply voltages lead to significant changes in the Success-Rates (SRs) of practical attacks.

2. To demonstrate that the lower-order statistical characteristics of the leakages are easily exploitable and meaningful for actual key extraction. That is, it is possible to make 1^{st}-order leakages more informative than 2^{nd}-order ones simply by adversarially-controlled external tweaks (transparent to the device).

We recall that the DOM architecture is byte-serial, based on shift-registers, and a secret variable is shifted in the system for 23 clock cycles (depending on the flavor chosen for the design and the S-box data-path, in our case the "AES-simple" with 8 SBOX stages was used). In turn, and even if ideal refreshing takes place (between the shift operations), if there exist physical couplings, they will be present in the system for a very long duration (which will be concretely observed in the following).

3.1 External Amplification *vs.* Internal Coupling: T-tests

As discussed in the introduction, all secret-sharing based designs suffer from physical couplings to some extent. This issue has been discussed in previous manuscripts. As a result, the main open problem is to understand how severe the phenomena is and to what extent can it be systematically exploited. For example in [DFS15] it was theoretically modeled by a (flaw) f factor, and in [CBG+17] it was shown in practice that internal couplings can be observed and that such a problem can lead to security order reductions (despite note yet impacting the security level, due to the low amplitude of these low-order leakages). In this manuscript, we aim to show how practical attacks can benefit from externally-amplified lower-order leakages thanks to modification of the setup's resistor and implementation's power supply, which we posit can be explained by the model in the previous section and the concept of externally-amplified couplings.

As a preliminary (and to reproduce previous reports), we start by performing evaluations based on leakage detection. We note that the experiments done in this and the following sections were (at least) 10-fold cross-validated (with subsets of the data). In particular for the fixed *vs.* random T-tests, the results were cross-validated across random (but) fixed vectors. We focus on Points-Of-Interest (POI) which are the output of the first AES round (which we will target in our MCP-DPA analysis next). Figure 4(a-b) shows 1^{st} and 2^{nd} order non-specific leakage-detection (T-tests) results *vs.* the number of traces. Devices with external amplification appear in solid-black and solid-red curves. As done by De-Cnudde *et-al.*, we also demonstrate experiments with aggressive internal-amplification (by constraining the placement of different shares on the device) which appear in blue and dashed black curves. It is first shown (Figure 4(a) and (b)) that, both for the 1^{st}- and the 2^{nd}-order, externally-amplified couplings are more significant than internal couplings.

The last set of curves on Figure 4(a) and (b) demonstrate a noisy setup/environment scenario. Our goal is to stress how critical the evaluation setup quality is and how prominent externally-amplified couplings are, even in noisy environments. First, the black curves with triangle marker show the exact same experiment with an 8-bit resolution oscilloscope (whereas the rest of the experiments are performed with 12-bit resolution) and the circle- and plus-marked curves show results with artificially increased noise (we have added Gaussian noise with standard deviations of 2x and 4x the one of the measured noise in our setup). As expected, the effect of these changes is significant, recalling the importance of the setup in security evaluations (*i.e.*, that noisy setups can lead to a false sense of security, as in general any suboptimal attack choice). To confirm the impact of

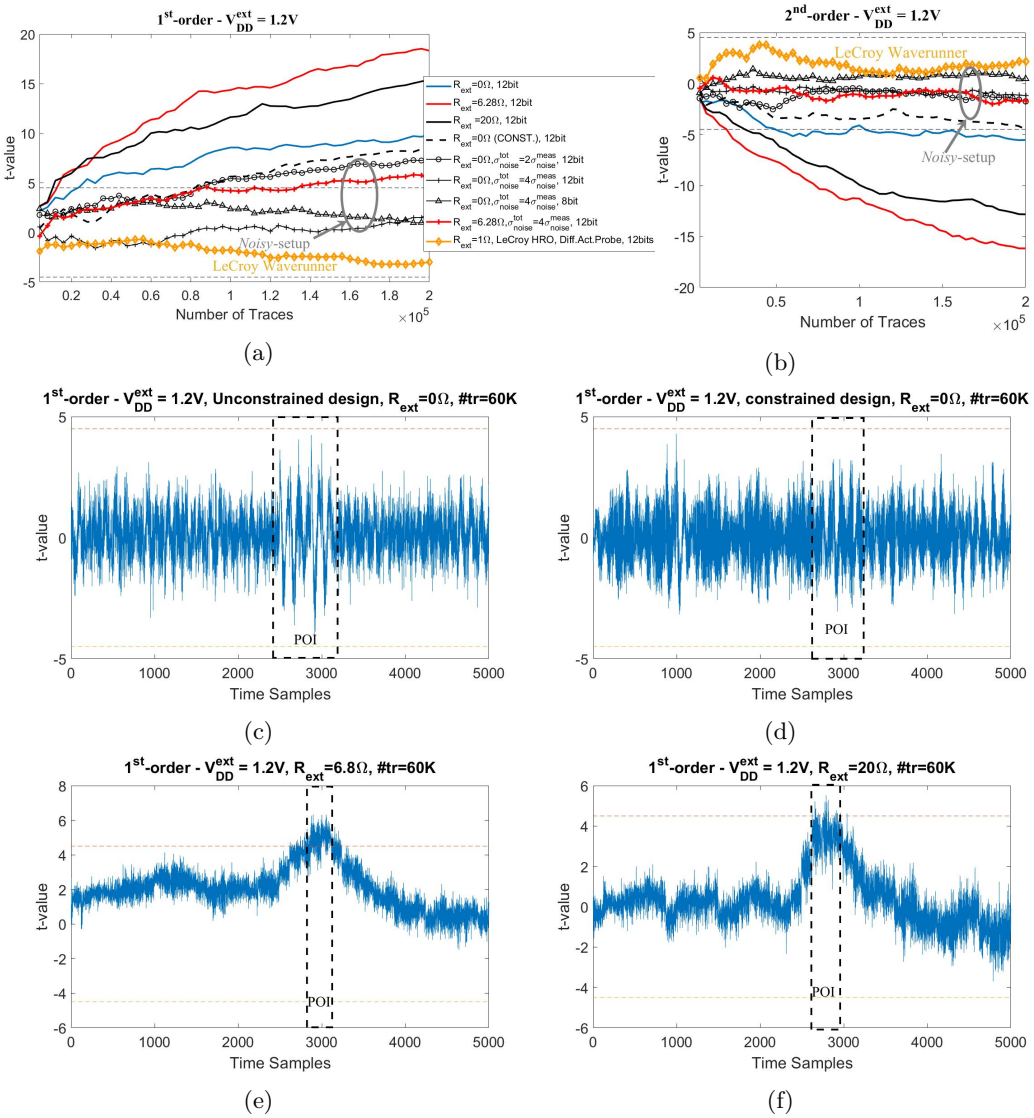

Figure 4: AES DoM Order 2. T-test value versus $\#traces$ for different external resistor values and noise levels (for all $V_{DD}^{ext} = 1.2V$). (a) 1^{st}-order (b) 2^{nd}-order, and examples in the time domain: (c) $R_{ext} = 0\Omega$ proximity unconstrained design, (d) $R_{ext} = 0\Omega$ proximity constrained design, (e) $R_{ext} = 6.8\Omega$ and (f) $R_{ext} = 20\Omega$.

a noisy setup, experiments are also shown (with an orange curve and square markers) for a LeCroy WaveRunner Osciloscope with an active differential probe. As discussed in Section 1.2, we needed to collect $x10^2$ traces to reach the same detection in this case. Finally, the plus-denoted red curve represents the experimental results obtained with an increased artificial-noise over the externally-amplified couplings scenario. Even in this context, the detection remains more significant with a lower data-complexity than with the corresponding non-amplified (or internally-amplified) scenarios.

Figure 4(c-d) then shows the T-test values in the time domain while tweaking the leakage internally (by constraining the physical placement of our shares) with no amplification ($R_{ext} = 0\Omega$). And Figure 4(e-f) shows the T-test values while aggressively amplifying the low-order leakages externally ($R_{ext} = 6.8\Omega$ and 20Ω). All these experiments have

been performed with nominal supply voltage conditions (*i.e.*, $V_{DD}^{ext} = 1.2V$). Important observations from the figures include:

- Internal couplings: the leakage in both cases of $R_{ext} = 0$ (Figure 4(c-d)), while constraining the shares to be placed with minimal and maximum proximity, exhibit T-values which for the same data-complexity are lower than with external amplification.
- Long duration effect: external amplification which is done by large resistances adds a non-negligible parasitic capacitance. In practice, this is a very dangerous scenario as it filters the (coupled) leakages and makes it evident for a very long duration in the traces. This is clear in Figure 4(c-d) *vs.* Figure 4(e-f). It is important to note that such couplings can combine with operations in different computation cycles, which is quite problematic for designers (and is reminiscent from [MM13]).
- Noise *vs.* amplification *vs.* filtering trade-off: our simplified model suggests that for the same voltage, increasing R_{ext} will induce more coupling. By contrast, clearly, very large resistors induce large noise. For example, Figure 4(a) illustrates that the actual T-values for $R_{ext} = 6.8\Omega$ are actually larger than for 20Ω. Besides, and as discussed above, larger resistances increase the filtering which makes the coupling effect evident in more time-distant samples.

Before moving on with practical key extraction attacks, we finally compare these detection-based experiments with prior art. In Figure 4(a-b), it is shown that even in nominal conditions couplings can take place (presumably due to the internal power grid). This is actually similar to some scenarios investigated by De Cnudde et al. on the exact same design (Figures 14 and 15 in [CEM18]), which showed a detectable 1^{st}-order leakage on designs of orders 2-4 for the AES DOM core (with a very small shunt resistor of 1Ω, which in the scale of the current manuscript, is with almost no amplification). These results match quite nicely our results in Figure 4 with 0Ω resistor. Therefore, not only if there is amplification can a "theoretically 1^{st}-order secure" design be susceptible (since couplings are always there to some extent). In this respect, we note again that the main contribution of our manuscript is to better quantify how significant these leakages can become when amplified externally (in terms of concrete security level measured as a data-complexity). External amplification also corresponds to a more realistic adversarial setting, since internal amplification requires tweaking the placement/routing or to iterate several linear operations on the shares to increase their leakage amplitude [CBG+17, CEM18], which designers should typically avoid and adversaries have no ability to force.

In the following, we confirm these results with 100 repeated MCP-DPA attacks for which we evaluate the empirical Success-Rates. Moving from a detection-based evaluation to attack-based one will concretely reveal the severity of the discussed phenomena in terms of attack data complexity to perform a key recovery.

3.2 External Amplification *vs.* Internal Coupling: MCP-DPA

MCP-DPA is of interest in this work in order to assess the impact of the external (adversary-controlled) knobs on information lying in low-order statistical moments of the leakage distributions. In practice all the moments of the leakages are first profiled, and then the model is exploited in a rather simple correlation attack.

In our FPGA case study, we zoom-in to the first two AES cycles, with 5,000 time samples and a sampling frequency of 500 MS/s. The computed attack Success-Rate over 100 experiments is shown in Figure 5. It contains the 1^{st}-order attack SR for $V_{DD}^{ext} \in \{1, 1.2, 1.45\}V$ and for $R_{ext} \in \{0, 20\}\Omega$. It is clear that even with close to $1 \cdot 10^6$ traces, the SRs with no amplification ($R_{ext} = 0\Omega$) and with nominal (1.2V) and other extreme voltages, are quite low. By contrast with external amplification, with as little as

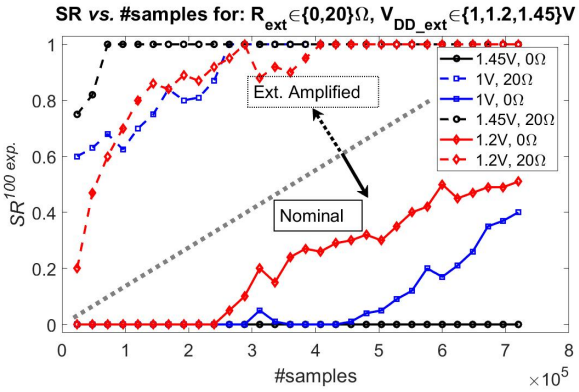

Figure 5: AES DoM Order 2.1^{st}-order MCP-DPA attack, 100-experiments Success-Rate for $R_{ext} \in \{0, 20\}\Omega, V_{DD\_ext} \in \{1, 1.2, 1.45\}V$.

$20 \cdot 10^3$ traces the leakage is fully exploitable (*i.e.,* SRs of 1 are reached). These results show concretely how significantly the effective security order reduces as well as the attack data-complexity. We therefore answer our first question which is to understand whether with this setup we get a clear impact (change in attacks Success-Rates *etc.*) as a function of the external knobs (*i.e.*, the adversarial control).

In the following, we move on to examine more carefully the results *vs.* the number-of-traces and in the time domain. In Figure 6, the 1^{st}-order MCP-DPA correlations are shown for all R_{ext} and V_{DD_ext} scenarios in the time domain.[4]. In the figure we zoom-in to 500 time samples between the two rounds captured (5000 samples). Note that besides the nominal voltage, the two voltage states chosen (1.45V and 1V) are quite extreme for the device in use. Similarly, the combination of the high-resistance value (of 20Ω) and the low supply voltage is quite drastic for such a device, pushing it to the verge of functionality (but exhibiting high couplings). Note also that we have chosen one scenario to present out of the repeated experiments performed which leads to the SR results discussed above.

Looking at the 1^{st}-order moment with no amplification (and nominal voltage) (Figure 6a), the profiled computation is visible (internal couplings) where the correct key is evident. Yet, the correlation values with no amplification are at maximum 0.05, for all voltage scenarios. For $R_{ext} = 20\Omega$ (Figure 6(b-d) and (f)), much higher correlation values are reached (at maximum 0.7) and the correct key is actually much more distinguishable and more importantly, for very long duration (in time). We conclude that in this 1^{st}-order scenario we can clearly see the low-order leakages amplification by only changing the external resistance to (sometimes extreme) values. The different scenarios for the 2^{nd}-order leakage (in Appendix A) show that the correlation values are significantly smaller and the correct key is more hidden within wrong-keys in all cases.

We continue our investigations by trying to answer the second question discussed above, *i.e.*, do the amplified couplings imply a reduced (effective) security order for the considered noise levels? As discussed in [MS16], the asymptotic correlation value ($\hat{\rho}_a$) of MCP-DPA relates to the number of traces needed for key recovery ($N_s \approx c/\hat{\rho}_a^2$).[5] Therefore, from the best 2^{nd}-order central-moment correlation value (among all scenarios) ∼0.06, to the worst 1^{st}-order moment correlation value (of the amplified ones) ∼0.8, we can expect at least an N_s improvement of 10^2 (x100 less traces) to reach stable correlation values. Figure 7 shows the MCP-DPA convergence *vs.* the number of samples for all of the examined scenarios. As exemplary shown (out of 100 experiments), the 1^{st}-order moment is stable (Figure 7(b-d)

[4] In Appendix A we complement these results with the corresponding 2^{nd}-order ones.
[5] With c a constant factor which depends on the target SR and number of bits guessed

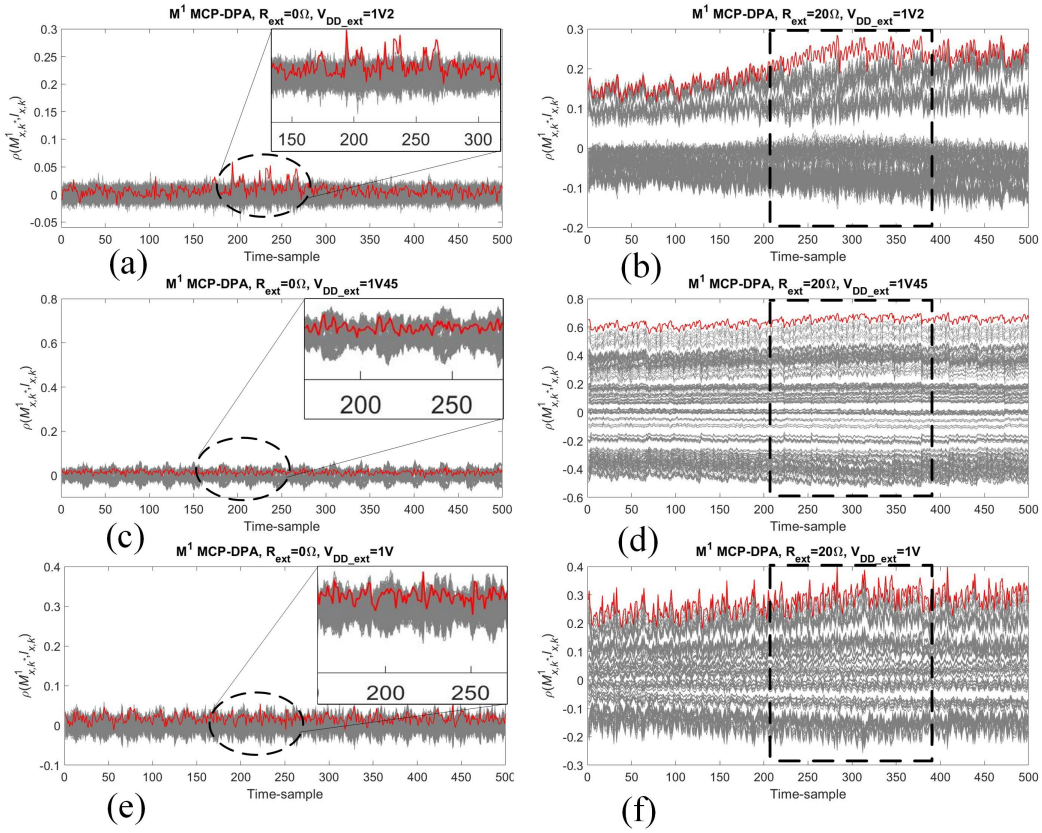

Figure 6: AES DoM Order 2. 1^{st}-order MCP-DPA correlation *vs.* time for 500 samples in the 2 first rounds: $V_{DD\_ext} = 1.2V$ (nominal): (a) $R_{ext} = 0\Omega$ (b) $R_{ext} = 20\Omega$. $V_{DD\_ext} = 1.45V$: (c) $R_{ext} = 0\Omega$, (d) $R_{ext} = 20\Omega$.$V_{DD\_ext} = 1V$: (e) $R_{ext} = 0\Omega$, (f) $R_{ext} = 20\Omega$.

and (f)) with $\sim 1 \cdot 10^3$ traces (with a profiling set of $25{\cdot}10^4$ traces) whereas the 2^{nd}-order moment converges (in Appendix A) with $\sim 2 \cdot 10^5$ traces with the same profiling effort, confirming that the 1^{st}-order moment can be made easier to exploit thanks to externally-amplified couplings. It is also captured in Figure 7 that each knob plays a cardinal part in the coupling effects: both the voltage (*i.e.*, the different rows) and the resistance (*i.e.*, the different columns). Note however that such aggressive voltage shifts (450 mV drop) are not always possible, especially not over software platforms (micro-controllers). Thus, FPGA and ASICs are more sensitive to amplification in this sense.

4 Software (ARM-32) Experiments

In this section, we complement the previous hardware experiments and perform an in-depth evaluation of the bit-wise parallel masking scheme of Barthe *et al.*, (see Subsection 1.1) in light of an adversary which has external access to the device and can vary R_{ext} and V_{DD_ext} (thanks to the setup environment described in Subsection 1.2). The Section is divided into several parts: first we verify the simulated leakage distributions from Section 2 (in Subsection 4.1), next we report on leakage exploitation and finally we provide some leakage detection results (to compare with the results in [JS17]). Overall, we use this section to demonstrate that the problem is not hardware-specific.

Preliminary Notes on External Amplification over Software Platforms. In the broad sense, moving from a hardware-based platform (*e.g.*, FPGAs and ASICs) to a software-

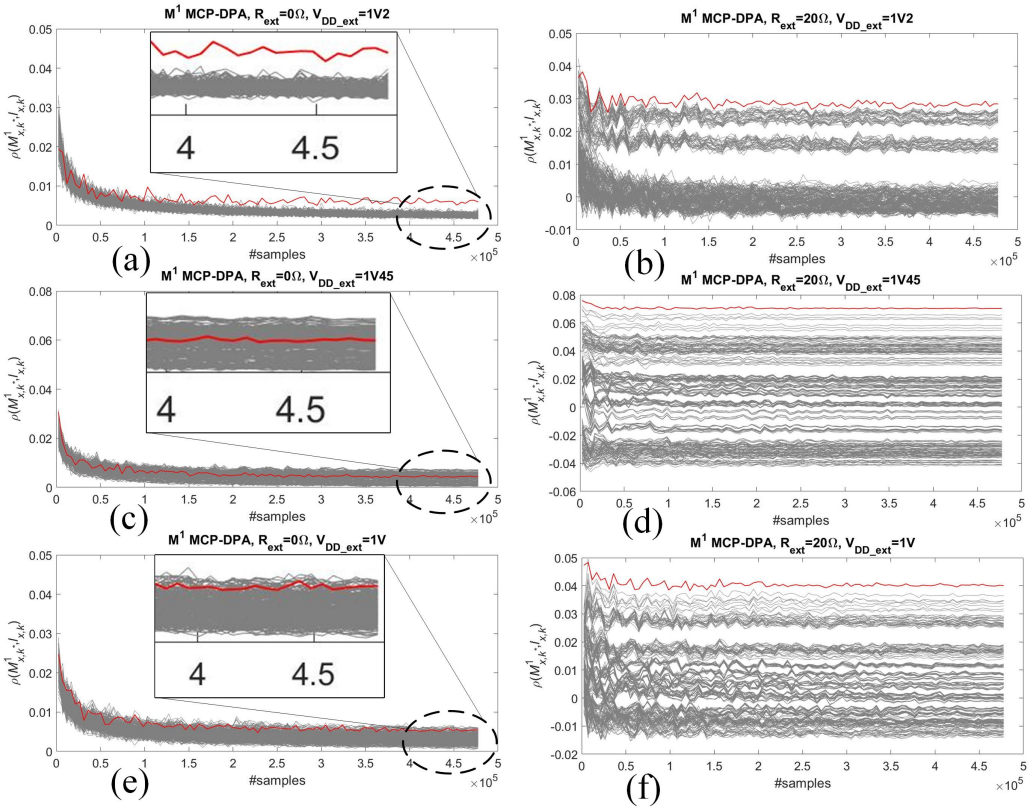

Figure 7: AES DoM Order 2. 1^{st}-order MCP-DPA correlation *vs.* the number of traces: $V_{DD\_ext} = 1.2V$ (nominal): (a) $R_{ext} = 0\Omega$ (b) $R_{ext} = 20\Omega$. $V_{DD\_ext} = 1.45V$: (c) $R_{ext} = 0\Omega$, (d) $R_{ext} = 20\Omega$.$V_{DD\_ext} = 1V$: (c) $R_{ext} = 0\Omega$, (d) $R_{ext} = 20\Omega$.

based platform we expect a significant difference. The reason is that in micro-controllers architectures the computation unit is typically centered and not spread (spatially). This implies that the shared power-grid is quite significant and external amplification would pick that up and more easily amplify it. On the other hand on (*e.g.*,) FPGAs, the power grid is deterministic, spread and spans the entire device or large segments of it and therefore is expected to be noisier (due to independent logic activity and larger electronic noise from parasitic elements). Yet, and admittedly, it is quite complicated to actually compare the two platforms for two main reasons:

- Building a (masked) design for an hardware device which will be comparable to the one implemented on a software architecture (*i.e.*, and advanced processor) is quite challenging (and not efficient) due to architectural limitations and differences and due to the different physical structure and resources etc.
- Advanced processor chips embed power regulators which are not present or comparable to those on FPGAs. For example, the 32-bit ARM Cortex-M4 processors, embedded in the Atmel SAM4C architecture we utilize, inhabits an on-chip power regulator which decouples the internal power-network from the adversary to some extent. As will be demonstrated next, physical coupling is significant to observe even in the presence of this regulator. This further stress the difficulty to mitigate risks of couplings. Such a regulator does not exists in our hardware test-case.

In addition, the evaluation kit used (SAM4C-EK) inhabits inherently quite a large capacitor

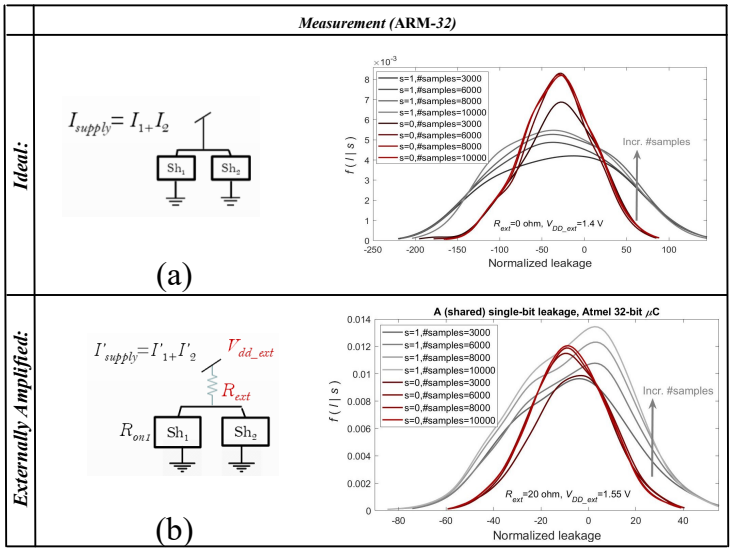

Figure 8: $f(l|s)$, $1 \cdot 10^6$ traces: (a) R_{ext}=0Ω (b) R_{ext}=20Ω.

bank (of 2.2 and 0.1μF) which filters the measured signal. We have removed all capacitors connected to the power supply. This can give even further inspection ability to instantaneous phenomena as typically exploited in side-channel attacks, which might explain the different results from [JS17]. So as for the rest of the paper (experiments and modeling), this section must be read as a first empirical confirmation that the risk of externally-amplified low-order leakages has a large extent and is observable on various implementations.

4.1 Leakage Distributions

In this (parallel) design, all the shares are processed simultaneously on the micro-controller and one sensitive bit at-a-time. The leakage-distribution conditioning a single-bit of a non-shared value (*i.e.*, $s[i]$) is demonstrated in Figure 8a-b as a function of R_{ext} (0Ω in 8a and 20Ω in 8b) and the number of samples used, #samples. (The plot is obtained thanks to a Kernel density estimation with an appropriate bandwidth).[6] The large agreement between these distributions and the simulated ones (in Figure 2a-b) is clear.

4.2 MCP-DPA

We performed a similar MCP-DPA analysis as for the hardware-based implementation. Figure 9 zooms-in to the relevant POI of the entire computation ($t \in \{13000..14200\}$ samples). The results are quite conclusive as well. The first moment with $R_{ext} = 0\Omega$ (Figure 9a) is borderline distinguishable with many close correlated keys and a maximum correlation value of 0.05 whereas with $R_{ext} = 20\Omega$ (Figure 9b) it is clearly distinguishable reaching a larger correlation of 0.08. Note that in this experiment, we utilized as little as $N_a = 0.7 \cdot 10^6$ samples, which in fact is not enough to consolidate the secret key from the second-order moment. However, it is possible to see that with the 0Ω resistor (Figure 9c) the 2^{nd}-order moment shows better results than with the 20Ω resistor (Figure 9d), considering the amplitudes of the false-keys of the 2^{nd}-order moment.

[6] The number of samples ranges from 1000 to 10000, where each leakage sample was averaged over 100 traces, totaling to 1e6 traces.

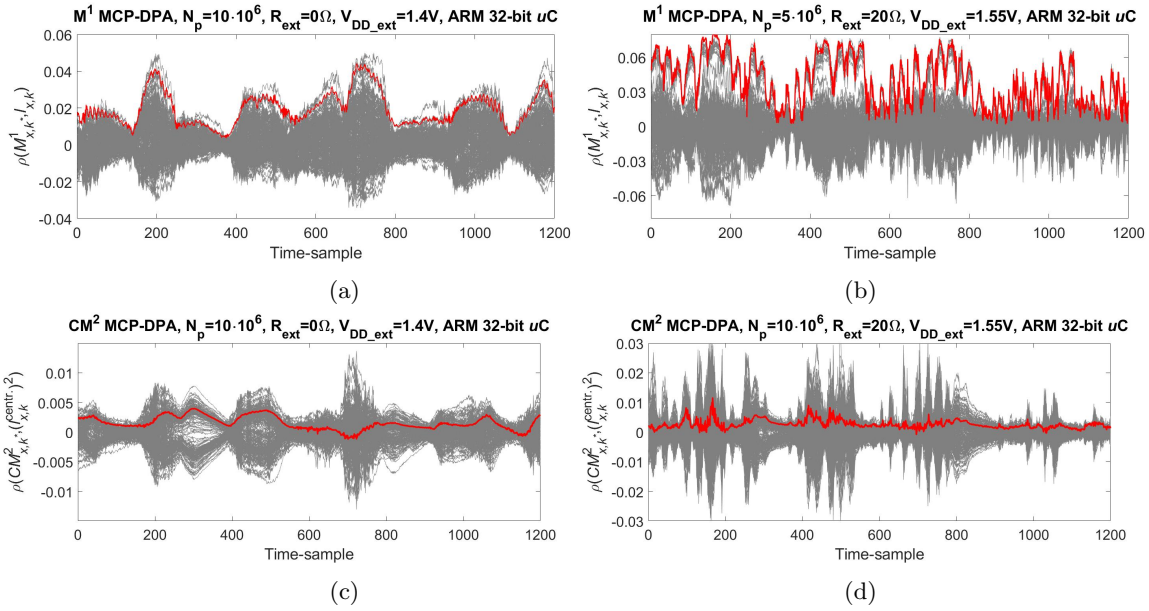

Figure 9: Atmel (ARM-32) parallel-Barthe *et al.* AES-SBOX 2-shares. MCP-DPA, with $\{N_p, N_a\} = \{10, 0.7\} \cdot 10^6$: $R_{ext} = 0\Omega, V_{DD\_ext} = 1.4V$: (a) M^1, (c) CM^2, and $R_{ext} = 20\Omega, V_{DD\_ext} = 1.55V$: (b) M^1, (d) CM^2.

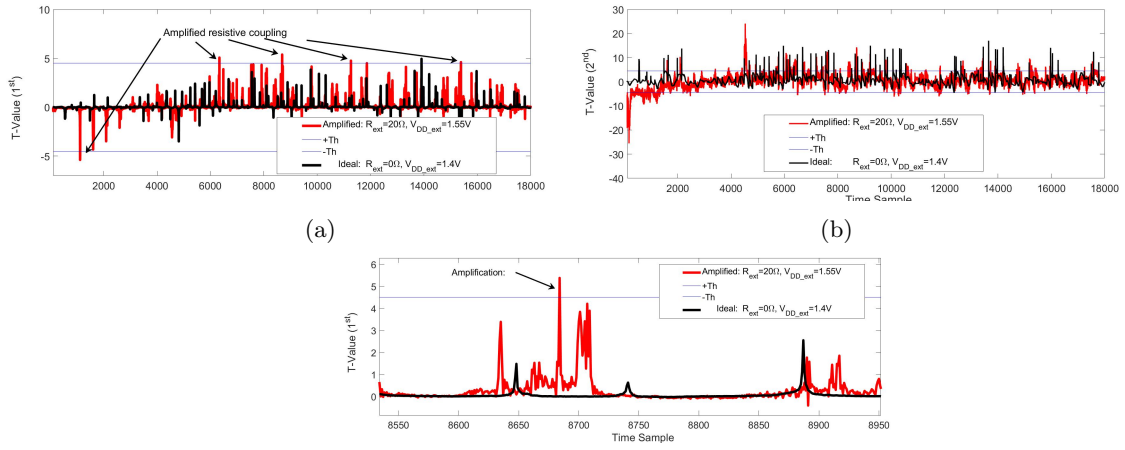

Figure 10: Atmel (ARM-32) parallel-Barthe *et al.* AES-SBOX 2-shares. Exemplary Fixed *vs.* Fixed 1^{st} and 2^{nd} order T-test for both $R_{ext} = 0\Omega, V_{DD\_ext} = 1.4V$ and $R_{ext} = 20\Omega, V_{DD\_ext} = 1.55V$: (a) Full trace 1^{st} order test,(b) Full trace 2^{nd} order test (c) Zoomed In to resistive dominated coupling.

4.2.1 Leakage Detection

We finally complete our findings with some detection results. As detailed in Subsection 1.3, we perform conventional (and high-order) T-tests based univariate detection. The sampling rate for the test was x10 the bandwidth of the design (more than the standard TVLA recommendation, x5). In Figure 10a, an exemplary fixed vs. fixed test result is shown. The red (or black) curves represent the 1^{st}-order T-test values with $R_{ext} =$

$20\Omega, V_{DD\_ext} = 1.55V$ (or $R_{ext} = 0\Omega, V_{DD\_ext} = 1.4V$). Standard thresholds are plotted in blue. Even though the test reveals sensitivity for the $R_{ext} = 0\Omega$ case, it is clear that with the $R_{ext} = 20\Omega$ case the amplification is effective. That is, multiple (positive and negative) threshold crossings are visible (this was shown over many tests with different fixed and random sets). Figure 10b shows the 2^{nd}-order test statistics. As expected, in this case both designs highly leak over numerous points. In Figure 10c, we finally take a closer look at intermediate leakage points: each leaky time-sample in the black curve is amplified in the red-curve (the time-shifts make sense due the parasitic effects of the amplification).

Those results are useful to emphasize the different factors which enable us to observe (in this work) such significant leakages as compared to [JS17], in which a similar device and architecture were used. First and foremost, in the investigations held in [JS17], the authors evaluate the device with nominal conditions (of voltage and minimal shunt resistance). Their work did not aim to account for physical couplings (although they indeed mention couplings – in their Section 4 – as a source of risk for further security reductions). Moreover, their analysis is focused on higher-orders (where for now we still have less intuition regarding couplings).

Concretely, the specific changes in setup that we capture and assume are critical for the observed changes are: (1) They utilized an active differential probe (more intrusive and noisy, as shown in Figure. 4(a-b)) whereas we utilized a low-noise passive inductive probe; (2) The device we evaluate was power-sourced by a separate (stable and low-noise) external power supply and large capacitors were removed from the evaluation board; (3) Special care was given to the conditions of the measurement setup, amplification circuitry, physical stability etc.; (4) In some scenarios, close to x2 of their sample-rate (1GS/s) and larger statistical sets were used (we used $20 \cdot 10^6$ traces at most).

5 Conclusions

We believe our results are important for both cryptographic hardware designers and evaluation laboratories, since they extend previous findings about setup manipulations and couplings in a way that can be systematically exploited by adversaries. For cryptographic engineers, it implies a new source of risk in the design of masked implementations, that is inherently connected to the physical layout of the target implementations and its electrical properties and power-network distribution, and is therefore more difficult to model/anticipate than other physical defaults like glitches or memory transitions. For evaluation laboratories, it implies that launching experiments with a single measurement setup may not be sufficient to evaluate the security order of a masked implementation, which may imply additional overheads in their evaluation processes.

Natural scopes for further research include the generalization of our findings to masked implementations with more shares and the better modeling/understanding of the physical effects exploited in order to design sound countermeasures. Several physical mechanisms which we target as important for future exploration are: amplification-aided capacitive elements; the trade-off between couplings and the SNR by reducing the power supply voltage or due to increased noise from the amplification circuitry; to better understand the couplings risk when the transistors operate in different modes (*e.g.*, in steady-state by leakage-power-analysis or in saturation mode). Regarding the generalization to larger number of shares, the main question is to evaluate how the reduction of the security order scales with d (*e.g.*, do the couplings imply a constant and systematic reduction of the security order independent of d or does the impact of couplings grow/vanish with d?). Regarding countermeasures, natural candidates are on-chip voltage regulators and randomizers which may limit the external amplification we put forward (but require a

re-design at the hardware level which is typically not available for masking implemented on commercial off-the-shelf devices).

Acknowledgments

François-Xavier Standaert is a senior associate researcher of the Belgian Fund for Scientific Research (FNRS-F.R.S.). This work has been funded in parts by the ERC project 724725 (acronym SWORD) and by the H2020 project REASSURE.

References

[BDF+17] Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, and Pierre-Yves Strub. Parallel implementations of masking schemes and the bounded moment leakage model. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 535–566, 2017.

[BGG+14] Josep Balasch, Benedikt Gierlichs, Vincent Grosso, Oscar Reparaz, and François-Xavier Standaert. On the cost of lazy engineering for masked software implementations. In Marc Joye and Amir Moradi, editors, *Smart Card Research and Advanced Applications - 13th International Conference, CARDIS 2014, Paris, France, November 5-7, 2014. Revised Selected Papers*, volume 8968 of *Lecture Notes in Computer Science*, pages 64–81. Springer, 2014.

[CBG+17] Thomas De Cnudde, Begül Bilgin, Benedikt Gierlichs, Ventzislav Nikov, Svetla Nikova, and Vincent Rijmen. Does coupling affect the security of masked implementations? In *Constructive Side-Channel Analysis and Secure Design - 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers*, pages 1–18, 2017.

[CEM18] Thomas De Cnudde, Maik Ender, and Amir Moradi. Hardware masking, revisited. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(2):123–148, 2018.

[CGP+12] Jean-Sébastien Coron, Christophe Giraud, Emmanuel Prouff, Soline Renner, Matthieu Rivain, and Praveen Kumar Vadnala. Conversion of security proofs from one leakage model to another: A new issue. In Werner Schindler and Sorin A. Huss, editors, *Constructive Side-Channel Analysis and Secure Design - Third International Workshop, COSADE 2012, Darmstadt, Germany, May 3-4, 2012. Proceedings*, volume 7275 of *Lecture Notes in Computer Science*, pages 69–81. Springer, 2012.

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer, 1999.

[CMG+] Jeremy Cooper, Elke De Mulder, Gilbert Goodwill, Josh Jaffe, Gary Kenworthy, and Pankaj Rohatgi. Test vector leakage assessment (TVLA) methodology in practice (extended abstract). ICMC 2013.

[DFS15] Alexandre Duc, Sebastian Faust, and François-Xavier Standaert. Making masking security proofs concrete - or how to evaluate the security of any leaking device. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 401–429. Springer, 2015.

[DS16] François Durvaux and François-Xavier Standaert. From improved leakage detection to the detection of points of interests in leakage traces. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 240–262. Springer, 2016.

[FGP+18] Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, and François-Xavier Standaert. Composable masking schemes in the presence of physical defaults & the robust probing model. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(3):89–120, 2018.

[GMK17] Hannes Groß, Stefan Mangard, and Thomas Korak. An efficient side-channel protected AES implementation with arbitrary protection order. In Helena Handschuh, editor, *Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings*, volume 10159 of *Lecture Notes in Computer Science*, pages 95–112. Springer, 2017.

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In *Annual International Cryptology Conference*, pages 463–481. Springer, 2003.

[JS17] Anthony Journault and François-Xavier Standaert. Very high order masking: Efficient implementation and security evaluation. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 623–643. Springer, 2017.

[MM13] Amir Moradi and Oliver Mischke. On the simplicity of converting leakages from multivariate to univariate - (case study of a glitch-resistant masking scheme). In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2013.

[MPG05] Stefan Mangard, Thomas Popp, and Berndt M. Gammel. Side-channel leakage of masked CMOS gates. In Alfred Menezes, editor, *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*, volume 3376 of *Lecture Notes in Computer Science*, pages 351–365. Springer, 2005.

[MS16] Amir Moradi and François-Xavier Standaert. Moments-correlating DPA. In Begül Bilgin, Svetla Nikova, and Vincent Rijmen, editors, *Proceedings of the ACM Workshop on Theory of Implementation Security, TIS@CCS 2016 Vienna, Austria, October, 2016*, pages 5–15. ACM, 2016.

[NRS11] Svetla Nikova, Vincent Rijmen, and Martin Schläffer. Secure hardware implementation of nonlinear functions in the presence of glitches. *J. Cryptology*, 24(2):292–321, 2011.

[PR13] Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 142–159. Springer, 2013.

[PS17] Santos Merino Del Pozo and François-Xavier Standaert. Getting the most out of leakage detection - statistical tools and measurement setups hand in hand. In *Constructive Side-Channel Analysis and Secure Design - 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers*, pages 264–281, 2017.

[RCN02] Jan M Rabaey, Anantha P Chandrakasan, and Borivoje Nikolic. *Digital integrated circuits*, volume 2. Prentice hall Englewood Cliffs, 2002.

[SM16] Tobias Schneider and Amir Moradi. Leakage assessment methodology - extended version. *J. Cryptographic Engineering*, 6(2):85–99, 2016.

[Wel47] Bernard L Welch. The generalization ofstudent's' problem when several different population variances are involved. *Biometrika*, 34(1/2):28–35, 1947.

Appendix A: 2^{nd}-order MCP-DPA results

In this Appendix we support the results of the main manuscript body with 2^{nd}-order MCP-DPA attack results of the AES DOM of order 2. These results appear here to make the main contribution in the manuscript body more accessible and less over-shadowed by sometimes superfluous information. As discussed above, and shown by the results (Figure 11 in the time domain and Figure 12 *vs.* the number of traces):

- For the same data-complexity as of the 1^{st}-order attacks it is still quite hard to extract information from the 2^{nd} order, as anticipated for attack based approach.
- Amplification (right columns in the figures) does not disclose the secret-keys nor substantially increase correlation values. Which fits our model from Section 2.

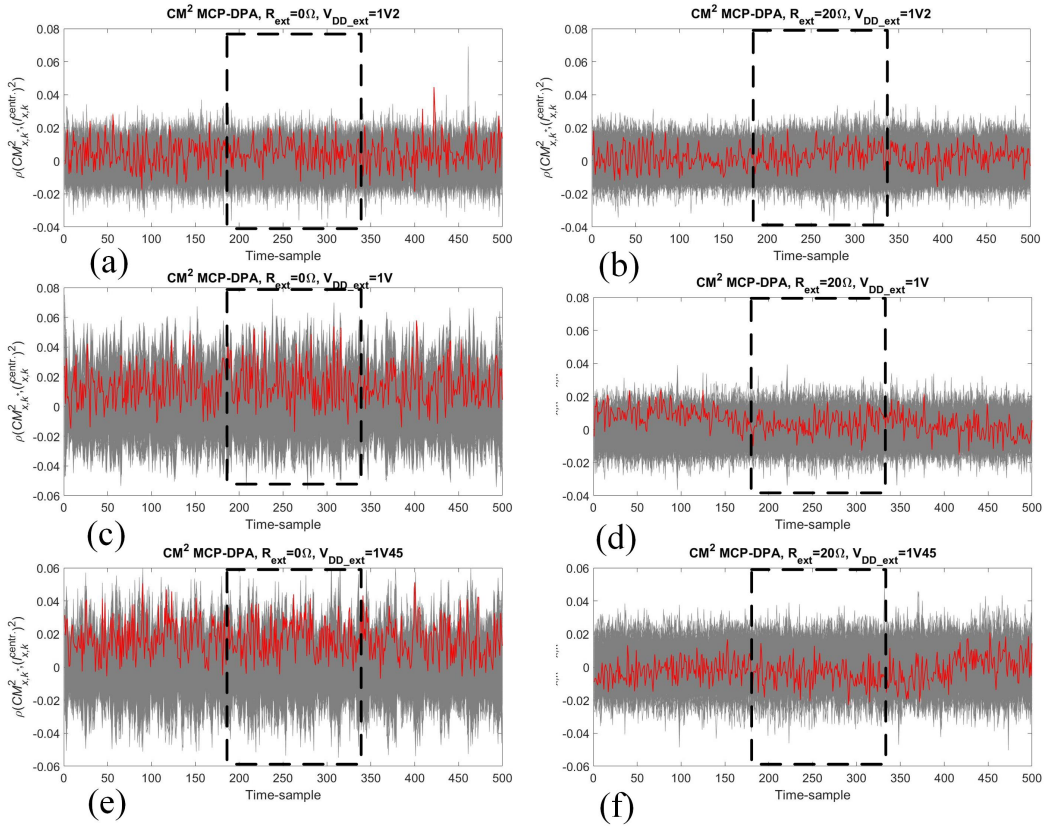

Figure 11: AES DOM Order 2. 1^{st}-order MCP-DPA correlation *vs.* time: $V_{DD\_ext} = 1.2V$ (nominal): (a) $R_{ext} = 0\Omega$ (b) $R_{ext} = 20\Omega$. $V_{DD\_ext} = 1.45V$: (c) $R_{ext} = 0\Omega$, (d) $R_{ext} = 20\Omega$.$V_{DD\_ext} = 1V$: (c) $R_{ext} = 0\Omega$, (d) $R_{ext} = 20\Omega$.

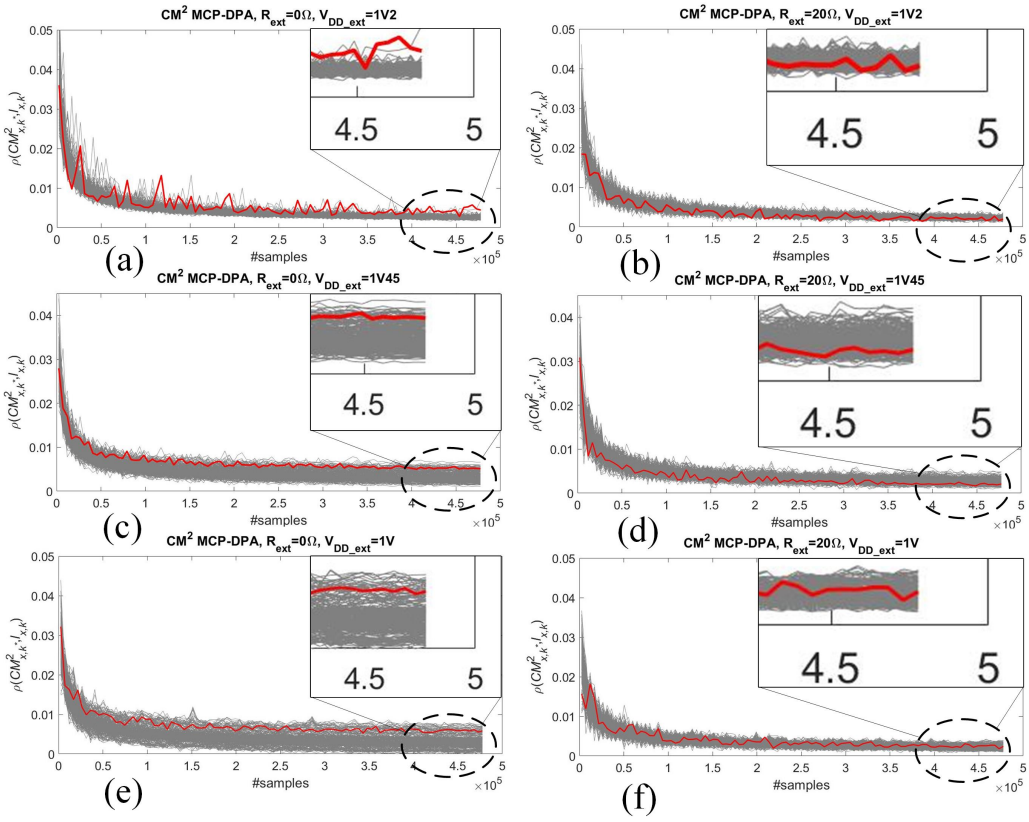

Figure 12: AES DoM Order 2. 2^{st}-order MCP-DPA correlation *vs*. the number of traces: $V_{DD\_ext} = 1.2V$ (nominal): (a) $R_{ext} = 0\Omega$ (b) $R_{ext} = 20\Omega$. $V_{DD\_ext} = 1.45V$: (c) $R_{ext} = 0\Omega$, (d) $R_{ext} = 20\Omega$.$V_{DD\_ext} = 1V$: (c) $R_{ext} = 0\Omega$, (d) $R_{ext} = 20\Omega$.