Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks

Maxime Nassar[1,2], Sylvain Guilley[2] and Jean-Luc Danger[2]

Email: {nassar,guilley,danger}@TELECOM-ParisTech.fr

[1] Bull TrustWay, Rue Jean Jaurès, B.P. 68,
78 340 Les Clayes-sous-Bois, France.
[2] Institut TELECOM / TELECOM ParisTech, CNRS LTCI (UMR 5141),
46 rue Barrault, 75 634 Paris Cedex, France.

Abstract. Several types of countermeasures against side-channel attacks are known. The one called masking is of great interest since it can be applied to any protocol and/or algorithm, without nonetheless requiring special care at the implementation level. Masking countermeasures are usually studied with the maximal possible entropy for the masks. However, in practice, this requirement can be viewed as too costly. It is thus relevant to study how the security evolves when the number of mask values decreases.
In this article, we study a first-order masking scheme, that makes use of one n-bit mask taking values in a strict subset of $\mathbb{F}_2^n$. For a given entropy budget, we show that the security does depend on the choice of the mask values. More specifically, we explore the space of mask sets that resist first- and second-order correlation analysis (CPA and 2O-CPA), using exhaustive search for word size $n \leqslant 5$ bit and a SAT-solver for n up to 8 bit. We notably show that it is possible to protect algorithms against both CPA and 2O-CPA such as AES with only 12 mask values. If the general trend is that more entropy means less leakage, some particular mask subsets can leak less (or on the contrary leak remarkably more). Additionally, we exhibit such mask subsets that allows for a minimal leakage.

Keywords: side-channel attacks (SCAs), masking countermeasure, non-injective leakage function, correlation power analysis (CPA), second-order CPA (2O-CPA), mutual information analysis (MIA), entropy *vs* security tradeoff, SAT-solvers.

1 Introduction

Implementations of cryptographic algorithms are vulnerable to so-called side-channel attacks. They consist in analysing the leakage of the device during its

operation, in a view to relate it to the internal data it processes. The prerequisite of the attack is a physical access to the targeted device. The attacker thus measures some analog quantity, such as the power [12] or the radiated field [7]. Several ways to resist side-channel have been suggested. They are often referred to as "countermeasures". High level countermeasures intend to deny the exploitation of the leakage by updating the secrets on a regular basis. It results in leakage-resilient protocols. They are nice as they indeed manage to thwart any kind of side-channel attacks, but require that the user adopts a new protocol. Therefore, other countermeasures have been devised that operate at a lower level, without altering the protocol. Typically, hiding strategies aim at leaking a constant side-channel. Although relevant from a theoretical perspective, this approach nonetheless requires physical hypotheses about resources indiscernibility that are not trivial to meet. Masking is another option, that is transparent to the user and does not demand any special backend balance. We therefore focus on this countermeasure. It consists in computing on data whose representation is randomized. The more entropy is used, the more secure the countermeasure can be (if the entropy is used intelligently). In this paper, we rather investigate the effect of the reduction of the entropy on the security. Moreover, we concentrate on a first-order masking scheme, *i.e.* that uses only one mask, that takes a restricted number of values.

The rest of the article is structured as follows. The studied countermeasure, called the rotating tables, is described in Sec. 2. This section introduces the leakage model considered in the sequel, and defines the notion of leakage and security metrics. The rotating tables countermeasure is then evaluated in the formal framework presented in [24]. Namely, its leakage is characterized in Sec. 3 and its resistance against CPA and 2O-CPA is quantified in Sec. 4. It is shown in the section that it is possible to reduce the leakage at a constant budget for masks of $n = 5$ bits. Masks of larger bitwidth, such as $n = 8$, are studied in Sec. 5. The exploration is conducted with the help of a SAT-solver. Conclusions and perspectives are in Sec. 6. Some illustrations and long proofs are relegated to appendix.

2 Description of the Rotating Tables Countermeasure

The goal of this section is to introduce the leakage model that will be studied next, and to explain why the cost of the countermeasure can be greatly reduced by limiting the mask values. We first give in subsection 2.1 a brief overview of a masking countermeasure with randomly selected precomputed tables. Then, in subsection 2.2, the leakage of this countermeasure is derived.

2.1 Rationale

Unprotected implementations are vulnerable to SCAs because they manipulate sensitive variables, that leak some physical quantities that depend somehow on them. Therefore, in a Boolean masking scheme, they are replaced by the

exclusive-or (XOR) with random variables. Let us take the example of a first-order masking scheme, where one mask m goes along with one the sensitive variable z. The bitvectors z and m have the same size, namely n bits. We call $\mathcal{S}_0 \doteq z \oplus m$ and $\mathcal{S}_1 \doteq m$ the two shares. The preconditions on the shares is that the sensitive variable can be recovered by XORing them: $Z = \mathcal{S}_0 \oplus \mathcal{S}_1$. The linear operations with respect to the XOR are straightforward. Indeed, to compute a linear operation S on z using the shares, it suffices to apply S on each share. As a matter of fact, it is trivial to check the following post-condition: $S(z) = S(\mathcal{S}_0) \oplus S(\mathcal{S}_1)$. Nonetheless, if S is a non-linear operation, this equality does not hold, and it is necessary to use judiciously both shares to be able to compute $S(z)$. This operation is costly in general [26] (unless some algebraic properties of the non-linear function S can be taken advantage of [19]) and error-prone [13].

Therefore, it is sometimes relevant to compute on only one share, namely $\mathcal{S}_0$. This share traverses the linear parts of the algorithm, and is all-in-one:

1. demasked at the entrance of a non-linear function S,
2. applied S, and
3. remasked so as to propagate through the next linear part.

For sure, the demasking and remasking operations are very sensitive. Nonetheless, the composition of the three operations can be tabulated: a table, such as a ROM block, conceals the intermediate variables (as in whitebox cryptography). Indeed, in cryptography, the non-linear function S will typically be a substitution box (*aka* sbox), that is hard to compute analytically, thus better saved in memory provided there are enough resources to store it. In this case, the intermediate variables never appear. In some sense, the computation is homomorphic in the masked representation, the mask refresh being done within the sboxes. For more details on the implementation of this table, we refer the interested reader to [17, Sec. 2], and more specifically to the paragraphs that concern the "sbox secure calculation".

In a platform that embarks an operating system, a task can be scheduled to recompute the masked sboxes $z \mapsto m_{\text{out}} \oplus S(z \oplus m_{\text{in}})$ periodically. Nonetheless, some embedded systems cannot afford a supervision for the masks update. Also, this process of mask refresh is itself sensitive, and should be protected adequately. In a view to relieve this constraint, one can get rid off the recomputation, and use masked sboxes that had been entered initially. This option is especially favorable for the cryptosystem that reuses several times the same sbox in each round (such as AES). The goal is not to create a security by obscurity solution. Indeed, the masks m_{in} and m_{out} can be disclosed (*i.e.* made public) without compromising the countermeasure[3]. The randomness that characterizes the masking scheme will result from the choice of the sbox for each computation. Let us take the example of a hardware implementation of AES that computes one round per

[3] This is a usual assumption in masking. Let us take the example of the first-order additive Boolean masking. The domain of definition of the masks is public: it is the whole $\mathbb{F}_2^n$. However, the choice of a mask associated for one encryption is private.

clock cycle. Sixteen masked $S[i]$ sboxes, $i \in [\![0, 15]\!]$, must be available in parallel. We assume that the masks $m_{\text{in}}[i]$ and $m_{\text{out}}[i]$ satisfy this chaining relationship: $\forall i \in [\![0, 15]\!], m_{\text{out}}[i] = m_{\text{in}}[i + 1 \mod 16]$. Then the computation of an AES-128 can start by drawing a random number $r \in [\![0, 15]\!]$; the algorithm then invokes $S[j + k \mod 16]$ to compute the sbox of byte $j \in [\![0, 16]\!]$ of the state at round $k \in [\![0, 9]\!]$. Because of the chaining property, the linear parts of AES in-between the sboxes are consistently masked and demasked with the same mask. This ensures the correctness of the AES encryption implemented with the rotating sboxes countermeasures.

The overhead of the countermeasure is directly linked to the number of masks[4]. Indeed, more masks mean more memory to store the masked tables. Also, the more tables, the more multiplexing logic to access them, which increases the critical path in a hardware implementation. Thus, in the sequel, we endeavour to reduce the number of masks, while nonetheless keeping an acceptable security level.

2.2 Modelization

Hardware implementations of AES are preferably attacked on the last round. Indeed, it is possible to guess one byte, noted y of the round 9 from one byte of the ciphertext x simply by guessing one byte of the last round key, because there is no MixColumns operation in the last round. The leakage is a function of the distance between y and x, *i.e.* $x \oplus y$ [25]. Now, when the rotating tables countermeasure is applied, the value y is actually replaced by $y \oplus m$, where m is one of the 16 mask values. The sensitive variable is the value $x \oplus y$, noted z. In a view to introduce statistical notions, we denote by capital letters (Z and M) the random variables and by small letters (z and m) their realizations. The leakage function thus has the form:

$$\mathcal{L}(Z, M) = \mathscr{L}(Z \oplus M) \ . \tag{1}$$

In this expression, Z and M are n-bit vectors, *i.e.* live in $\mathbb{F}_2^n$. Notice that if the leakage was, at least partially, in values (as opposed to distances), then the model of Eqn. (1) would still hold; instead of having Z represent the distance between Y and X, it simply represent Y, that has the same uniform distribution. Thus, the countermeasure protects at the same time between attacks that target the sensitive variable or its distance. This feature is very interesting in practice, because it seems that both leaking modalities coexist in some devices, as illustrated for instance in [15]. The leakage function $\mathscr{L} : \mathbb{F}_2^n \to \mathbb{R}$ depends on the hardware. In a conservative perspective, $\mathscr{L}$ is assumed to be bijective. This choice is the most favorable to the attacker, and is thus considered in the leakage estimation. Now, in practice, the leakage functions are not bijective. The canonical example

[4] Notice that in the rest of the article, we have only one masking variable, that takes few values. We sometimes refer to them as the "number of masks"; we attract the reader's attention on the fact this expression shall not be confused with "multi-masks" countermeasures, also known as "high-order" masking schemes.

is that of the Hamming weight leakage, where each bit of $Z \oplus M$ dissipate the same. Let us denote by x_i the component $i \in [\![1, n]\!]$ of $x \in \mathbb{F}_2^n$. The Hamming weight of x is expressed as $\mathsf{HW}[x] = \sum_{i=1}^{n} x_i$. The countermeasure demands that the leakage $\mathscr{L}$ be as close as possible to the Hamming weight. Indeed, it is the indiscernibility of the bits of Z that allows to reduce the entropy of the masking.

We underline that this section was not meant to introduce a new countermeasure (the rotating sboxes). Indeed, this pragmatic countermeasure is already well known and adopted in the industry [9,16]. We simply wished to provide the reader with a pedagogical introduction to the leakage function of Eqn. (1). This function will now be studied formally, as per the guidelines presented in [24]. More precisely, we employ:

- The mutual information between the $\mathcal{L}(Z, M)$ and the sensitive variable Z with $\mathscr{L}$ bijective as a leakage metric. This quantity is noted $\mathsf{I}[\mathcal{L}(Z, M); Z]$ — basic definitions of information theory applied to SCAs can be found in [24] — and referred to as "mutual information as a metric" (MIM [27]). We recall that a leakage metric points out vulnerabilities, that could in practice happen not be exploited by an attacker.
- Security metrics to quantify the easiness to actually turn a leakage into a successful attack. In this case, we will focus on $\mathscr{L} = \mathsf{HW}$. First of all, the optimal correlation between $\mathsf{HW}[Z \oplus M]$ and Z is considered a metric. It is traditionally called the (first-order) correlation power analysis, or CPA [4]. But CPA can be defeated easily with only two mask values. Therefore it is important to consider higher-order CPA (HO-CPA), and notably the second-order CPA, also abridged 2O-CPA [29]. However, CPA and 2O-CPA exploit only the first two moments of the distribution of $\mathcal{L}(Z, M)$. Therefore, we also use a second security metric, namely the mutual information. It is known in the literature as MIA [3]. Security-wise, our goal is to minimize the first- and second-order correlation coefficients and the MIA.

3 Information Theoretic Evaluation of the Countermeasure

The specificity of this study is to consider masks M that are not completely entropic. Thus, the probability $\mathsf{P}[M = m]$ depends on m. Our target is to restrict to a relevant subset of the masks uniformly, that is every mask is used with the same probability. We call $\mathcal{M} \subseteq \mathbb{F}_2^n$ the set of masks actually used. Thus:

$$\mathsf{P}[M = m] = \begin{cases} 1/\mathsf{Card}[\mathcal{M}] & \text{if } m \in \mathcal{M}, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

We also write this probability law $M \sim \mathcal{U}(\mathcal{M})$. From an information theoretic point of view, we can characterize the entropy of M. By definition, $\mathsf{H}[M] = -\sum_{m \in \mathcal{M}} \frac{1}{\mathsf{Card}[\mathcal{M}]} \log_2 \frac{1}{\mathsf{Card}[\mathcal{M}]} = \log_2 \mathsf{Card}[\mathcal{M}]$ bit. The minimal number of masks is 1, which corresponds to the absence of countermeasure (take $M = 0$ in

Eqn. (1)). At the opposite, when all the 2^n masks are used, the countermeasure is optimal.

Eventually, we assume that the attacker does not conduct a chosen message attack, *i.e.* $Z \sim \mathcal{U}(\mathbb{F}_2^n)$. We notice that even if the attacker cannot actually choose the messages, she has nonetheless the possibility to discard some messages so as to artificially bias the side-channel attack. But a priori, the attacker does not know which plaintext Z to favor. A biased side-channel attack has been detailed in [11,28]. However, this attack is adaptative, and thus requires that a breach be already found. Nonetheless, in our context, we target the protection of the secret at the early stages of the attack; the attacker still does not have any clue about the most likely hypotheses for the secret. This hypothesis is called the *non-adaptive known plaintext model* in [24].

Whatever the actual leakage function $\mathscr{L}$, $\mathsf{I}[\mathscr{L}(Z \oplus M); Z] = 0$ if $\mathsf{H}[M] = n$ bit (or equivalently, if $M \sim \mathcal{U}(\mathbb{F}_2^n)$). So with all the masks, the countermeasure is perfect.

If $\mathscr{L}$ is bijective (*e.g.* $\mathscr{L} = \mathsf{Id}$), then $\mathsf{I}[\mathscr{L}(Z \oplus M); Z] = n - \mathsf{H}[M]$. This results directly from the observation that:

- $\mathsf{H}[\mathscr{L}(Z \oplus M)] = \mathsf{H}[\mathscr{L}(Z)] = n$ bit, since $Z \sim \mathcal{U}(\mathbb{F}_2^n)$, and
- $\mathsf{H}[\mathscr{L}(Z \oplus M) \mid Z] = \mathsf{H}[M]$ bit because Z and M are independent.

We notice that this quantity is independent of the exact $\mathcal{M}$, provided $\mathsf{Card}[\mathcal{M}]$ is fixed. This means that degrading the countermeasure (*i.e.* choosing $\mathsf{Card}[\mathcal{M}] < 2^n$) introduces a vulnerability, while decreasing the cost.

Now, it can checked to which extent this vulnerability is exploitable, considering a realistic leakage function. Specifically, it can be shown that if $\mathscr{L}$ is not injective, then the MIA metric $\mathsf{I}[\mathscr{L}(Z \oplus M); Z]$ depends on $\mathcal{M}$. Appendix A provides an example. More precisely, when $\mathcal{M}$ as two (complementary) elements, then the MIA is independent of $\mathcal{M}$ (refer to appendix B). But when $\mathcal{M}$ is made up of strictly more than two masks, the MIA depends on $\mathcal{M}$. For example, on $n = 8$ bits, with $\mathscr{L} = \mathsf{HW}$,

- $\mathsf{I}[\mathscr{L}(Z \oplus M); Z] = 1.42701$ bit if $\mathcal{M} = \{\texttt{0x00}, \texttt{0x0f}, \texttt{0xf0}, \texttt{0xff}\}$, but
- $\mathsf{I}[\mathscr{L}(Z \oplus M); Z] = 0.73733$ bit if $\mathcal{M} = \{\texttt{0x00}, \texttt{0x01}, \texttt{0xfe}, \texttt{0xff}\}$.

Thus, it is relevant to search for mask sets, at a constant budget (*i.e.* for a given $\mathsf{Card}[\mathcal{M}]$), that minimize the mutual information $\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z]$. Nonetheless, without a method, it is not obvious to conduct a reasoned search. Indeed, the default solution is to draw at random one mask set $\mathcal{M}$ and to compute $\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z]$. It is immediate to see that such method will indeed provide solutions harder to attack using MIA than the others, but that will maybe fail in front of other less sophisticated attacks. Typically, $\mathcal{M}$ sets only constrained by their cardinality are likely to yield functions trivially attackable by CPA. We therefore propose the following method:

- First mask sets $\mathcal{M}$ that resist first- and second-order correlation attacks (*i.e.* CPA and 2O-CPA, the easiest attacks against single-masked countermeasures) are found. This is the topic of Sec. 4.

– Then, amongst these solutions, those minimizing the risk of MIA are selected. Section 5 specifically analyses this point (already quickly discussed in Sec. 4.5).

Another argument to focus primarily on CPA and 2O-CPA is that they require in practice less side-channel measurements to succeed the attack than MIA. Indeed, MIA, as well all other information theoretic-based attacks (*e.g.* template attacks [6] and stochastic attacks [20]), need to estimate conditional probability functions, which needs many traces [8]. Also, from the certification standpoint, the common criteria [1] demand that the implemented countermeasures resist "state-of-the-art" attacks [2]. Now, CPA and 2O-CPA are much more studied in the information technology security evaluation facilities (ITSEFs) than information theoretic attacks.

4 Security against CPA and 2O-CPA

The average of the leakage function given in Eqn. (1) depends on $\mathscr{L} : \mathbb{F}_2^n \to \mathbb{R}$. As already mentioned, to conduct exact computations and to match with realistic leakage functions observed in practice, we opt for the Hamming weight ($\mathscr{L} = \mathsf{HW}$). Thus the average of leakage function, noted $\mathsf{E}\mathcal{L}(Z, M)$, is equal to:

$$\mathsf{E}\ \mathsf{HW}[Z \oplus M] = \frac{1}{\mathsf{Card}[\mathcal{M}]} \sum_{m \in \mathcal{M}} \frac{1}{2^n} \sum_{z \in \mathbb{F}_2^n} \mathsf{HW}[z \oplus m] = \frac{1}{\mathsf{Card}[\mathcal{M}]} \sum_{m \in \mathcal{M}} \frac{n}{2} = \frac{n}{2}\,. \tag{2}$$

Against HO-CPA of order $d \geqslant 1$, the most powerful attacker correlates her guesses about the sensitive variable with the optimal function [18] defined as:

$$\begin{aligned} f_{\mathrm{opt}}^{(d)}(z) &\doteq \mathsf{E}\left(\left(\mathcal{L}(Z, M) - \mathsf{E}\mathcal{L}(Z, M)\right)^d \mid Z = z \right) \\ &= \mathsf{E}\left(\left(\mathsf{HW}[Z \oplus M] - \frac{n}{2}\right)^d \mid Z = z \right) \\ &= \frac{1}{\mathsf{Card}[\mathcal{M}]} \sum_{m \in \mathcal{M}} \left(\frac{-1}{2} \sum_{i=1}^{n} (-1)^{(z \oplus m)_i} \right)^d , \end{aligned} \tag{3}$$

because if $b \in \{0, 1\}$, then $b - \frac{1}{2} = -\frac{1}{2}(-1)^b$. Recall that the rotating tables countermeasure uses only one mask variable M, and thus leaks at only one date (*i.e.* for a given timing sample). In this context, HO-CPA consists in studying the linear dependency between the d-th moments of the leakage classes and the optimal function $f_{\mathrm{opt}}^{(d)}(z)$ of the sensitive variable z.

For the designer of the countermeasure, the objective is to make Eqn. (3) independent of z. There is always a solution that consists in choosing $\mathcal{M} = \mathbb{F}_2^n$. Nonetheless, with $\mathsf{Card}[\mathcal{M}] < 2^n$, the existence of solutions is a priori not trivial. In this case, if is impossible to find masks that keep $f_{\mathrm{opt}}^{(d)}(z)$ (defined in Eqn. (3))

independent from z, the secondary goal is to minimize the correlation coefficient:

$$\rho_{\text{opt}}^{(d)} \doteq \frac{\mathsf{Var}\left(f_{\text{opt}}^{(d)}(Z)\right)}{\mathsf{Var}\left(\left(\mathcal{L}(Z,M) - \mathsf{E}\mathcal{L}(Z,M)\right)^d\right)} = \frac{\mathsf{Var}\left(\mathsf{E}\left(\left(\mathsf{HW}[Z \oplus M] - \frac{n}{2}\right)^d \mid Z\right)\right)}{\mathsf{Var}\left(\left(\mathsf{HW}[Z \oplus M] - \frac{n}{2}\right)^d\right)}. \tag{4}$$

In this equation, Var represents the variance operator, defined on a random variable X as $\mathsf{Var}(X) \doteq \mathsf{E}\,(X - \mathsf{E}X)^2$.

In the two next subsections 4.1 and 4.2, the analytical expression of Eqn. (4) is derived. Then these expressions are unified in subsection 4.3 by replacing the notion of subset $\mathcal{M}$ by an indicator function f. The sets of masks that completely allow to deny CPA and 2O-CPA are given exhaustively in subsection 4.4 for $n = 4$ and in subsection 4.5 for $n = 5$.

4.1 Resistance against First-Order Correlation Attacks

As shown in appendix C.1, when $d = 1$, Eqn. (4) is equal to:

$$\rho_{\text{opt}}^{(1)} = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{1}{\mathsf{Card}[\mathcal{M}]}\sum_{m\in\mathcal{M}}(-1)^{m_i}\right)^2. \tag{5}$$

This correlation $\rho_{\text{opt}}^{(1)}$ can be equal to zero if and only if (iff), for all $i \in [\![1, n]\!]$, $\mathsf{E}M_i = 1/2$. This means that the masks are balanced. It is possible to find such masks iff $\mathsf{Card}[\mathcal{M}]$ is a multiple of two. A construction consists in building a set of masks by adding a new mask and its complement. Conversely, in a set containing an odd number of different masks, it is impossible to as many ones as zeros for any component. For instance, we illustrate how to generate balanced sets of masks in the case $n = 4$ in Tab. 1.

A trivial example consists in taking two masks, m and $\neg m$ (such as `0x00` and `0xff` on $n = 8$ bits). This is sufficient to thwart first-order attacks. At the opposite, without mask ($\mathcal{M}$ is equal to the singleton $\{\texttt{0x00}\}$) or with a single mask ($\mathcal{M} = \{m\}$, whatever $m \in \mathbb{F}_2^n$), the correlation coefficient reaches its maximum (*i.e.* $+1$, because Eqn. (4) considers a correlation in absolute value).

4.2 Resistance against Second-Order Correlation Attacks

As shown in appendix C.2, when $d = 2$, Eqn. (4) is equal to:

$$\rho_{\text{opt}}^{(2)} = \frac{1}{n(n-1)}\left(\frac{1}{\mathsf{Card}[\mathcal{M}]^2}\sum_{(m,m')\in\mathcal{M}^2}\left(\sum_{i=1}^{n}(-1)^{(m\oplus m')_i}\right)^2 - n\right). \tag{6}$$

As an illustration, we show in Tab. 2 the optimal correlation coefficients of order 1 and 2 for the masks sets of Tab. 1 ($n = 4$ bit). We have added a column (the last one), for $\mathscr{L} = \mathsf{Id}$; also, in the last row, we have included a constant

Table 1. Mask sets $\mathcal{M}$ that make the masking countermeasure immune to first order CPA. The masks go by pair, symmetrically with the middle of the table.

	$\mathsf{Card}[\mathcal{M}] = 2^4$	$\mathsf{Card}[\mathcal{M}] = 2^3$	$\mathsf{Card}[\mathcal{M}] = 2^2$	$\mathsf{Card}[\mathcal{M}] = 2^1$
$\mathcal{M}$	0000	0000	0000	0000
	0001			
	0010			
	0011	0011	0011	
	0100	0100		
	0101			
	0110			
	0111	0111		
	1000	1000		
	1001			
	1010			
	1011	1011		
	1100	1100	1100	
	1101			
	1110			
	1111	1111	1111	1111

masking (unprotected implementation), which serves as a reference. In this table, we see a simple law: the more entropy, the less leakage in HW and Id. But this is specific to the example of $\mathcal{M}$ taken here. In Sect. 4.4, we will see the relationship is not that trivial. Especially, it is clear that the heuristic construction of Tab. 1 is not resistance against second-order attacks.

Table 2. Security metrics for the masks sets of Tab. 1 and the singleton.

$\mathsf{Card}[\mathcal{M}]$	$\mathsf{H}[M]$	$\rho^{(1)}_{\mathrm{opt}}$	$\rho^{(2)}_{\mathrm{opt}}$	$\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z]$	$\mathsf{I}[Z \oplus M; Z]$
2^4	4	0	0	0	0
2^3	3	0	0.166667	0.15564	1
2^2	2	0	0.333333	1.15564	2
2^1	1	0	1	1.40564	3
2^0	0	1	1	2.03064	4

4.3 Expression of $\rho_{\text{opt}}^{(1,2)}$ as a Function of an Indicator f

The expressions of $\rho_{\text{opt}}^{(1)}$ and $\rho_{\text{opt}}^{(2)}$ (altogether referred to as $\rho_{\text{opt}}^{(1,2)}$) defined in Eqn. (5) and (6) lay a mathematical ground to search for suitable $\mathcal{M}$. Nonetheless, these equations remain at the set-theory level. To simplify the problem, we introduce the Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, defined as: $\forall m \in \mathbb{F}_2^n, f(m) = 1 \Leftrightarrow m \in \mathcal{M}$. Then, we can simply replace "$\sum_{m\in\mathcal{M}}$" by "$\sum_{m\in\mathbb{F}_2^n} f(m)$" in the equations previously established.

The Fourier transform $\hat{f} : \mathbb{F}_2^n \to \mathbb{Z}$ of the Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined as $\forall a \in \mathbb{F}_2^n, \hat{f}(a) \doteq \sum_{m\in\mathbb{F}_2^n} f(m)(-1)^{a\cdot m}$. It allows for instance to write $\mathsf{Card}[\mathcal{M}] = \sum_{m\in\mathcal{M}} 1 = \sum_{m\in\mathbb{F}_2^n} f(m) = \hat{f}(0)$. Recall $\mathsf{Card}[\mathcal{M}] \in [\![1, 2^n]\!]$, hence $\hat{f}(0) > 0$.

Then Eqn. (5) rewrites:

$$\rho_{\text{opt}}^{(1)} = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{\hat{f}(e_i)}{\hat{f}(0)}\right)^2, \tag{7}$$

where e_i are the canonical basis vectors $(0, \cdots, 0, 1, 0, \cdots, 0)$, the unique 1 laying at position i.

Also, Eqn. (6) rewrites:

$$\begin{aligned}\rho_{\text{opt}}^{(2)} &= \frac{1}{n(n-1)}\sum_{(i,i')\in[\![1,n]\!]^2}\left(\left(\frac{\hat{f}(e_i\oplus e_{i'})}{\hat{f}(0)}\right)^2 - n\right)\\ &= \frac{1}{n(n-1)}\sum_{\substack{(i,i')\in[\![1,n]\!]^2\\ i\neq i'}}\left(\frac{\hat{f}(e_i\oplus e_{i'})}{\hat{f}(0)}\right)^2.\end{aligned} \tag{8}$$

Thus, the rotating tables countermeasure resists:

1. first-order attacks iff $\forall a$, $\mathsf{HW}[a] = 1 \Rightarrow \hat{f}(a) = 0$;
2. first- and second-order attacks iff $\forall a$, $1 \leqslant \mathsf{HW}[a] \leqslant 2 \Rightarrow \hat{f}(a) = 0$.

As a sanity check, we can verify that these properties hold when all the 2^n masks are used, *i.e.* when f is constant (and furthermore equal to 1). Indeed, in this case, $\hat{f}(a) = \sum_m f(m)(-1)^{a\cdot m} = \sum_m (-1)^{a\cdot m} = 2^n\delta(a)$, where δ is the Kronecker symbol.

Now, we notice that for Boolean functions, the notions of Fourier and Walsh transforms are very alike. Indeed,

$$\forall a \neq 0, \hat{f}(a) = \sum_m f(a)(-1)^{a\cdot m} = \sum_m (-1)^{a\cdot m}\tfrac{1}{2}\left(1 - (-1)^{f(m)}\right) = -\tfrac{1}{2}\widehat{(-1)^f}(a)\,.$$

Therefore, the previous conditions are equivalent to saying the following: the countermeasure resists $d \in \{1, 2\}$ order CPA iff $\forall a$, $\mathsf{HW}[a] \leqslant d \Rightarrow \widehat{(-1)^f}(a) = 0$.

We insist that this characterization is not equivalent to saying that f is d-resilient (defined in [5, page 45]). Indeed, a resilient function is balanced, which is explicitly not the case of f. Therefore, we study in the sequel a new kind of Boolean functions, that have everything in common with resilient functions but the balancedness of the plain function. The corollary is that, to the authors' best knowledge, no known construction method exists for this type of functions. Nonetheless, it is interesting to get an intuition about what characterizes a good resilient function. In [5, §7.1, page 95], it is explained that the highest degree of resiliency of a $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is $n-2$. This maximum is reached by affine functions (functions of unitary algebraic degree). Nonetheless, in our case, affine functions are not the best choice, because they are balanced. This means that the cardinality of their support (*i.e.* $\mathsf{Card}[\mathcal{M}]$) is 2^{n-1}, which is large. Therefore, we will be interested, whenever possible, by non-affine functions f of algebraic degree strictly greater than one (noted $d^\circ_{\text{alg}}(f) > 1$).

4.4 Functions $f : \mathbb{F}_2^4 \to \mathbb{F}_2$ that Cancel $\rho^{(1,2)}_{\text{opt}}$

For $n = 4$, all the sets $\mathcal{M}$ can be tested. The table 3 reports all the functions f that cancel $\rho^{(1)}_{\text{opt}}$ and $\rho^{(2)}_{\text{opt}}$. In this table, the truth-table of f, given in the first column, is encoded in hexadecimal. We note $\mathsf{HW}[f]$ the number of ones in the truth-table, and recall that $\mathsf{HW}[f] = \mathsf{Card}[\mathcal{M}]$. Columns 4, 5 and 6 are security metrics, whereas column 7 is the leakage metric (MIM). There are non-trivial solutions only for $\mathsf{Card}[\mathcal{M}]$ equal to half of the complete mask set cardinal. The MIA (column 6) shows two values: 0.219361 and 1 bit. Those values shall be contrasted with the MIA:

- without countermeasure ($\mathsf{Card}[\mathcal{M}] = 1$): MIA = 2.19819 bit and
- with two complementary masks ($\mathsf{Card}[\mathcal{M}] = 2$, which thwarts CPA but not 2O-CPA): MIA = 1.1981 bit (refer to appendix B).

Thus the countermeasure resists better correlation and information theoretic attacks, at the expense of more masks. Indeed, apart from $f = 1$, all the solutions are affine ($d^\circ_{\text{alg}}(f) = 1$), and thus have a Hamming weight of $2^{n-1} = 8 \gg 2$.

In this table, some functions belong to equivalent classes. Namely, two of them can be identified:

- the permutations of the bits (because the summations over i in Eqn. (7) or i, i' in Eqn. (8) is invariant in any change of the bits order), and
- the complementation. Indeed, $\widehat{\neg f}(a) = \sum_{m\in\mathbb{F}_2^n} \neg f(m)(-1)^{a\cdot m} = \sum_{m\in\mathbb{F}_2^n}(1 - f(m))(-1)^{a\cdot m} = 2^n\delta(a) - \hat{f}(a)$. Now, in Eqn. (7) and (8), $a \neq 0$ and $\hat{f}$ is involved squared. Thus $\rho^{(1,2)}_{\text{opt}}(\neg f) = \rho^{(1,2)}_{\text{opt}}(f)$.

The same can be said for the mutual information. This lemma is useful:

Lemma 1. *Let A and B be two random variables and ϕ a bijection; then $\mathsf{I}[A;\phi(B)] = \mathsf{I}[A;B]$.*

Table 3. All the functions $f : \mathbb{F}_2^4 \to \mathbb{F}_2$ that cancel $\rho_{\text{opt}}^{(1,2)}$.

f	$\mathsf{HW}[f]$	$\mathsf{H}[M]$	$\rho_{\text{opt}}^{(1)}$	$\rho_{\text{opt}}^{(2)}$	$\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z]$	$\mathsf{I}[Z \oplus M; Z]$	$d_{\text{alg}}^{\circ}(f)$
0x3cc3	8	3	0	0	0.219361	1	1
0x5aa5	8	3	0	0	0.219361	1	1
0x6699	8	3	0	0	0.219361	1	1
0x6969	8	3	0	0	0.219361	1	1
0x6996	8	3	0	0	1	1	1
0x9669	8	3	0	0	1	1	1
0x9696	8	3	0	0	0.219361	1	1
0x9966	8	3	0	0	0.219361	1	1
0xa55a	8	3	0	0	0.219361	1	1
0xc33c	8	3	0	0	0.219361	1	1
0xffff	16	4	0	0	0	0	0

This equality is obtained simply by writing the definition of the mutual information as a function of the probabilities, and by doing a variable change. Then:

- Let us call σ a permutation of $[\![1, n]\!]$. This function is a bijection, and its inverse is also a permutation. The Hamming weight is invariant if σ is applied on its input (*i.e.* $\mathsf{HW} = \mathsf{HW} \circ \sigma$). Hence $\mathsf{HW}[Z \oplus \sigma(M)] = \mathsf{HW}[\sigma^{-1}(Z \oplus \sigma(M))] = \mathsf{HW}[\sigma^{-1}(Z) \oplus M]$ (because σ is furthermore linear with respect to the addition). Let us note $Z' = \sigma^{-1}(Z)$, a random variable that is also uniform. Thus, $\mathsf{I}[\mathsf{HW}[Z \oplus \sigma(M)]; Z] = \mathsf{I}[\mathsf{HW}[Z' \oplus M]; \sigma(Z')]$. By considering $\phi = \sigma$, we prove that $\mathsf{I}[\mathsf{HW}[Z \oplus \sigma(M)]; Z] = \mathsf{I}[\mathsf{HW}[Z' \oplus M]; Z'] = \mathsf{I}[\mathsf{HW}[Z \oplus M]; Z]$, because Z and Z' have the same probability density function.
- Regarding the complementation, it is straightforward to note that $\mathsf{HW}[Z \oplus \neg M] = \mathsf{HW}[\neg(Z \oplus M)] = n - \mathsf{HW}[Z \oplus M]$. By considering $\phi : x \mapsto n - x$, we also have the invariance of the mutual information by the complementation of the mask.

So, there are eventually only three classes of functions listed in Tab. 3, modulo the two abovementioned equivalence classes. They are summarized below:

1. $f(x_1, x_2, x_3, x_4) = \bigoplus_{\substack{i \in I \subseteq [\![1,4]\!] \\ \mathsf{Card}[I]=3}} x_i$, (*aka* 0x3cc3, 0x5aa5, 0x6699, 0x6969) or complemented (*aka* 0x9696, 0x9966, 0xa55a, 0xc33c); According to the criteria stated at the end of Sec. 3, those functions are the best solutions for $n = 4$.
2. $f(x_1, x_2, x_3, x_4) = \bigoplus_{i=1}^{4} x_i$ (*aka* 0x6996) or $f(x_1, x_2, x_3, x_4) = 1 \oplus \bigoplus_{i=1}^{4} x_i$ (*aka* 0x9669), that have no advantage over the previous solutions, because they leak more;
3. the constant function $f = 1$ (*aka* 0xffff).

To resist first-order attacks, the masks set can be partitioned in two complementary sets; this means that there exists $\tilde{\mathcal{M}}$, a subset of $\mathcal{M}$, such that: $\mathcal{M} = \tilde{\mathcal{M}} \sqcup \neg\tilde{\mathcal{M}}$, where $\neg\tilde{\mathcal{M}} \doteq \{\neg m, m \in \mathcal{M}\}$ and "$\sqcup$" is the disjoint union operator[5]. Incidentally, we notice that this is not a mandatory property. Typically, this property is not verified any longer at order 2. For instance, in the solution $f = \texttt{0x3cc3}$, $\texttt{0x0} \in \mathcal{M}$ but $\neg\texttt{0x0} = \texttt{0xf} \notin \mathcal{M}$.

In conclusion, when $n = 4$ and the designer cannot afford using all the 16 masks, then with 8 masks, the rotating tables countermeasure is able to resist CPA, 2O-CPA and leak the minimal value of 0.219361 bit (about ten times less than the unprotected implementation, for which the MIA is 2.19819 bit).

4.5 Functions $f : \mathbb{F}_2^5 \to \mathbb{F}_2$ that Cancel $\rho_{\text{opt}}^{(1,2)}$

For $n = 5$, all the subsets $\mathcal{M}$ of $\mathbb{F}_2^5$ (2^{32} of them, it is the maximum achievable on a personal computer, as precised in [5, page 6]) have been tested. There are 1057 functions that cancel $\rho_{\text{opt}}^{(1,2)}$. The lowest value for $\mathsf{HW}[f]$ is 8. There are 60 functions of weight 8, but only three classes modulo the invariants. The functions, sorted regarding their properties, are shown in Tab. 4. As opposed to the case $n = 4$, there are non-affine solutions. In this table, only the number of equivalent classes is given. For a list of all functions, refer to appendix D.1.

Table 4. Summary of the security metrics of $f : \mathbb{F}_2^5 \to \mathbb{F}_2$ that cancel $\rho_{\text{opt}}^{(1,2)}$.

Nb. classes	$\mathsf{HW}[f]$	$\mathsf{H}[M]$	$\rho_{\text{opt}}^{(1)}$	$\rho_{\text{opt}}^{(2)}$	$\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z]$	$\mathsf{I}[Z \oplus M; Z]$	$d_{\text{alg}}^{\circ}(f)$
3	8	3	0	0	0.32319	2	2
4	12	3.58496	0	0	0.18595	1.41504	3
2	16	4	0	0	0.08973	1	1
2	16	4	0	0	0.08973	1	2
4	16	4	0	0	0.12864	1	2
2	16	4	0	0	0.16755	1	1
4	16	4	0	0	0.26855	1	2
6	16	4	0	0	0.32495	1	2
1	16	4	0	0	1	1	1
4	20	4.32193	0	0	0.07349	0.67807	3
3	24	4.58496	0	0	0.04300	0.41504	2
1	32	5	0	0	0	0	0

The greater $\mathsf{H}[M]$, the smaller the mutual information with $\mathscr{L} = \mathsf{HW}$ in general, but for some remarkable solutions (*e.g.* there is one MIA = $\mathsf{I}[\mathsf{HW}[Z \oplus$

[5] Let A and B be two sets, then the set $C = A \sqcup B$ is equal to $A \cup B$ if $A \cap B = \emptyset$.

$M]; Z] = 1$ of algebraic degree 1 for $\mathsf{HW}[f] = 16$). Also, it is worth noting that for a given budget (*e.g.* 16 masks) and security requirement (resistance against CPA and 2O-CPA), some solutions are better than the others against MIA. Indeed, the leaked information in Hamming weight model spans from 0.0897338 bit to 1 bit.

5 Exploring More Solutions Using SAT-Solvers

In order to explore problems of greater complexity, SAT-solver are indicated tools. We model f as a set of 2^n Boolean unknowns. The problem consists in finding f such that $\forall a, 1 \leqslant \mathsf{HW}[a] \leqslant 2, \hat{f}(a) = 0$, for a given $\mathsf{Card}[\mathcal{M}] = \hat{f}(0)$. A SAT-solver either:

- proves that there is no solution, or
- proves that a solution exists, and provides for (at least) one.

We notice that a SAT-solver may not terminate on certain instances of large exploration space; this has not been an issue in the work we report here. In this section, we first explain how our problem can be fed into a SAT-solver. Then, we use a SAT-solver in the case $n = 8$, relevant for AES. We look for low $\mathsf{Card}[\mathcal{M}]$ solutions, and for a given $\mathsf{Card}[\mathcal{M}]$, for the solutions of minimal MIA.

5.1 Mapping of the Problem into a SAT-Solver

Knowing that $\mathsf{Card}[\mathcal{M}] = \hat{f}(0)$, the problem $\rho_{\text{opt}}^{(1,2)}(f) = 0$ rewrites:

$$\begin{aligned} &\forall a, 1 \leqslant \mathsf{HW}[a] \leqslant 2, \quad \sum_x f(x)(-1)^{a \cdot x} = 0 \quad \Leftrightarrow \\ &\forall a, 1 \leqslant \mathsf{HW}[a] \leqslant 2, \quad \sum_x f(x) \wedge (a \cdot x) = \frac{1}{2} \sum_x f(x) = \frac{1}{2} \mathsf{Card}[\mathcal{M}] \ . \end{aligned} \tag{9}$$

A SAT-solver verifies the validity of clauses, usually expressed in conjunctive normal form (CNF). We note f as of 2^n literals noted $f_x = f(x)$. This yields the problem:

$$\left(\sum_{x \in \mathbb{F}_2^n} f_x = \mathsf{Card}[\mathcal{M}] \right) \wedge \bigwedge_{\substack{a \in \mathbb{F}_2^n, \text{ s.t.} \\ 1 \leqslant \mathsf{HW}[a] \leqslant 2}} \left(\sum_{x \in \mathbb{F}_2^n} f_x \wedge (a \cdot x) = \frac{1}{2} \mathsf{Card}[\mathcal{M}] \right) \ .$$

It is known that cardinality constraints can be formulated compactly thanks to Boolean clauses. More precisely, any condition "$\leqslant k(f_1, \cdots, f_n)$", for $0 \leqslant k \leqslant n$, can be expressed in terms of CNF clauses [21]. We note that:

$$\mathsf{HW}[x] \leqslant k \quad \Leftrightarrow \quad n - \mathsf{HW}[\neg x] \leqslant k \quad \Leftrightarrow \quad \mathsf{HW}[\neg x] \geqslant n - k \, .$$

As a consequence, satisfying the condition "$\geqslant k(x_1, \cdots, x_n)$" is equivalent to satisfying the condition "$\leqslant \{n-k\}(\neg x_1, \cdots, \neg x_n)$". Thus, testing the equality of a Hamming to $\frac{1}{2}\mathsf{Card}[\mathcal{M}]$ can be achieved by the conjunction of two clauses:

$$\leqslant \left\{\frac{1}{2}\mathsf{Card}[\mathcal{M}]\right\}(x_1, \cdots, x_n) \quad \text{and} \quad \leqslant \left\{n - \frac{1}{2}\mathsf{Card}[\mathcal{M}]\right\}(\neg x_1, \cdots, \neg x_n) \ .$$

The $n = 8$, the number of useful literals, $\{f(x), x \in \mathbb{F}_2^n\}$, is 2^8. However, the constraints $\mathsf{Card}[\mathcal{M}] = \hat{f}(0)$ and $\rho_{\text{opt}}^{(1,2)}(f) = 0$ (see Eqn. (9)) introduce 1,105,664 auxiliary variables and translate into 2,219,646 clauses, irrespective of $\mathsf{Card}[\mathcal{M}] \in \mathbb{N}^*$.

5.2 Existence of Low Hamming Weight Solutions for $n = 8$

The software `cryptominisat` [22,23] is used to search for solutions. The problem is tested for all the $\mathsf{Card}[\mathcal{M}]$ from 2 to 2^n, by steps of 2, as independent problems. Each problem requires a few hours to be solved. Impressively low Hamming weight solutions are found. The table 5 represents some of them. There are solutions only for $\mathsf{Card}[\mathcal{M}] \in \{4 \times \kappa, \kappa \in [\![3, 61]\!] \cup \{64\}\}$. Also, the mutual information with a Hamming weight leakage as a function of $\mathsf{H}[M]$ is plotted in Fig. 1. These values are low when compared to:

- MIA = 2.5442 bit without masking ($\mathsf{Card}[\mathcal{M}] = 1$) and
- MIA = 1.8176 bit with a mask random variable that takes two complementary values ($\mathsf{Card}[\mathcal{M}] = 2$).

Those MIA figures are computed in appendix B, and concern countermeasures that do not protect against 2O-DPA. The table 5 basically indicates that the margin gain in MIA resistance decreases when the cost of the countermeasures, proportional to $\mathsf{HW}[f]$, increases.

5.3 Exploration of Solutions for $n = 8$ and a Fixed $\mathsf{Card}[\mathcal{M}]$

There are nonequivalent solutions for a same $\mathsf{Card}[\mathcal{M}]$. Various seeds of the SAT-solver are needed to discover these solutions. The appendix D.2 gives some nonequivalent solutions for the minimal value $\mathsf{Card}[\mathcal{M}] = 12$, and details the truth-table of one solution. We note that all the solutions found by the SAT-solver for $\mathsf{Card}[\mathcal{M}] = 12$ have the same MIA value: 0.387582 bit. The same section in the appendix shows that for $\mathsf{Card}[\mathcal{M}] = 16$, various MIA values exist. The SAT-solver has notably came across, from best to worst: 0.181675, 0.213996, 0.215616, 0.216782, 0.219567, 0.220733, 0.246318, 0.249556, 0.251888, 0.253508, 0.254674, 0.257459, 0.388196, 0.434113, 1.074880 and 1.074950. We insist that with the SAT-solver, we find some solutions, but we cannot easily classify them. Thus we are unsure we have indeed found the best one. Nonetheless, it is already of great practical importance to exhibit some solutions.

Table 5. Metrics for one $f : \mathbb{F}_2^8 \to \mathbb{F}_2$ (per support cardinality) that cancels $\rho_{\text{opt}}^{(1,2)}$, found by a SAT-solver.

$\mathsf{HW}[f]$	$\mathsf{H}[M]$	$\rho_{\text{opt}}^{(1)}$	$\rho_{\text{opt}}^{(2)}$	$\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z]$	$\mathsf{I}[Z \oplus M; Z]$	$d_{\text{alg}}^{\circ}(f)$
12	3.58496	0	0	0.387582	4.41504	6
16	4	0	0	0.219567	4	5
20	4.32193	0	0	0.228925	3.67807	6
24	4.58496	0	0	0.235559	3.41504	5
28	4.80735	0	0	0.144147	3.19265	6
32	5	0	0	0.135458	3	5
36	5.16993	0	0	0.090575	2.83007	6
40	5.32193	0	0	0.078709	2.67807	5
44	5.45943	0	0	0.067960	2.54057	6
48	5.58496	0	0	0.060515	2.41504	5
52	5.70044	0	0	0.092676	2.29956	6
56	5.80735	0	0	0.054936	2.19265	5
60	5.90689	0	0	0.049069	2.09311	6
64	6	0	0	0.035394	2	2
68	6.08746	0	0	0.042374	1.91254	6
72	6.16993	0	0	0.036133	1.83007	5
76	6.24793	0	0	0.034194	1.75207	6
80	6.32193	0	0	0.031568	1.67807	5
84	6.39232	0	0	0.030072	1.60768	6
88	6.45943	0	0	0.026941	1.54057	5
92	6.52356	0	0	0.027042	1.47644	6
96	6.58496	0	0	0.022992	1.41504	5
100	6.64386	0	0	0.024316	1.35614	6
104	6.70044	0	0	0.022257	1.29956	5
108	6.75489	0	0	0.021458	1.24511	6
112	6.80735	0	0	0.019972	1.19265	4
116	6.85798	0	0	0.020481	1.14202	6
120	6.90689	0	0	0.018051	1.09311	5
124	6.9542	0	0	0.018397	1.0458	6
128	7	0	0	0.015095	1	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮

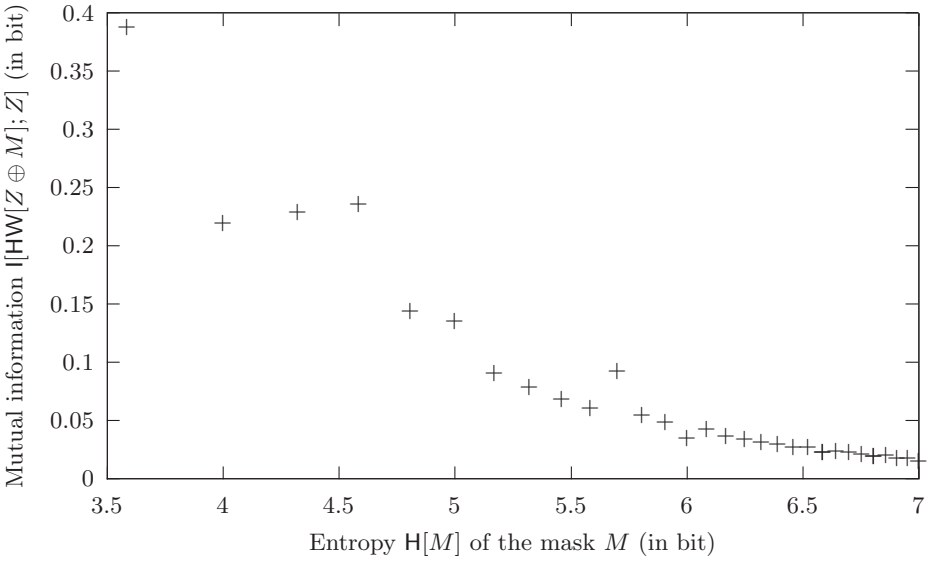

Fig. 1. Mutual information of the leakage in Hamming weight with the sensitive variable Z, for one solution on $n = 8$ bit that cancels $\rho_{\text{opt}}^{(1,2)}$ found by the SAT-solver.

6 Conclusions and Perspectives

Masking is a pro-active countermeasure against side-channel attacks. It implies adequately extra random variables amidst the computation in order to remove dependencies between the leakage of computation and guesses of internal sensitive values by a prospective attacker. Based on a representative first-order leakage model, this article explores the connections between the mask entropy and the best achievable security. If the implementation leaks its data values, then the leakage increases in proportion of the mask entropy reduction. Nonetheless, in practice, the implementation leaks a non-bijective value of its internal variables, such as the sum of their n bits. In this case, we show that the leakage is never null when limiting to a subset of few mask values amongst the 2^n possible. Furthermore, higher-order attacks can defeat this protection even if the mask losses as little as 1 single bit of entropy. Thus, we explore other mask entropy *vs* security tradeoffs. Our methodology is to demand resistance against CPA and 2O-CPA, and to minimize the leakage.

The criteria for masks selection has been formalized as a condition on the Walsh transform of an indicator function. This criteria has been used heuristically in a SAT-solver, but we expect that constructive methods based on the Boolean theory, for all n, can be invented. We exhibit the best solutions for $n = 4$ and $n = 5$, and prove the existence of varied values of mutual information for some masks cardinality for $n = 8$ (thanks to the SAT-solver). We notably

show that amongst the masks subsets that allow for a resistance at orders 1 and 2 against CPA, some are less sensitive to MIA than others, especially for $\mathsf{Card}[\mathcal{M}] = 16$. Therefore, there is a real opportunity for the designer to reduce the cost of the countermeasure in a reasoned way. The CM remains provably efficient even if $\mathcal{M}$ is made public. We insist that, at first sight, it can seem very audacious to mask an eight bit sensitive data with only four bits of mask. But it is indeed possible due to the high non-injectivity of the HW function, that maps 256 values into only 9.

Controlling the overhead in terms of resources is an enabler for masking technologies. Some countermeasures are expensive and our proposed tradeoff definitely shows that it is possible to quantify the security loss when one downgrades a countermeasure. As a perspective, we note that to further save area and speed, instead of storing the sboxes in RAM and selecting them randomly, we could take advantage of the dynamic partial reconfiguration of modern FPGAs to do so [14]. The idea is that even if computed at full throughput, the attacker does not have enough time to collect enough traces with a consistent set of sboxes to succeed an attack. This assumption is the same as those used for the resilient "leakage-proof" countermeasures [10].

Acknowledgments

The authors thank Manuel San Pedro for insightful discussions about SAT-solvers, and Sébastien Briais for ideas about the constructions of indicator functions. This work has been partly supported by the French National Research Agency (ANR), under grant ANR-09-SEGI-013 (ARPEGE project **SecReSoC**, "**Sec**ured **Re**configurable **S**ystem **o**n **C**hip").

References

1. Common Criteria (*aka* CC) for Information Technology Security Evaluation (standard ISO/IEC 15408), website: http://www.commoncriteriaportal.org/
2. Common Criteria consortium: Application of Attack Potential to Smartcards v2.7 (March 2009), http://www.commoncriteriaportal.org/files/supdocs/CCDB-2009-03-001.pdf
3. Batina, L., Gierlichs, B., Prouff, E., Rivain, M., Standaert, F.X., Veyrat-Charvillon, N.: Mutual Information Analysis: a Comprehensive Study. J. Cryptology 24(2), 269–291 (2011)
4. Brier, É., Clavier, C., Olivier, F.: Correlation Power Analysis with a Leakage Model. In: CHES. LNCS, vol. 3156, pp. 16–29. Springer (August 11–13 2004), Cambridge, MA, USA
5. Carlet, C.: Boolean Functions for Cryptography and Error Correcting Codes: Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering. pp. 257–397. Cambridge University Press, Y. Crama and P. Hammer eds (2010), preliminary version available at http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf

6. Chari, S., Rao, J.R., Rohatgi, P.: Template Attacks. In: CHES. LNCS, vol. 2523, pp. 13–28. Springer (August 2002), San Francisco Bay (Redwood City), USA
7. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic Analysis: Concrete Results. In: CHES. LNCS, vol. 2162, pp. 251–261. Springer (May 14-16 2001), Paris, France
8. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual information analysis. In: CHES, 10th International Workshop. Lecture Notes in Computer Science, vol. 5154, pp. 426–442. Springer (August 10-13 2008), Washington, D.C., USA
9. Guilley, S., Danger, J.L.: Patent WO 2011057991 (A1) entitled "Low-Complexity Electronic Circuit Protected by Customized Masking" (May 19 2011), Also published as FR 2952773 (A1)
10. Guilley, S., Sauvage, L., Danger, J.L., Selmane, N., Réal, D.: Performance Evaluation of Protocols Resilient to Physical Attacks. In: HOST. pp. 51–56. IEEE Computer Society (June 5-6 2011), Convention Center, San Diego, California, USA. DOI: 10.1109/HST.2011.5954995
11. Köpf, B., Basin, D.: An information-theoretic model for adaptive side-channel attacks. In: CCS'07: Proceedings of the 14th ACM conference on Computer and communications security. pp. 286–296. ACM, New York, NY, USA (2007)
12. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer (December 2006), ISBN 0-387-30857-1, http://www.dpabook.org/
13. Mangard, S., Schramm, K.: Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations. In: CHES. LNCS, vol. 4249, pp. 76–90. Springer (October 10-13 2006), Yokohama, Japan
14. Mentens, N., Gierlichs, B., Verbauwhede, I.: Power and Fault Analysis Resistance in Hardware through Dynamic Reconfiguration. In: CHES. Lecture Notes in Computer Science, vol. 5154, pp. 346–362. Springer (August 10–13 2008), Washington, D.C., USA
15. Moradi, A., Mischke, O.: How Far Should Theory be from Practice? Evaluation of a Countermeasure. In: CHES (September 9-12 2012), Leuven, Belgium
16. Nassar, M., Souissi, Y., Guilley, S., Danger, J.L.: RSM: a Small and Fast Countermeasure for AES, Secure against First- and Second-order Zero-Offset SCAs. In: DATE. pp. 1173–1178 (March 12-16 2012), Dresden, Germany. (TRACK A: "Application Design", TOPIC A5: "Secure Systems")
17. Prouff, E., Rivain, M.: A Generic Method for Secure SBox Implementation. In: Kim, S., Yung, M., Lee, H.W. (eds.) WISA. Lecture Notes in Computer Science, vol. 4867, pp. 227–244. Springer (2007)
18. Prouff, E., Rivain, M., Bevan, R.: Statistical Analysis of Second Order Differential Power Analysis. IEEE Trans. Computers 58(6), 799–811 (2009)
19. Rivain, M., Prouff, E.: Provably Secure Higher-Order Masking of AES. In: Mangard, S., Standaert, F.X. (eds.) CHES. LNCS, vol. 6225, pp. 413–427. Springer (2010)
20. Schindler, W.: Advanced stochastic methods in side channel analysis on block ciphers in the presence of masking. Journal of Mathematical Cryptology 2(3), 291–310 (October 2008), ISSN (Online) 1862-2984, ISSN (Print) 1862-2976, DOI: 10.1515/JMC.2008.013
21. Sinz, C.: Towards an Optimal CNF Encoding of Boolean Cardinality Constraints. In: van Beek, P. (ed.) CP. Lecture Notes in Computer Science, vol. 3709, pp. 827–831. Springer (2005)
22. Soos, M.: SAT-solver "`cryptominisat`", Version 2.9.0 (January 20 2011), https://gforge.inria.fr/projects/cryptominisat

23. Soos, M., Nohl, K., Castelluccia, C.: Extending SAT Solvers to Cryptographic Problems. In: Kullmann, O. (ed.) SAT. Lecture Notes in Computer Science, vol. 5584, pp. 244–257. Springer (2009)
24. Standaert, F.X., Malkin, T., Yung, M.: A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In: EUROCRYPT. LNCS, vol. 5479, pp. 443–461. Springer (April 26-30 2009), Cologne, Germany
25. Standaert, F.X., Peeters, É., Macé, F., Quisquater, J.J.: Updates on the Security of FPGAs Against Power Analysis Attacks. In: ARC. LNCS, vol. 3985, pp. 335–346. Springer-Verlag (March 2006), delft, The Netherlands
26. Standaert, F.X., Rouvroy, G., Quisquater, J.J.: FPGA Implementations of the DES and Triple-DES Masked Against Power Analysis Attacks. In: FPL. IEEE (August 2006), Madrid, Spain
27. Veyrat-Charvillon, N., Standaert, F.X.: Mutual Information Analysis: How, When and Why? In: CHES. LNCS, vol. 5747, pp. 429–443. Springer (September 6-9 2009), Lausanne, Switzerland
28. Veyrat-Charvillon, N., Standaert, F.X.: Adaptive Chosen-Message Side-Channel Attacks. In: Zhou, J., Yung, M. (eds.) ACNS. Lecture Notes in Computer Science, vol. 6123, pp. 186–199 (2010)
29. Waddle, J., Wagner, D.: Towards Efficient Second-Order Power Analysis. In: CHES. LNCS, vol. 3156, pp. 1–15. Springer (2004), Cambridge, MA, USA

A If $\mathscr{L}$ is not injective, then $\mathsf{I}[\mathscr{L}(Z \oplus M); Z]$ depends on $\mathcal{M}$, where $Z \sim \mathcal{U}(\mathbb{F}_2^n)$ and $M \sim \mathcal{U}(\mathcal{M})$

This property is exemplified in the following case-study, where $n = 2$, $\mathsf{Card}[\mathcal{M}] = 2$ and $\mathscr{L}$ is defined in Tab. 6. This leakage function is not meant to be realistic: it is simply an example to illustrate how computations unfold. Let us define $Y \doteq Z \oplus M$. Then $Y \sim \mathcal{U}(\mathbb{F}_2^n)$, and the entropy of $\mathscr{L}(Y)$ is equal to $\mathsf{H}[\mathscr{L}(Z \oplus M)] = -\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{4}\log_2\frac{1}{4} - \frac{1}{4}\log_2\frac{1}{4} = \frac{3}{2}$ bit.

Table 6. Imaginary truth-table of $\mathscr{L} : \mathbb{F}_2^2 \to \mathbb{R}$, used in subsections A.1 and A.2.

y	$\mathscr{L}(y)$
00	0
01	0
10	1
11	2

In the two next subsections A.1 and A.2, we compute $\mathsf{I}[\mathscr{L}(Z \oplus M); Z]$. We recall that, for all random variable X and all ℓ belonging to the image of $\mathbb{F}_2^n$ by $\mathscr{L}$:

$$\begin{aligned}\mathsf{P}[\mathscr{L}(Y) = \ell] &= \sum_{y \in \mathbb{F}_2^n} \mathsf{P}[\mathscr{L}(Y) = \ell \mid Y = y] \cdot \mathsf{P}[Y = y] \\ &= \sum_{\substack{y \in \mathbb{F}_2^n \\ \mathscr{L}(y) = \ell}} \mathsf{P}[Y = y] = \sum_{y \in \mathscr{L}^{-1}(\ell)} \mathsf{P}[Y = y]\,.\end{aligned}$$

Also, $\mathsf{H}[\mathscr{L}(Y)] = -\sum_{\ell \in \mathscr{L}(\mathbb{F}_2^n)} \mathsf{P}[\mathscr{L}(Y) = \ell] \log_2 \mathsf{P}[\mathscr{L}(Y) = \ell]$.

A.1 $\mathcal{M} = \{00, 01\}$

Some intermediate computations are detailed in Tab. 7. They allow to derive that the mutual information $\mathsf{I}[\mathscr{L}(Z \oplus M); Z]$ is equal to $\frac{3}{2} - \left(\frac{1}{4}\cdot 0 + \frac{1}{4}\cdot 0 + \frac{1}{4}\cdot 1 + \frac{1}{4}\cdot 1\right) = 1$ bit.

A.2 $\mathcal{M} = \{01, 10\}$

Some intermediate computations are detailed in Tab. 8. These results yield that the mutual information $\mathsf{I}[\mathscr{L}(Z \oplus M); Z]$ is equal to $\frac{3}{2} - \left(\frac{1}{4}\cdot 1 + \frac{1}{4}\cdot 1 + \frac{1}{4}\cdot 1 + \frac{1}{4}\cdot 1\right) = \frac{1}{2}$ bit. Consequently, this choice of $\mathcal{M}$ is better than the previous one.

Table 7. Memento for the computation of conditional probabilities and entropies when $\mathscr{L}$ is defined in Tab. 6 and $\mathcal{M} = \{00, 01\}$.

z	$\mathsf{P}[\mathscr{L}(z \oplus M) = \ell]$			$\mathsf{H}[\mathscr{L}(z \oplus M)]$
	$\ell = 0$	$\ell = 1$	$\ell = 2$	
00	$\mathsf{P}[00] + \mathsf{P}[01] = \frac{1}{2} + \frac{1}{2} = 1$	$\mathsf{P}[10] = 0$	$\mathsf{P}[11] = 0$	0
01	$\mathsf{P}[01] + \mathsf{P}[00] = \frac{1}{2} + \frac{1}{2} = 1$	$\mathsf{P}[11] = 0$	$\mathsf{P}[10] = 0$	0
10	$\mathsf{P}[10] + \mathsf{P}[11] = 0 + 0 = 0$	$\mathsf{P}[00] = \frac{1}{2}$	$\mathsf{P}[01] = \frac{1}{2}$	1
11	$\mathsf{P}[11] + \mathsf{P}[10] = 0 + 0 = 0$	$\mathsf{P}[01] = \frac{1}{2}$	$\mathsf{P}[00] = \frac{1}{2}$	1

Table 8. Memento for the computation of conditional probabilities and entropies when $\mathscr{L}$ is defined in Tab. 6 and $\mathcal{M} = \{01, 10\}$.

z	$\mathsf{P}[\mathscr{L}(z \oplus M) = \ell]$			$\mathsf{H}[\mathscr{L}(z \oplus M)]$
	$\ell = 0$	$\ell = 1$	$\ell = 2$	
00	$\mathsf{P}[00] + \mathsf{P}[01] = 0 + \frac{1}{2} = \frac{1}{2}$	$\mathsf{P}[10] = \frac{1}{2}$	$\mathsf{P}[11] = 0$	1
01	$\mathsf{P}[01] + \mathsf{P}[00] = \frac{1}{2} + 0 = \frac{1}{2}$	$\mathsf{P}[11] = 0$	$\mathsf{P}[10] = \frac{1}{2}$	1
10	$\mathsf{P}[10] + \mathsf{P}[11] = \frac{1}{2} + 0 = \frac{1}{2}$	$\mathsf{P}[00] = 0$	$\mathsf{P}[01] = \frac{1}{2}$	1
11	$\mathsf{P}[11] + \mathsf{P}[10] = 0 + \frac{1}{2} = \frac{1}{2}$	$\mathsf{P}[01] = \frac{1}{2}$	$\mathsf{P}[00] = 0$	1

Table 9. Memento for the computation of conditional probabilities and entropies when $\mathscr{L} = \mathsf{HW}$.

$\mathcal{M} = \{00, 11\}$

z	$\mathsf{P}[\mathscr{L}(z \oplus M) = \ell]$			$\mathsf{H}[\mathscr{L}(z \oplus M)]$
	$\ell = 0$	$\ell = 1$	$\ell = 2$	
00	$\frac{1}{2}$	0	$\frac{1}{2}$	1
01	0	1	0	0
10	0	1	0	0
11	$\frac{1}{2}$	0	$\frac{1}{2}$	1

$\mathcal{M} = \{01, 10\}$

z	$\mathsf{P}[\mathscr{L}(z \oplus M) = \ell]$			$\mathsf{H}[\mathscr{L}(z \oplus M)]$
	$\ell = 0$	$\ell = 1$	$\ell = 2$	
00	0	1	0	0
01	$\frac{1}{2}$	0	$\frac{1}{2}$	1
10	$\frac{1}{2}$	0	$\frac{1}{2}$	1
11	0	1	0	0

A.3 Other Case Study

If $\mathscr{L} = \mathsf{HW}$, then $\mathscr{L}(00) = 0$, $\mathscr{L}(01) = \mathscr{L}(10) = 1$ and $\mathscr{L}(11) = 2$. For two $\mathcal{M}$, the conditional probabilities and entropies are given in Tab. 9.

So, contrarily to the previous $\mathscr{L}$, we now have with $\mathscr{L} = \mathsf{HW}$ that, for both cases, $\mathsf{I}[\mathscr{L}(Z \oplus M); Z] = \frac{3}{2} - \frac{1}{4}(1+1) = 1$ bit.

B Exact Calculation of $\mathsf{H}[\mathsf{HW}[Z]]$ and of $\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z]$ when M Takes Two Complementary Values

In general, it is not obvious to compute a mutual information generically. However, for some specific case, it is possible to get an analytical expression. In this section, we compute the "MIA" when $\mathsf{Card}[\mathcal{M}] = 2$, and more precisely $M \in \{m, \neg m\}$.

First of all, the mutual information without countermeasure is equal to: $\mathsf{I}[\mathsf{HW}[Z]; Z] = \mathsf{H}[\mathsf{HW}[Z]] = -\sum_{h=0}^{n} \frac{\binom{n}{h}}{2^n} \log_2 \frac{\binom{n}{h}}{2^n}$ bit, because Z is uniformly distributed on $\mathbb{F}_2^n$.

Second, we are interested in the mutual information with the countermeasure, *i.e.* $\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z] = \mathsf{H}[\mathsf{HW}[Z \oplus M]] - \mathsf{H}[\mathsf{HW}[Z \oplus M] \mid Z]$. Now, the entropy $\mathsf{H}[\mathsf{HW}[Z \oplus M]]$ is equal to $\mathsf{H}[\mathsf{HW}[Z]]$, whatever the distribution of M, because $Z \sim \mathcal{U}(\mathbb{F}_2^n)$. When M takes complementary values, the random variable $(\mathsf{HW}[Z \oplus M] \mid Z = z)$ takes values $\mathsf{HW}[z \oplus m]$ or $\mathsf{HW}[z \oplus \neg m] = n - \mathsf{HW}[z \oplus m]$. Those two values are different, but when $\mathsf{HW}[z \oplus m] = n/2$. When n is odd, this cannot happen. Thus, the random variable $(\mathsf{HW}[Z \oplus M] \mid Z = z)$ takes two equiprobable values, hence has unitary entropy. When n is even, for $\binom{n}{n/2}$ values of z amongst the 2^n possible, the random variable has only one value $n/2$, hence is deterministic. This property is independent on the choice for the mask $m \in \mathbb{F}_2^n$. Therefore, $\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z] = \mathsf{I}[\mathsf{HW}[Z]; Z] - 1 + \delta(n \mod 2) \times \binom{n}{n/2}/2^n$.

So, to summarize, when masking with two complementary masks, the leaked information in Hamming weight is reduced by:

- exactly one bit if n is odd, but
- less than one bit if n is even. This case is unfavorable, because of an indiscernibility property that makes the mask useless in some configurations.

The values of the MIA without and with countermeasure are given in Fig. 2.

C Derivation of Eqn. (5) and (6)

The Eqn. (4) for $d = 1$ and 2 is calculated thanks to an alternative form of the variance: $\mathsf{Var}(X) = \mathsf{E}X^2 - (\mathsf{E}X)^2$. Also, in the two following subsections C.1 and C.2, we abridge "$\sum_{x \in \mathbb{F}_2^n}$", "$\sum_{m \in \mathcal{M}}$" and "$\sum_{i \in [\![1,n]\!]}$" simply by "$\sum_x$", "$\sum_m$", "$\sum_i$", respectively.

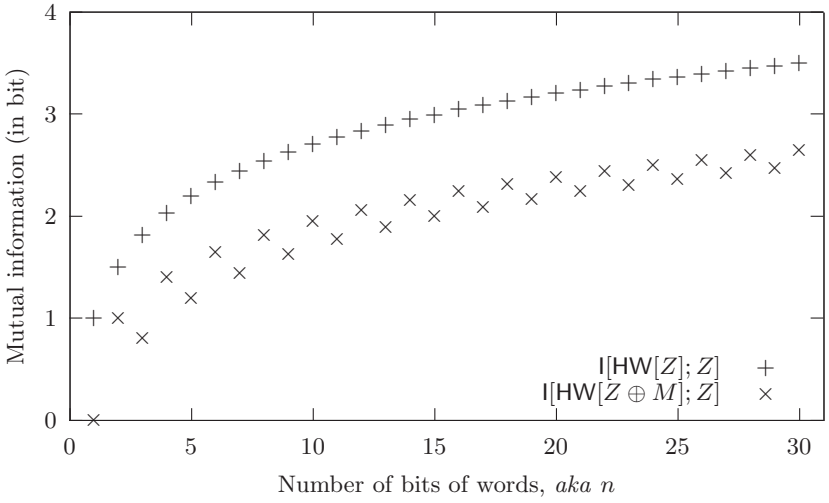

Fig. 2. Mutual information (exploitable by an MIA) without the masking and with masking when M takes two random complementary values with equal probability.

C.1 Derivation of Eqn. (5)

To compute the denominator of Eqn. (4), we need to estimate:

- $\mathsf{E}\frac{-1}{2}\sum_i (-1)^{(Z\oplus M)_i} = 0$ (by summation over $z \in \mathbb{F}_2^n$) and
- $\mathsf{E}\left(\frac{-1}{2}\sum_i (-1)^{(Z\oplus M)_i}\right)^2$.

This latter equation writes:

$$\begin{aligned}
&\frac{1}{\mathsf{Card}[\mathcal{M}]}\sum_m \frac{1}{2^n}\sum_z \frac{1}{2^2}\left(\sum_{i=1}^{n}(-1)^{(z\oplus m)_i}\right)^2 \\
&= \frac{1}{2^n\mathsf{Card}[\mathcal{M}]}\sum_m \frac{1}{2^2}\sum_{i_0,i_1}\sum_z (-1)^{(z\oplus m)_{i_0}\oplus(z\oplus m)_{i_1}} \\
&= \frac{1}{2^n\mathsf{Card}[\mathcal{M}]}\sum_m \frac{1}{2^2}\sum_{i_0,i_1} 2^n\delta(i_0-i_1) \quad \begin{array}{l}\text{// Recall that } \delta \text{ is the} \\ \text{// Kronecker symbol.}\end{array} \\
&= \frac{1}{2^n\mathsf{Card}[\mathcal{M}]}\sum_m \frac{1}{2^2} n2^n = \frac{n}{4}\,. \qquad (10)
\end{aligned}$$

Now, the numerator of Eqn. (4) involves on the one hand:

$$\mathsf{E}\left(\frac{-1}{2}\sum_i (-1)^{(Z\oplus M)_i}\right)^1 = \frac{-1}{2\cdot 2^n\cdot\mathsf{Card}[\mathcal{M}]}\sum_m\sum_i\left(\sum_z (-1)^{(z\oplus m)_i}\right) = 0\ ,$$

and on the other hand:

$$\begin{aligned}
&\mathsf{E}\left(\mathsf{E}\left(\left(\frac{-1}{2}\sum_i(-1)^{(Z\oplus M)_i}\right)^{d=1} \mid Z\right)\right)^2 \\
&= \frac{1}{2^2 2^n \mathsf{Card}[\mathcal{M}]^2}\sum_{m_0,m_1}\sum_{i_0,i_1}\sum_z(-1)^{(z\oplus m_0)_{i_0}\oplus(z\oplus m_1)_{i_1}} \\
&= \frac{1}{2^{n+2}\mathsf{Card}[\mathcal{M}]^2}\sum_{m_0,m_1}\sum_i 2^n(-1)^{(m_0\oplus m_1)_i} \\
&= \frac{1}{2^2}\sum_i\left(\frac{1}{\mathsf{Card}[\mathcal{M}]}\sum_m(-1)^{m_i}\right)^2 .
\end{aligned}$$

Consequently, we obtain the expression announced in Eqn. (5):

$$\rho^{(1)}_{\text{opt}} = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{1}{\mathsf{Card}[\mathcal{M}]}\sum_{m\in\mathcal{M}}(-1)^{m_i}\right)^2 .$$

C.2 Derivation of Eqn. (6)

The denominator of Eqn. (4), in the case $d = 2$, requires the computation of $\mathsf{E}\left(\frac{-1}{2}\sum_i(-1)^{(Z\oplus M)_i}\right)^2$. It has already been computed in the previous section 4.1 in Eqn. (10). Its value is $n/4$. The second value required for the denominator is: $\frac{1}{2^n\mathsf{Card}[\mathcal{M}]}\sum_m\frac{1}{2^4}\sum_z\left(\sum_i(-1)^{(z\oplus m)_i}\right)^4$. This expression is proportional to:

$$\begin{aligned}
&\sum_m\sum_z\left(\sum_{i=1}^{n}(-1)^{(z\oplus m)_i}\right)^4 \\
&= \sum_m\sum_{\substack{i_0,i_1,\\ i_2,i_3}}\sum_z(-1)^{(z\oplus m)_{i_0}\oplus(z\oplus m)_{i_1}\oplus(z\oplus m)_{i_2}\oplus(z\oplus m)_{i_3}} . \qquad (11)
\end{aligned}$$

If $(z\oplus m)_{i_0}\oplus(z\oplus m)_{i_1}\oplus(z\oplus m)_{i_2}\oplus(z\oplus m)_{i_3}$ depends on z, then the summation over z yields zero in Eqn. (11). The cases where this expression depends on z are enumerated below:

a) i_0, i_1, i_2 and i_3 are different: it depends on z;
b) Two indices are equal, and the other are different: it depends on z;
c) Two indices are equal and the other two are also equal: it does not depend on z;
d) Three indices are equal and the last one is different: it depends on z;
e) The four indices are equal: it does not depend on z;

Thus, we need to enumerate the cases where indices are equal two by two (which include the last case of equality between all the masks). The possibilities are shown in Fig. 3, where the identical indices are linked together. Each case happens $n\times(n-1)$ times: n times to choose the first couple, and $n-1$ remaining possibilities for the second couple. We must add n cases for configurations where $i_0 = i_1 = i_2 = i_3$. Thus, the total number of possibilities is $3n(n-1)+n = n(3n-2)$. Therefore, we deduce that $\frac{1}{2^n \mathsf{Card}[\mathcal{M}]} \sum_m \frac{1}{2^4} \sum_z \left(\sum_{i=1}^n (-1)^{(z\oplus m)_i}\right)^4 = \frac{n(3n-2)}{4}$.

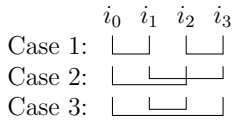

Fig. 3. Pairwise equality relationships in a set of four indices.

Eventually, the denominator is equal to: $\frac{1}{4^2}\left(n(3n-2)-n^2\right) = \frac{n(n-1)}{2^3}$.
To compute the numerator, it can be first noted that:

$$\mathsf{E}\left(\mathsf{E}\left(\left(\frac{-1}{2}\sum_i (-1)^{(Z\oplus M)_i}\right)^{d=2} \mid Z\right)\right) = \frac{n}{4} \ ,$$

as already demonstrated in Eqn. (10). Then, we compute:

$$\begin{aligned}
&\frac{1}{2^n}\sum_z \left(\frac{1}{\mathsf{Card}[\mathcal{M}]}\sum_m \left(\frac{-1}{2}\sum_i (-1)^{(z\oplus m)_i}\right)^{d=2}\right)^2 \\
&= \frac{1}{2^4 2^n \mathsf{Card}[\mathcal{M}]^2}\sum_z \left(\sum_m \sum_{i_0,i_1} (-1)^{(z\oplus m)_{i_0}\oplus(z\oplus m)_{i_1}}\right)^2 \\
&= \frac{1}{2^{n+2}\mathsf{Card}[\mathcal{M}]^2}\sum_{m,m'}\sum_{\substack{i_0,i_1,\\ i'_0,i'_1}}\sum_z (-1)^{(z\oplus m)_{i_0}\oplus(z\oplus m)_{i_1}\oplus(z\oplus m')_{i'_0}\oplus(z\oplus m')_{i'_1}} \ . \quad (12)
\end{aligned}$$

This summation resembles that depicted in Fig. 3, but now the indices already refer to some classes: i_0 and i_1 relate to mask m, whereas i'_0 and i'_1 relate to mask m'. This setup is shown in Fig. 4. In this section, we count the case $i_0 = i_1 = i'_0 = i'_1$ in each case, and we eventually subtract those multiply counted. Therefore:

– In case 1: the masks m and m' cancel out one each other, so the sum is equal to $\frac{1}{2^4}n^2$.

– In case 2: the sum is equal to:

$$\frac{1}{2^4\mathsf{Card}[\mathcal{M}]^2}\sum_{m,m'}\sum_{\substack{i_0,i_1,\\ i'_0,i'_1}}(-1)^{m_{i_0}\oplus m_{i_1}\oplus m'_{i'_0}\oplus m'_{i'_1}}\times\delta(i_0-i'_0)\times\delta(i_1-i'_1)$$

$$=\frac{1}{2^4\mathsf{Card}[\mathcal{M}]^2}\sum_{m,m'}\sum_{i_0,i_1}(-1)^{(m\oplus m')_{i_0}\oplus(m\oplus m')_{i_1}}$$

$$=\frac{1}{2^4\mathsf{Card}[\mathcal{M}]^2}\sum_{m,m'}\left(\sum_i(-1)^{(m\oplus m')_i}\right)^2.$$

– In case 3: it yields the same as case 2, because of the invariance of Eqn. (12) in $i_0\leftrightarrow i_1$ and in $i'_0\leftrightarrow i'_1$.

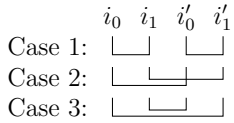

Fig. 4. Pairwise equality relationships in a set of four indices, already belonging to two classes (nominal and primed).

Now, the equality between the four indices is counted three times, and thus shall be subtracted twice. Therefore, the numerator for Eqn. (4) when $d=2$ is equal to:

$$\frac{1}{2^4}\left(\cancel{n^2}+2\times\frac{1}{2^4\mathsf{Card}[\mathcal{M}]^2}\sum_{m,m'}\left(\sum_i(-1)^{(m\oplus m')_i}\right)^2-2n\right)-\cancel{(n-1)^2}$$

$$=\frac{1}{2^3}\left(\frac{1}{\mathsf{Card}[\mathcal{M}]^2}\sum_{m,m'}\left(\sum_i(-1)^{(m\oplus m')_i}\right)^2-n\right).$$

The optimal correlation coefficient for a second-order attack is thus equal to the expression already disclosed in Eqn. (6):

$$\rho^{(2)}_{\text{opt}}=\frac{1}{n(n-1)}\left(\frac{1}{\mathsf{Card}[\mathcal{M}]^2}\sum_{m,m'}\left(\sum_i(-1)^{(m\oplus m')_i}\right)^2-n\right). \tag{13}$$

D More Details About the Solutions for $n=5$ and $n=8$

D.1 All the Solutions that Cancel $\rho^{(1,2)}_{\text{opt}}$ for $n=5$

The 1057 solutions for $n=5$ can be grouped by equivalence classes, that consist in permuting the bits or complementing them (when $\mathsf{Card}[\mathcal{M}]=2^{n-1}$). The

table 10 complements Tab. 4 by giving in addition the smallest element that generates each class. Also, it can be noticed that if a class of functions of Hamming weight $h \neq 2^n$ exists, then a class of functions of Hamming weight $2^n - h$ also exists. This is due to the complementary identity discussed in Sec. 4.4.

Table 10. Complete list of generators of Boolean functions $f : \mathbb{F}_2^5 \to \mathbb{F}_2$ that cancel $\rho_{\text{opt}}^{(1,2)}$.

$\mathsf{HW}[f]$	$\mathsf{I}[\mathsf{HW}[Z \oplus M]; Z]$	$\mathsf{I}[Z \oplus M; Z]$	$d^{\circ}_{\text{alg}}(f)$	Generators of classes
8	0.32319	2	2	{ 0x06609009, 0x06909006, 0x81182442 }
12	0.18595	1.41504	3	{ 0x1698a443, 0x19a4c216, 0x83586429, 0x83589426 }
16	0.08973	1	1	{ 0x0ff0f00f, 0x96969696 }
16	0.08973	1	2	{ 0x1bd8e427, 0x87b4d21e }
16	0.12864	1	2	{ 0x1be4e41b, 0x2dd2e11e, 0x8778b44b, 0x96969966 }
16	0.16755	1	1	{ 0x3cc3c33c, 0x96699669 }
16	0.26855	1	2	{ 0x17e8e817, 0x8778e11e, 0x2bd4d42b, 0x99969666 }
16	0.32495	1	2	{ 0x1ee1e11e, 0x2dd2d22d, 0x69969696, 0x87787887, 0x96699696, 0x96969669 }
16	1	1	1	{ 0x69969669 }
20	0.07349	0.67807	3	{ 0x3ddae697, 0x6bd9e53e, 0x97bcda67, 0x9bd6e53e }
24	0.04300	0.41504	2	{ 0x6ff6f99f, 0x9ff6f69f, 0xbddbe77e }
32	0	0	0	{ 0xffffffff }

D.2 Detail of the the First Solutions Given in Tab. 5 for $n = 8$

The lowest possible number of mask values to achieve CPA and 2O-CPA resistance for $n = 8$ is $\mathsf{Card}[\mathcal{M}] = 12$. Many different classes are found, but they share the same metrics, *i.e.* those indicated in Tab. 5. As an example, with 57 seed values, 14 non-equivalent solutions are found. They are listed below:

0x0200000004008000040020000010000000400100200000800000001000008,
0x1000080000000001000800000040200000000040800200000100002000000400,
0x0000002080000001004008000100000002040000000040000000100000200008,

0x0000000440200000010020000000000800028000000001000040000008000010,
0x0000080020000004010000200040000000810000000010000000400008000002,
0x0001800000000100002000000800004000000008204000000400100000000002,
0x2000040000000040000000028001000000100000000802000400008000001000,
0x2000000000080400000180000000001000400100000000200000000842000000,
0x0004002000004000010000000080020000000800100200008000001000000004,
0x0000040000800010100800000000020000018000020000000000002040000004,
0x8000000000200400000000180100000000010200000000404000000000082000,
0x0001200004000000000000080020400000000040008002001800000000000001,
0x0002000010000400800000400000000200042000000000800000010008100000,
0x0000004042000000000801000000002000012000000000088000000000100400.

The algebraic normal form of the first solution writes as follows: $f(x) = x_2x_1 \oplus x_3x_2x_1 \oplus x_4x_2x_1 \oplus x_4x_3x_2x_1 \oplus x_5x_2x_1 \oplus x_5x_3x_2x_1 \oplus x_5x_4 \oplus x_5x_4x_1 \oplus x_5x_4x_2 \oplus x_5x_4x_3 \oplus x_5x_4x_3x_1 \oplus x_5x_4x_3x_2 \oplus x_6x_2x_1 \oplus x_6x_3x_2x_1 \oplus x_6x_4x_2x_1 \oplus x_6x_4x_3x_2x_1 \oplus x_6x_5x_2x_1 \oplus x_6x_5x_3x_2x_1 \oplus x_6x_5x_4 \oplus x_6x_5x_4x_1 \oplus x_6x_5x_4x_2 \oplus x_6x_5x_4x_3 \oplus x_6x_5x_4x_3x_1 \oplus x_6x_5x_4x_3x_2 \oplus \mathbf{x_6x_5x_4x_3x_2x_1} \oplus x_7x_2x_1 \oplus x_7x_3x_2x_1 \oplus x_7x_4x_2x_1 \oplus x_7x_4x_3x_2x_1 \oplus x_7x_5x_2x_1 \oplus x_7x_5x_3x_1 \oplus x_7x_5x_4 \oplus x_7x_5x_4x_1 \oplus x_7x_5x_4x_2 \oplus x_7x_5x_4x_3 \oplus x_7x_5x_4x_3x_2 \oplus \mathbf{x_7x_5x_4x_3x_2x_1} \oplus x_7x_6 \oplus x_7x_6x_1 \oplus x_7x_6x_2 \oplus x_7x_6x_3 \oplus x_7x_6x_3x_1 \oplus x_7x_6x_3x_2 \oplus x_7x_6x_4 \oplus x_7x_6x_4x_1 \oplus x_7x_6x_4x_2 \oplus x_7x_6x_4x_3 \oplus x_7x_6x_4x_3x_1 \oplus \mathbf{x_7x_6x_4x_3x_2x_1} \oplus x_7x_6x_5 \oplus x_7x_6x_5x_1 \oplus x_7x_6x_5x_2 \oplus x_7x_6x_5x_3 \oplus x_7x_6x_5x_3x_2 \oplus \mathbf{x_7x_6x_5x_3x_2x_1} \oplus \mathbf{x_7x_6x_5x_4x_2x_1} \oplus \mathbf{x_7x_6x_5x_4x_3x_1} \oplus \mathbf{x_7x_6x_5x_4x_3x_2} \oplus x_8x_2x_1 \oplus x_8x_3x_2x_1 \oplus x_8x_4x_2x_1 \oplus x_8x_4x_3 \oplus x_8x_4x_3x_1 \oplus x_8x_4x_3x_2 \oplus x_8x_5x_2x_1 \oplus x_8x_5x_3x_2x_1 \oplus x_8x_5x_4 \oplus x_8x_5x_4x_1 \oplus x_8x_5x_4x_2 \oplus \mathbf{x_8x_5x_4x_3x_2x_1} \oplus x_8x_6x_2x_1 \oplus x_8x_6x_3x_1 \oplus x_8x_6x_4x_2x_1 \oplus x_8x_6x_4x_3 \oplus x_8x_6x_4x_3x_2 \oplus \mathbf{x_8x_6x_4x_3x_2x_1} \oplus x_8x_6x_5x_2 \oplus x_8x_6x_5x_3x_1 \oplus x_8x_6x_5x_3x_2 \oplus \mathbf{x_8x_6x_5x_3x_2x_1} \oplus x_8x_6x_5x_4 \oplus x_8x_6x_5x_4x_1 \oplus \mathbf{x_8x_6x_5x_4x_2x_1} \oplus \mathbf{x_8x_6x_5x_4x_3x_1} \oplus \mathbf{x_8x_6x_5x_4x_3x_2} \oplus x_8x_7x_2x_1 \oplus x_8x_7x_3x_2x_1 \oplus x_8x_7x_4x_3 \oplus x_8x_7x_4x_3x_1 \oplus x_8x_7x_4x_3x_2 \oplus \mathbf{x_8x_7x_4x_3x_2x_1} \oplus x_8x_7x_5x_2x_1 \oplus x_8x_7x_5x_3x_1 \oplus x_8x_7x_5x_3x_2 \oplus \mathbf{x_8x_7x_5x_3x_2x_1} \oplus x_8x_7x_5x_4 \oplus x_8x_7x_5x_4x_1 \oplus x_8x_7x_5x_4x_2 \oplus \mathbf{x_8x_7x_5x_4x_2x_1} \oplus \mathbf{x_8x_7x_5x_4x_3x_1} \oplus \mathbf{x_8x_7x_5x_4x_3x_2} \oplus x_8x_7x_6 \oplus x_8x_7x_6x_1 \oplus x_8x_7x_6x_2 \oplus x_8x_7x_6x_3 \oplus x_8x_7x_6x_3x_2 \oplus \mathbf{x_8x_7x_6x_3x_2x_1} \oplus x_8x_7x_6x_4 \oplus x_8x_7x_6x_4x_1 \oplus x_8x_7x_6x_4x_2 \oplus \mathbf{x_8x_7x_6x_4x_2x_1} \oplus \mathbf{x_8x_7x_6x_4x_3x_1} \oplus \mathbf{x_8x_7x_6x_4x_3x_2} \oplus x_8x_7x_6x_5 \oplus x_8x_7x_6x_5x_1 \oplus \mathbf{x_8x_7x_6x_5x_2x_1} \oplus x_8x_7x_6x_5x_3 \oplus \mathbf{x_8x_7x_6x_5x_3x_1} \oplus \mathbf{x_8x_7x_6x_5x_3x_2} \oplus \mathbf{x_8x_7x_6x_5x_4x_1} \oplus \mathbf{x_8x_7x_6x_5x_4x_2} \oplus \mathbf{x_8x_7x_6x_5x_4x_3}$.

In this expression, the products of 6 variables are shown in bold font. It is thus clear that the algebraic degree of f is $d^{\circ}_{\mathrm{alg}}(f) = 6$. The corresponding twelve masks are:

{ 0x03, 0x18, 0x3f, 0x55, 0x60, 0x6e, 0x8c, 0xa5, 0xb2, 0xcb, 0xd6, 0xf9 }.

For the next masks subsets ($\mathsf{Card}[\mathcal{M}] = 16$), there are also different classes. But their MIA do differ, as represented in Fig. 5 for elements of 286 different classes. Most solutions have algebraic degree 5, but some have 4. The mutual information for algebraic degree 5 is more spread than for $d^{\circ}_{\mathrm{alg}}(f) = 4$. The best solution found by the SAT-solver has an MIA of 0.181675 bit.

Eventually, we mention that for $\mathsf{Card}[\mathcal{M}] > 16$, there still exists different solutions when $\mathsf{Card}[\mathcal{M}] \in \{12 + 4\kappa, 0 \leqslant \kappa \leqslant 61\}$, but that the MIA are less spread. For instance, for $\mathsf{Card}[\mathcal{M}] = 20$, we have found these MIA values: 0.191514,

0.197768, 0.200909, 0.201735, 0.201907, 0.202508, 0.215823, 0.219964, 0.220303, 0.221462, 0.223525, 0.224186, 0.224328, 0.224450, 0.224958 and 0.228925.

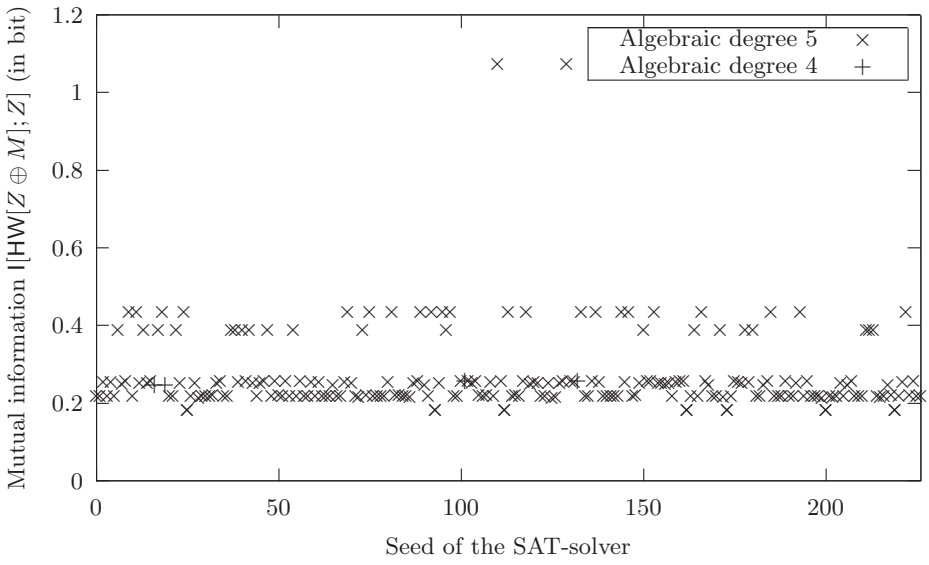

Fig. 5. Mutual information of the leakage in Hamming weight with the $n = 8$-bit sensitive variable Z, for many nonequivalent solutions f of weight $\hat{f}(0) = 16$ that cancels $\rho_{\text{opt}}^{(1,2)}$ found by the SAT-solver.