Side-channel information leakage of code-based masked implementations

Wei Cheng, Olivier Rioul, Yi Liu, Julien Béguinot, Sylvain Guilley

Side-Channel Information Leakage of Code-Based Masked Implementations

Wei Cheng*, Olivier Rioul*, Yi Liu*, Julien Béguinot*, and Sylvain Guilley†*
*LTCI, Télécom Paris, Institut Polytechnique de Paris, Palaiseau, France, firstname.lastname@telecom-paris.fr
†Secure-IC S.A.S., Paris, France, sylvain.guilley@secure-ic.com

***Abstract*—Side-channel attacks (SCAs) are among the most powerful physical attacks against cryptographic implementations. To thwart SCAs, a well-established countermeasure is random masking. A recent code-based masking formalism unifies several known masking schemes and allows one to carry out an all-in-one leakage quantification.**

In this paper, we investigate how a code-based masked implementation leaks in an information-theoretic setting, where the mutual information measures the impact of both number and positions of probes in the probing attack model. We also establish that the mutual information decreases as the measurement noise variance increases, with an exponent equal to the dual distance of the masking code. Our findings quantitatively connect the attacker's capability to recover secret keys with the actual mutual information leakage of the protected implementation.

I. Introduction

Side-channel attacks consist in retrieving sensitive information from compromising emanations (e.g., electromagnetic, power consumption) of cryptographic devices [10], [13], [15]. In the probing model [12], it is assumed that the adversary has the capability to measure a limited amount of intermediate data from the device. Randomly masking sensitive information is a method to thwart such attacks, up to a given probing order [15]. A fairly general formalization of masking is *code-based masking*, where the probing security order relates to the dual distance of the underlying linear code [6], [9], [17].

The defender can always increase the probing security order if the attacker has a higher number of probes, but this comes at a higher cost. This cat-and-mouse game can be seen as futile and even detrimental to the defender who runs for more expenses. The attacker is also hindered beyond the number of probes he can deploy. When probed sensitive variables are tainted with noise, the advantage gained by the attacker is reduced as the number of probes increases. This was the spearhead for motivating masking as a well-founded countermeasure since the seminal work of Waddle and Wagner [20] in 2004.

In a sense, the masking setting under the probing model can be viewed as a special case of a wiretap channel of Type II (WTC II) [16], where an eavesdropper has access to a given number of bits. Assuming that the information symbols are elements in a finite field $\mathbb{F}$, the information $X \in \mathbb{F}^k$ is encoded as $Z \in \mathbb{F}^n$ by using a random mask $Y \in \mathbb{F}^m$ (with $n = k+m$), and the d probed bits ($0 < d \leqslant n$) are denoted by $Z^{\text{ı}}$. This is illustrated in Fig. 1. The eavesdropper should be able to recover X when she probed a sufficient number of bits.

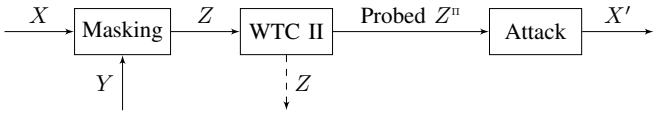

Fig. 1. The archetype of a WTC of type II adapted for masking in a noiseless scenario. Note that the dashed part is mainly for illustration of the masked variable in the following computations.

The SCA scenario, however, differs from the classical WTC scenario in one important respect: While each wiretap channel use corresponds to a different message to be communicated to a legitimate user, every side-channel use corresponds to a query of the unintended leakage arising from the same sensitive variable X.

Furthermore, in a practical side-channel scenario, the eavesdropper only has access to a noisy leakage because of some intrinsic noise N from various sources (e.g., measurement noise). An example of setup is shown in Fig. 2. Therefore, the question arising is the following: *how much information is leaking in presence of masking?*

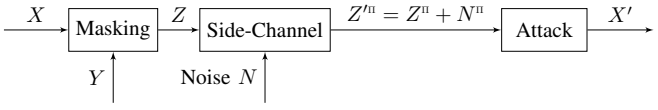

Fig. 2. The realistic side-channel setup in the presence of noise. The intrinsic noise N is from the acquisition environment, instruments and specific settings.

In this paper, we evaluate the mutual information leakage in the presence of the code-based masking countermeasure, without noise or with noise. In this way, we quantify the powerfulness of this countermeasure by revisiting the adversary's advantage. More precisely, we show that there is a gap between the attacker's means (probes) and the actual information leakage. Quite surprisingly, the exploitable information requires that the number of probes placed by the attacker should be at least equal to the dual distance of the masking code but otherwise irrespective of their positions.

The remainder of this article is organized as follows. Section II introduces notations and the code-based masking scheme. Section III studies the information leakage in a noiseless scenario. Section IV studies the impact of measurement noise and provides a numerical validation. Section V concludes.

II. Code-Based Masking and Leakage Model

The rationale of masking is to split each sensitive (secret-dependent) variable into several shares and then perform the

corresponding cryptographic operations separately on each share. As a result, knowing only a subset of shares is not enough to recover the secret when the cardinality of the probed set is smaller than a certain threshold t, called the *security order* of the masking scheme.

A recent line of research generalizes several masking schemes and unifies them from a code-theoretic perspective into the so-called *code-based masking* [8], [21]. Let $\mathbb{F}$ be a finite field with q elements (where q is a power of 2), and let $n = k+m$ where k and m are positive integers. The considered code-based masking is modeled by

$$Z = X\mathbf{G} + Y\mathbf{H}, \tag{1}$$

where $X \sim \mathcal{U}(\mathbb{F}^k)$ is the secret, a random row vector uniformly distributed over $\mathbb{F}^k$; $Y \sim \mathcal{U}(\mathbb{F}^m)$ is the mask, a row random vector uniformly distributed over $\mathbb{F}^m$; $\mathbf{G}$ is an $k \times n$ matrix of full rank k over $\mathbb{F}$; $\mathbf{H}$ is an $m \times n$ matrix of full rank m over $\mathbb{F}$, so that $Z \in \mathbb{F}^n$. This attacker aims at guessing values of X based on the exploitation of the measurement of some coordinates in Z.

Let $\mathcal{C} = V_{\mathbf{G}}$ be the row space of $\mathbf{G}$ and $\mathcal{D} = V_{\mathbf{H}}$ be the row space of $\mathbf{H}$. Thus, $\mathcal{C}$ is an $[n, k]$ linear code and $\mathcal{D}$ is an $[n, m]$ linear code (the masking code). We assume that $\mathcal{C}$ and $\mathcal{D}$ are in direct sum and complementary codes:

$$\begin{aligned} V_{\mathbf{G}} \cap V_{\mathbf{H}} &= \mathcal{C} \cap \mathcal{D} = \{0_n\}, \\ V_{\mathbf{G}} \oplus V_{\mathbf{H}} &= \mathcal{C} \oplus \mathcal{D} = \mathbb{F}^n, \end{aligned} \tag{2}$$

where 0_n is the all-zero vector. To simplify the derivations in the following sections, we represent $\mathbb{F}_q$ in $\mathbb{F}_2$ by the sub-field representation [9], [14, § 7.7]. This allows one to focus only on *binary variables in* $\mathbb{F} = \mathbb{F}_2$ throughout this paper.

The following example is perhaps the simplest family of code-based masking schemes for arbitrary n:

Example 1 (Boolean masking [7]): *Let $k = 1$ and $n = m+1$, then the two generator matrices are as follows.*

$$\begin{aligned} \mathbf{G} &= \begin{pmatrix} 1 & 0_{n-1} \end{pmatrix} \\ \mathbf{H} &= \begin{pmatrix} 1_{n-1}^T & I_{n-1} \end{pmatrix} \end{aligned}$$

where 1_{n-1}^T denotes the transpose of an all-one vector and I_{n-1} is the identity matrix of order $n-1$.

Relying on the encoding in (1) and two conditions in (2), the code-based masking encompasses the Boolean masking, Inner Product masking (IPM) [1], Leakage Squeezing (LS) [5] and Direct Sum masking (DSM) [3], [6], [17]. By the uniform representation, the side-channel security order under the probing model is equal to the *dual distance* of $\mathcal{D}$ (the minimum distance of its dual code $\mathcal{D}^\perp$) [6], [17] minus one: $t = d_{\mathcal{D}}^\perp - 1$. In addition, the amount of information that can be extracted by any adversaries from noisy leakage is also related to the *kissing number* of the dual code $\mathcal{D}^\perp$ [9].

In order to quantify the impact of probes, we adopt the following definition of the probing model in a d-dimensional attack [12].

Definition 1 (Probing Model): *Let $d > 0$ be the* dimension *of the attack, and $\mathrm{п} \in \mathbb{F}^n$ be a binary vector of Hamming weight d. The location of the nonzero elements in $\mathrm{п}$ represent the "location" of probes in a d-dimensional attack. Let $\mathbf{A}^{\mathrm{п}}$ denote the $m \times d$ matrix obtained from $\mathbf{A}$ by removing all columns $(A_{i,j})_j$ corresponding to zero elements $\mathrm{п}_j = 0$ in $\mathrm{п}$. The probing model is described as*

$$Z^{\mathrm{п}} = X\mathbf{G}^{\mathrm{п}} + Y\mathbf{H}^{\mathrm{п}}.$$

The question is whether $Z^{\mathrm{п}}$ (or some noisy version of it) leaks information about secret X in the presence of masking Y.

Note that with our notation, $\mathrm{п}^{\mathrm{п}} \in \mathbb{F}^d$ is the all-one vector and we have $\mathbf{A} \cdot \mathrm{п}^t = \mathbf{A}^{\mathrm{п}} \cdot (\mathrm{п}^{\mathrm{п}})^t$.

Let $w_H(\cdot)$ denote the Hamming weight of a vector. In particular $w_H(\mathrm{п}) = d$. The following notion of *generalized Hamming weight* is known to be a sound tool to characterize the leakage [22], especially under the probing model in the noiseless scenario where the information leakage in code-based masking is modeled by a special case of wire-tap channel II.

Definition 2 (Generalized Hamming Weight [22]): *For any linear code $\mathcal{C}$, the* support $\chi(\mathcal{C})$ *of $\mathcal{C}$ is the set of not-always-zero coordinates of $\mathcal{C}$. The r-th Hamming weight of an $[n, k]$ linear code $\mathcal{C}$, where $1 \leqslant r \leqslant k$, is defined as the cardinality of the smallest support of a r-dimensional subcode of $\mathcal{C}$:*

$$d_{r,\mathcal{C}} = \min_{\mathcal{C}'} \{ |\chi(\mathcal{C}')| \ ; \ \mathcal{C}' \text{ is an } [n, r] \text{ subcode of } \mathcal{C} \}. \tag{3}$$

In particular $d_{1,\mathcal{C}}$ is the minimum Hamming weight of codewords in $\mathcal{C}$, i.e., the minimum distance of $\mathcal{C}$.

Definition 3 (Weight Enumerators): *Let $B_i = |\{u \in \mathcal{D}; w_H(u) = i\}|$ be the Hamming weight distribution of the linear code $\mathcal{D}$ generated by $\mathbf{H}$, and let A_i denote the weight distribution of the dual code $\mathcal{D}^\perp$. The corresponding weight enumerator polynomials A and B are*

$$A(x, y) = \sum_{i=0}^{d} A_i x^i y^{d-i}, \qquad B(x, y) = \sum_{i=0}^{d} B_i x^i y^{d-i}. \tag{4}$$

The MacWilliams identity [14] applied to this weight enumerators for $x = p$ and $y = 1 - p$ is

$$B(p, 1-p) = \frac{1}{|\mathcal{D}^\perp|} A(2p-1, 1). \tag{5}$$

III. Noiseless Attacks

A. Evaluation of Mutual Information

In a noiseless attack, the attacker knows $Z^{\mathrm{п}}$ without noise. The question is what quantity of information it can leak about the secret X. The information leakage is classically measured [19, §5] by Shannon's mutual information

$$I(X; Z^{\mathrm{п}}) = H(Z^{\mathrm{п}}) - H(Z^{\mathrm{п}}|X) \tag{6}$$

where $H(\cdot)$ denotes the discrete entropy.

Remark 1: *If $X \sim \mathcal{U}(V)$ where vector space V has dimension d over $\mathbb{F}$ of cardinality 2, then clearly*

$$H(X) = \log_2 |V| = d \text{ bits}. \tag{7}$$

Lemma 1: *Let $\mathbf{A}$ be an $m \times n$ matrix of rank r over $\mathbb{F}$, and $V_{\mathbf{A}} \subset \mathbb{F}^n$ its row space. If $X \sim \mathcal{U}(\mathbb{F}^m)$ is a row random vector*

uniformly distributed over $\mathbb{F}^m$, then $Y = X\mathbf{A} \sim \mathcal{U}(V_{\mathbf{A}})$ is uniformly distributed over $V_{\mathbf{A}}$.

Proof: By the canonical decomposition of the linear application $\Phi : x \mapsto y = x\mathbf{A}$, $\operatorname{Im}\Phi = V_{\mathbf{A}} \cong \mathbb{F}^m/\operatorname{Ker}\Phi$ where $\operatorname{Ker}\Phi$ has dimension $m-r$. In other words $\Phi^{-1}(y) = x + \operatorname{Ker}\Phi$ for any $y \in V_{\mathbf{A}}$.

Now if $X \sim \mathcal{U}(\mathbb{F}^m)$ with $\mathbb{P}(X = x) = \frac{1}{2^m}$ and $Y = X\mathbf{A} = \Phi(X)$, then for any $y \in V_{\mathbf{A}}$, we have

$$\mathbb{P}(Y = y) = \mathbb{P}(X \in \Phi^{-1}(y)) = \mathbb{P}(X \in x + \operatorname{Ker}\Phi)$$
$$= \frac{|\operatorname{Ker}\Phi|}{2^m} = \frac{2^{m-r}}{2^m} = \frac{1}{2^r} = \frac{1}{|V_{\mathbf{A}}|}.$$ ∎

Lemma 2: *One has*

$$H(Z^{\pi}) = d \text{ bits.} \tag{8}$$

Proof: From Lemma 1, $X\mathbf{G} \sim \mathcal{U}(\mathcal{C})$, $Y\mathbf{H} \sim \mathcal{U}(\mathcal{D})$, hence $Z = X\mathbf{G} + Y\mathbf{H} \sim \mathcal{U}(\mathcal{C} \oplus \mathcal{D}) = \mathcal{U}(\mathbb{F}^n)$. It follows that $Z^{\pi} \sim \mathcal{U}(\mathbb{F}^d)$, hence $H(Z^{\pi}) = \log|\mathbb{F}^d| = d$ bits. ∎

Next consider the dual code $\mathcal{D}^{\perp}$. We have $\pi \in \mathcal{D}^{\perp}$ if and only if $\mathbf{H} \cdot \pi^t = \mathbf{H}^{\pi} \cdot (\pi^{\pi})^t = 0$. Thus to every codeword of $\pi \in \mathcal{D}^{\perp}$ of weight d correspond to d linearly dependent columns in $\mathbf{H}^{\pi}$. Now if $d < d_{\mathcal{D}}^{\perp}$ every set of d columns of $\mathbf{H}$ are linearly independent so that $\mathbf{H}^{\pi}$ always has full rank[1] d.

Theorem 1: *Let $d_{\mathcal{D}}^{\perp}$ be the dual distance of the code $\mathcal{D}$. If $d < d_{\mathcal{D}}^{\perp}$ then*

$$I(X; Z^{\pi}) = 0. \tag{9}$$

Proof: Since $\mathbf{H}^{\pi}$ has full rank d, by Lemma 1, $Y\mathbf{H}^{\pi} \sim \mathcal{U}(V_{\mathbf{H}^{\pi}}) = \mathcal{U}(\mathbb{F}^d)$. The conditional distribution of Z^{π} given $X = x$ is then $Z^{\pi}|X = x \sim x\mathbf{G}^{\pi} + \mathcal{U}(\mathbb{F}^d) = \mathcal{U}(\mathbb{F}^d)$, which does not depend of x. Thus Z^{π} is independent of X, that is, $I(X; Z^{\pi}) = 0$. ∎

Hence Z^{π} does not leak any information about the secret. In particular, we recover the following result from [9]: If a polynomial P has numerical degree $< d_{\mathcal{D}}^{\perp}$, then $I(X; P(Z^{\pi})) = 0$.

Theorem 2 (Noiseless Information Leakage): *If an adversary chooses $d = d_{\mathcal{D}}^{\perp}$ probes, then*

$$I(X; Z^{\pi}) = \begin{cases} 1 \text{ bit} & \text{if } \pi \in \mathcal{D}^{\perp} \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

Proof: If $\pi \notin \mathcal{D}^{\perp}$ then the d columns of $\mathbf{H}^{\pi}$ are linearly independent and $\mathbf{H}^{\pi}$ has full rank. Then as in the proof of Theorem 1, $I(X; Z^{\pi}) = 0$.

If $\pi \in \mathcal{D}^{\perp}$ then the d columns of $\mathbf{H}^{\pi}$ are linearly dependent while every subset of less than d columns of $\mathbf{H}$ is linearly independent. Hence $\mathbf{H}^{\pi}$ has rank $d-1$. By Lemma 1, $Y\mathbf{H}^{\pi} \sim \mathcal{U}(V_{\mathbf{H}^{\pi}})$ where $V_{\mathbf{H}^{\pi}}$ has dimension $d-1$, so that $H(Z^{\pi}|X = x) = H(x\mathbf{G}^{\pi} + Y\mathbf{H}^{\pi}) = d-1$ bits. Averaging over X gives $H(Z^{\pi}|X) = d-1$ bits. From Lemma 2, $I(X; Z^{\pi}) = H(Z^{\pi}) - H(Z^{\pi}|X) = d - (d-1) = 1$ bit. ∎

Assuming the attacker chooses her probes' locations at random, let Π be a random vector chosen uniformly among all $\pi \in \mathbb{F}^n$ of weight d. Then we have the following

[1] As a byproduct this gives $d \leqslant m = n - k$ for any $d < d_{\mathcal{D}}^{\perp}$, a proof of Singleton's bound $d_{\mathcal{D}}^{\perp} \leqslant n - k + 1$.

Corollary 1: *If an adversary chooses d positions of probe randomly and $d = d_{\mathcal{D}}^{\perp}$, then on average*

$$I(X; Z^{\Pi}) = \frac{A_d}{\binom{n}{d}} \text{ bits} \tag{11}$$

where $A_d = |\{v \in D^{\perp} \mid w_H(v) = d\}|$ is the kissing number [18] in the weight distribution of the dual code $\mathcal{D}^{\perp}$ and $w_H(v)$ is the Hamming weight of codeword v.

Proof: From Theorem 2, $I(X; Z^{\Pi} \mid \Pi = \pi) = 1$ or 0 according to whether $\pi \in \mathcal{D}^{\perp}$ (A_d possibilities) or not ($\binom{n}{d} - A_d$ possibilities). Averaging over π gives

$$I(X; Z^{\Pi}) = \frac{A_d}{\binom{n}{d}} \times 1 + \frac{\binom{n}{d} - A_d}{\binom{n}{d}} \times 0 = \frac{A_d}{\binom{n}{d}} \text{ bits.}$$ ∎

Theorem 2 can be generalized as follows.

Theorem 3: *If an adversary can choose $d \geqslant d_{\mathcal{D}}^{\perp} = d_{1,\mathcal{D}^{\perp}}$ probes, then the maximum amount of information she can extract is determined by:*

$$\max_{\pi} I(X; Z^{\pi}) = \max\{r \ ; \ d_{r,\mathcal{D}^{\perp}} \leqslant w_H(\pi)\} \text{ bits,} \tag{12}$$

where $d_{r,\mathcal{D}^{\perp}}$ is the rth generalized Hamming weight of the code $\mathcal{D}^{\perp}$.

Proof: Probing $w_H(\pi)$ positions is equivalent with taping $w_H(\pi)$ coordinates of a codeword in the wiretap channel II. Therefore, it is straightforward from [22] that the extractable information is determined by (12). ∎

B. The "Exact Information" Brought by the Attack

Lemma 3: *We have $I(X; Z^{\pi}) = I(X\mathbf{G}^{\pi}; Z^{\pi})$ where (by Lemma 1) $X\mathbf{G}^{\pi} \sim \mathcal{U}(V_{\mathbf{G}^{\pi}})$.*

In other words, the information brought by the attack z^{π} depends on the secret x only through $x\mathbf{G}^{\pi}$.

Proof: Write $I(X; Z^{\pi}) = H(Z^{\pi}) - H(Z^{\pi}|X)$. Since $X\mathbf{G}^{\pi}$ is a deterministic function of X, $H(Z^{\pi}|X) = H(Z^{\pi}|X, X\mathbf{G}^{\pi})$. But since Z^{π} depends on X only through $X\mathbf{G}^{\pi}$, one has $H(Z^{\pi}|X, X\mathbf{G}^{\pi}) = H(Z^{\pi}|X\mathbf{G}^{\pi})$. Hence $I(X; Z^{\pi}) = H(Z^{\pi}) - H(Z^{\pi}|X\mathbf{G}^{\pi}) = I(X\mathbf{G}^{\pi}; Z^{\pi})$. ∎

Lemma 4: *If $\mathbf{H}^{\pi} \cdot (\pi^{\pi})^t = 0$ then $\mathbf{G}^{\pi} \cdot (\pi^{\pi})^t \neq 0$.*

Proof: It is equivalent to prove that if $\pi \in \mathbb{F}^n$ is a non zero vector, then it is impossible to have both $\mathbf{H} \cdot \pi^t = 0$ and $\mathbf{G} \cdot \pi^t = 0$. In other words, this amounts to prove that $\mathcal{C}^{\perp} \cap \mathcal{D}^{\perp} = \{0\}$. Now $\mathcal{C}^{\perp} \cap \mathcal{D}^{\perp} = (\mathcal{C} + \mathcal{D})^{\perp} = (\mathcal{C} \oplus \mathcal{D})^{\perp} = \mathbb{F}^{n\perp} = \{0\}$. ∎

Theorem 4: *If $\pi \in \mathcal{D}^{\perp}$ is of weight $d = d_{\mathcal{D}}^{\perp}$, the "exact information" brought by Z^{π} on the secret x is the bit*

$$x \cdot (\mathbf{G} \cdot \pi^t) \in \mathbb{F}. \tag{13}$$

What is meant here by "exact information" brought by Z^{π} on X is that $I(X; Z^{\pi}) = H(X \cdot (\mathbf{G} \cdot \pi^t)) = 1$ bit where $X \cdot (\mathbf{G} \cdot \pi^t)$ is a function of Z^{π}.

Proof: By Lemma 3, the information brought by z^{π} on x is only on $x' = x\mathbf{G}^{\pi} \in V_{\mathbf{G}^{\pi}}$. By the proof of Theorem 2, $Z^{\pi}|X = x$ is uniformly distributed over $x' + V_{\mathbf{H}^{\pi}} = x' + (\pi^{\pi})^{\perp}$ which covers $V_{\mathbf{G}^{\pi}}/V_{\mathbf{G}^{\pi}} \cap (\pi^{\pi})^{\perp}$.

By Lemma 4, $\mathbf{G}\cdot \mathrm{n}^t = \mathbf{G}^{\mathrm{n}}\cdot(\mathrm{n}^{\mathrm{n}})^t$ is nonzero. It follows that the linear form $\Phi : x' = x\mathbf{G}^{\mathrm{n}} \in V_{\mathbf{G}^{\mathrm{n}}} \mapsto x'\cdot(\mathrm{n}^{\mathrm{n}})^t$ is nonzero, hence $\operatorname{Im}\Phi$ has dimension 1. By the canonical decomposition of Φ, $V_{\mathbf{G}^{\mathrm{n}}}/\operatorname{Ker}\Phi \cong \operatorname{Im}\Phi$ where $\operatorname{Ker}\Phi = V_{\mathbf{G}^{\mathrm{n}}} \cap (\mathrm{n}^{\mathrm{n}})^{\perp}$.

Hence $V_{\mathbf{G}^{\mathrm{n}}}/V_{\mathbf{G}^{\mathrm{n}}} \cap (\mathrm{n}^{\mathrm{n}})^{\perp}$ is canonically isomorphic to $\operatorname{Im}\Phi$. Now we assert that the exact information brought by z^{n} on x' is given by the element $\Phi(x') = x'\cdot(\mathrm{n}^{\mathrm{n}})^t = x\cdot\mathbf{G}^{\mathrm{n}}\cdot(\mathrm{n}^{\mathrm{n}})^t = x\cdot\mathbf{G}\cdot\mathrm{n}^t$. Indeed, given $z = x\mathbf{G} + y\mathbf{H}$, we recover the bit $x\cdot(\mathbf{G}\cdot\mathrm{n}^t)$ by taking

$$x\cdot(\mathbf{G}\cdot\mathrm{n}^t) = z\cdot\mathrm{n}^t \tag{14}$$

where $\mathrm{n}\in\mathcal{D}^{\perp}$. Since $X\cdot(\mathbf{G}\cdot\mathrm{n}^t)\sim\mathcal{U}(\operatorname{Im}\Phi) = \mathcal{U}(\mathbb{F})$ is a deterministic function of Z^{n}, $H(X\cdot(\mathbf{G}\cdot\mathrm{n}^t)) = I(X\cdot(\mathbf{G}\cdot\mathrm{n}^t); Z^{\mathrm{n}})$ $= I(X; Z^{\mathrm{n}}) = 1$ bit. ∎

Remark 2: *Since $x\cdot(\mathbf{G}\cdot\mathrm{n}^t) = z\cdot\mathrm{n}^t$ where $\mathrm{n}\in\mathcal{D}^{\perp}$, the corresponding attack is simply an instance of* syndrome decoding *where $z\cdot\mathrm{n}^t$ is the syndrome.*

IV. Attacks Under Noisy Measurements

In classical side-channel analysis setups [4], [11], the attacker exploits directly the noisy leakage, usually assumed to be equal to the leakage of Z in the presence of some additive white Gaussian noise (AWGN) of variance σ^2. However, such setups require to make an ad-hoc assumption about the leakage model, i.e., a function that transduces a vector of field elements in $\mathbb{F}$ into a real number in $\mathbb{R}$. In order to be more general, we assume in this paper a narrower attack model, which digitizes the measured side-channel leakage for subsequent analysis. This corresponds to the situation of a hard detection or hard decision making—the side-channel is digitized prior to analysis.

Consider a AWGN channel with i.i.d noise $\sim\mathcal{N}(0,\sigma^2)$ in transmitting binary variables, followed by a binary detector. As is well known, the overall channel model becomes a memoryless binary symmetric channel (BSC) of probability $p = Q(\sqrt{\gamma})$ where

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-\frac{t^2}{2}}\,\mathrm{d}t$$

is the Q-function and $\gamma = 1/\sigma^2$ is the actual signal-to-noise ratio (SNR). Therefore, in this section, we consider a discrete noise (a.k.a. binary error vector E) which follows the i.i.d. Bernoulli distribution and show how this discrete noise affects the amount of information an adversary can extract.

Let $E\in\mathbb{F}^n$ be the error vector with i.i.d components $E_i\sim\mathcal{B}(p)$ where $p = \mathbb{P}(E_i = 1)$. In short $E\sim\mathcal{B}(p)^{\otimes n}$. Let

$$Z' = X\mathbf{G} + Y\mathbf{H} + E$$

be the noisy leakage, and considering $d = w_H(\mathrm{n})$ probes gives

$$Z'^{\mathrm{n}} = Z^{\mathrm{n}} + E^{\mathrm{n}} = X\mathbf{G}^{\mathrm{n}} + Y\mathbf{H}^{\mathrm{n}} + E^{\mathrm{n}}. \tag{15}$$

The problem is to evaluate the mutual information $I(X; Z'^{\mathrm{n}})$.

By Theorem 1, d probes provide no information about the sensitive variable X when $d < d_{\mathcal{D}}^{\perp}$. In this case $I(X; Z'^{\mathrm{n}}) = 0$. Therefore, we shall only consider the scenario for which $d = d_{\mathcal{D}}^{\perp}$ with $\mathrm{n}\in\mathcal{D}^{\perp}$. Then, from the analysis of the previous section, $\mathbf{H}^{\mathrm{n}}$ has rank $d-1$ and generates a $[d, d-1]$ parity check code $\mathcal{D}^{\mathrm{n}} = V_{\mathbf{H}^{\mathrm{n}}}$, with the $[d,1]$ repetition code as the dual code $\mathcal{D}^{\mathrm{n}\perp} = \{0, \mathrm{n}^{\mathrm{n}}\}$.

Theorem 5 (Noisy Information Leakage): *In our hard decision probing model with $d = d_{\mathcal{D}}^{\perp}$ with $\mathrm{n}\in\mathcal{D}^{\perp}$, one has*

$$I(X; Z'^{\mathrm{n}}) = 1 - H_2(p^*) \tag{16}$$

where $H_2(p) = -p\log p - (1-p)\log p$ denotes the binary entropy and $p^* = B(p, 1-p) = \sum_i B_i p^i(1-p)^{d-i}$, the weight enumerator polynomial of the code $\mathcal{D}^{\mathrm{n}}$ generated by $\mathbf{H}^{\mathrm{n}}$.
Notice that $0\leqslant p^*\leqslant\sum_i\binom{d}{i}p^i(1-p)^{d-i}\leqslant 1$ hence p^* is a probability.

Proof: Consider $I(X; Z'^{\mathrm{n}}) = H(Z'^{\mathrm{n}}) - H(Z'^{\mathrm{n}}|X)$. Because E is independent of Z, $Z'^{\mathrm{n}} = Z^{\mathrm{n}} + E^{\mathrm{n}}$ is, like Z^{n}, uniformly distributed over $\mathcal{U}(\mathbb{F}^d)$ so that $H(Z'^{\mathrm{n}}) = d$.

The conditioned entropy $H(Z'^{\mathrm{n}}|X = x) = H(x\mathbf{G}^{\mathrm{n}} + Y\mathbf{H}^{\mathrm{n}} + E^{\mathrm{n}}) = H(Y\mathbf{H}^{\mathrm{n}} + E^{\mathrm{n}})$ is independent of the value of x because the probability distribution of $Y\mathbf{H}^{\mathrm{n}} + E^{\mathrm{n}}$ is only affected by the invertible shift operator which adds $x\mathbf{G}^{\mathrm{n}}\in\mathbb{F}^d$. Hence averaging over X gives $H(Z'^{\mathrm{n}}|X) = H(Y\mathbf{H}^{\mathrm{n}} + E^{\mathrm{n}})$.

Now consider the dth extension of the memoryless BSC channel, which transforms each input vector $v\in V_{\mathbf{H}^{\mathrm{n}}} = \mathcal{D}^{\mathrm{n}}$ to some output $v'\in V_{\mathbb{F}^d}$. Noting $p^* = \sum_i B_i p^i(1-p)^{d-i}$, a direct inspection shows that there are two possible cases:

- $v'\in V_{\mathbf{H}^{\mathrm{n}}}$: the probability of each v' is $\frac{p^*}{2^{d-1}}$;
- $v'\notin V_{\mathbf{H}^{\mathrm{n}}}$: the probability of each v' is $\frac{1-p^*}{2^{d-1}}$.

Then we have

$$\begin{aligned} H(Z'^{\mathrm{n}}|X) &= H(Y\mathbf{H}^{\mathrm{n}} + E^{\mathrm{n}}) \\ &= \sum_1^{2^{d-1}}\frac{p^*}{2^{d-1}}\log\frac{2^{d-1}}{p^*} + \sum_1^{2^{d-1}}\frac{1-p^*}{2^{d-1}}\log\frac{2^{d-1}}{1-p^*} \\ &= d - 1 + H_2(p^*), \end{aligned}$$

hence $I(X; Z'^{\mathrm{n}}) = H(Z'^{\mathrm{n}}) - H(Z'^{\mathrm{n}}|X) = 1 - H_2(p^*)$. ∎

Theorem 5 shows that adding noise can only decrease the mutual information $I(X; Z'^{\mathrm{n}})$. In the sequel, we further detail the evaluation of mutual information under weak and strong noise, respectively.

A. Attacks Under Weak Noise

For weak noise we consider $\sigma\to 0$, $\gamma\to+\infty$, and, therefore [2],

$$p = Q(\sqrt{\gamma}) \sim \frac{\mathrm{e}^{-\gamma/2}}{\sqrt{2\pi\gamma}} \tag{17}$$

tends exponentially toward zero. As a result we have the following behavior.

Theorem 6 (Information Leakage Under Weak Noise): *In our hard decision probing model with $d = d_{\mathcal{D}}^{\perp}$ with $\mathrm{n}\in\mathcal{D}^{\perp}$, as $\sigma\to 0$ (hence $p\to 0$), one has the asymptotic equivalence*

$$1 - I(X; Z'^{\mathrm{n}}) \sim \frac{d\cdot\mathrm{e}^{-1/2\sigma^2}}{2\sqrt{2\pi\sigma^2}} \to 0. \tag{18}$$

Proof: Applying MacWilliams' identity (5) to the code $\mathcal{D}^{\mathrm{n}} = V_{\mathbf{H}^{\mathrm{n}}}$, whose dual code $\mathcal{D}^{\mathrm{n}\perp}$ is the $[d,1]$ repetition code, we obtain

$$p^* = \frac{1}{2}\sum_{i=0}^{d} A_i(2p-1)^i = \frac{1+(2p-1)^d}{2}$$

Since $p \to 0$, according to whether d is even or odd, $p^* \to 1$ or $p^* \to 0$. Hence $H_2(p^*) \to 0$ is equivalent to either $-(1-p^*)\log(1-p^*)$ or $-p^* \log p^*$. Therefore, $1-I(X;Z'^{\text{п}}) = H_2(p^*) \sim -pd\log(pd) \sim -pd\log(p) \sim \frac{\gamma d e^{-\gamma/2}}{2\sqrt{2\pi\gamma}}$ where $\gamma = \sigma^{-2}$, which yields the announced formula . ∎

Since $I(X;Z'^{\text{п}})$ will tend to 1 when the noise approaches zero, one recovers Theorem 2 in the noiseless case.

B. Attacks Under Strong Noise

One of the main benefits of masking is that, under sufficient strong noise, the number of measurements to recover the secret key used in a masked cryptographic implementation increases exponentially with the protection order (indicated by the dual distance in code-based masking). Herein we investigate the asymptotic features of information leakage quantified by $I(X;Z'^{\text{п}})$ under a strong noise, i.e., when $\sigma \to +\infty$, $\gamma \to 0$ so that $p \to \frac{1}{2}$.

Theorem 7 (Information leakage under strong noise): *In our hard decision probing model with $d = d_{\mathcal{D}}^{\perp}$ with $\text{п} \in \mathcal{D}^{\perp}$, as $\sigma \to +\infty$, one has the following equivalence:*

$$I(X;Z'^{\text{п}}) \sim \frac{2^{d-1}}{\pi^d \cdot \ln 2} \cdot \sigma^{-2d}, \tag{19}$$

where d is the minimum distance of the dual code of the code generated by $\mathbf{H}^{\text{п}}$.

Proof: By first-order Taylor expansion, $Q(x) = \frac{1}{2} - \frac{1}{\sqrt{2\pi}}\int_0^x \mathrm{e}^{\frac{-t^2}{2}} dt = \frac{1}{2} - \frac{x}{\sqrt{2\pi}} + o(x)$ and $p = Q(\sqrt{\gamma}) = \frac{1}{2} - \sqrt{\frac{\gamma}{2\pi}} + o(\sqrt{\gamma}) = \frac{1}{2} - \varepsilon + o(\varepsilon)$ where $\varepsilon = \sqrt{\frac{\gamma}{2\pi}} = \frac{1}{\sqrt{2\pi\sigma^2}} \to 0$ when $\sigma \to +\infty$.

Applying MacWilliams' identity (5) to $\mathcal{D}^{\text{п}} = V_{\mathbf{H}^{\text{п}}}$, we obtain

$$p^* = \frac{1}{2}\sum_{i=0}^{d} A_i (2p-1)^i = \frac{1}{2} - 2^{d-1}\varepsilon^d + o(\varepsilon^d).$$

Now by Taylor's expansion at second order for the entropy $H_2(p^*)$ is $H_2(\frac{1}{2}) + H'(\frac{1}{2})(\frac{1}{2}-p^*) + \frac{1}{2}H''(\frac{1}{2})\cdot(\frac{1}{2}-p^*)^2 = 1 - 2\log_2(\mathrm{e})\cdot(\frac{1}{2}-p^*)^2$. Finally, we have

$$\begin{aligned} I(X;Z'^{\text{п}}) = 1 - H_2(p^*) &\sim 2\log_2(\mathrm{e}) \cdot \left(2^{d-1}\varepsilon^d\right)^2 \\ &= 2^{2d-1}\varepsilon^{2d} \cdot \log_2(\mathrm{e}) \\ &= \frac{2^{d-1}}{\pi^d \cdot \ln 2} \cdot \sigma^{-2d} \end{aligned}$$

∎

Theorem 7 shows that the mutual information between the sensitive variable X and the noisy measurements is exponentially decreasing in σ^2 with an exponent equal to the protection order d (dual distance).

C. Numerical Simulations

To verify our theoretical findings, we carried out numerical experiments based on Monte-Carlo simulation. To simplify, we chose the simplest code-based masking with varying n given in Example 1. Here $\mathbf{H}^{\perp} = (1_n)$ generates a repetition code with the minimum distance n, which is thus equal to the dual distance the code generated by $\mathbf{H}$. We generated random draws

- $X \sim \mathcal{U}(\mathbb{F}_2)$,
- $Y \sim \mathcal{U}(\mathbb{F}_2^{n-1})$,
- $Z = X\mathbf{G} + Y\mathbf{H} \sim \mathcal{U}(\mathbb{F}_2^n)$,
- $E \in \mathbb{F}_2^n$ such that $E_i \sim \mathcal{B}(p)$ with various p,
- $Z' = Z + E \in \mathbb{F}_2^n$, and $Z'^{\text{п}} = Z^{\text{п}} + E^{\text{п}} \in \mathbb{F}_2^d$ where $d = w_H(\text{п})$ (and accordingly, $A_d = 1$).

Since the dual distance of the corresponding code $\mathcal{D}$ is $d_{\mathcal{D}}^{\perp} = n$, we select $d = n$ probes in our simulation.

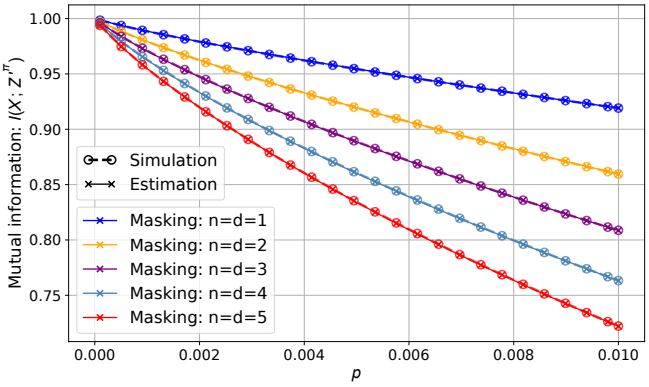

Fig. 3. Numerical evaluation and theoretical estimation of mutual information $I(X;Z'^{\text{п}})$ for $n \in \{1,2,3,4,5\}$ under weak noise. Note that $d = w_H(\text{п})$ is the number of attacker's probes and the estimation is calculated by Theorem 6.

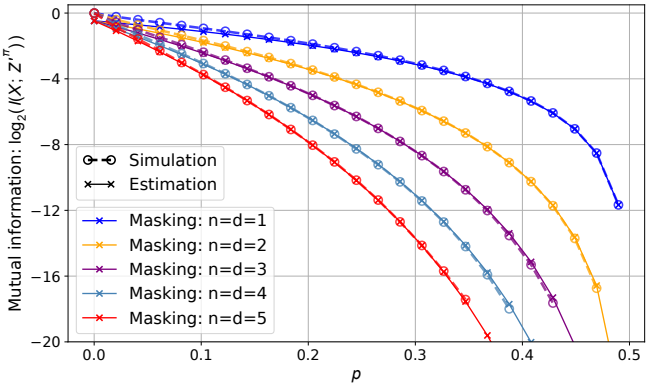

Fig. 4. Numerical evaluation and theoretical estimation of mutual information $I(X;Z'^{\text{п}})$ for $n \in \{1,2,3,4,5\}$ under strong noise. Note that $d = w_H(\text{п})$ is the number of attacker's probes and the estimation is calculated by Theorem 7.

The numerical results of mutual information $I(X;Z'^{\text{п}})$, along with the corresponding theoretical estimation of Theorem 6 and 7, are shown in Fig. 3 and 4 for weak and strong noises, respectively. Note that Fig. 4 is plotted in logarithmic scale to highlight the small values of mutual information under strong noise. Particularly, Fig. 4, shows that Theorem 7 gives very accurate approximation when p is greater than 0.1.

Overall, we obtain an accurate evaluation of the commonly adopted assumption that the information leakage decreases exponentially in masking order under sufficient noise [1], [12].

V. Conclusion

We have investigated how a code-based masked implementation leaks in an information-theoretic setting, where mutual information measures the impact of both number and positions of probes in the probing attack model, without or with additive measurement noise. This allowed us to demonstrate the notion of probing security order.

From the situation where one probe is missing (hence a zero mutual information between the leakage and the secret), we

show that each additional probe brings a maximum of *one* bit of information. Interestingly, this additional advantage is irrespective of the position of the probes, provided that Π lies in the dual code $\mathcal{D}^{\perp}$. This shows that there is no optimal strategy to position the probes except in increasing the gained information by an integral number of bits. On the opposite, it can happen that adding one more probe surprisingly brings no further information to the adversary, and we characterize such cases with a notion of generalized Hamming weight.

We also explore how noise impacts the mutual information: For low noise, the mutual information is little impacted, while for high noise, the mutual information is vanishing at least as σ^{-2d} with d probes, where d is equal to or greater than the dual distance of the masking code. This shows that masking is more and more efficient as the measurement noise and protection order increase.

As a perspective, one may consider a generalization of the rate of decrease of mutual information as noise variance increases for more general leakage, as studied (informally) under the terms of high-order correlation immunity (HCI [5]), as well as the constructions of optimal linear codes in code-based masking.

REFERENCES

[1] J. Balasch, S. Faust, B. Gierlichs, C. Paglialonga, and F. Standaert, "Consolidating Inner Product Masking," in *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, ser. Lecture Notes in Computer Science, T. Takagi and T. Peyrin, Eds., vol. 10624. Springer, 2017, pp. 724–754. [Online]. Available: https://doi.org/10.1007/978-3-319-70694-8_25

[2] P. O. Börjesson and C. W. Sundberg, "Simple Approximations of the Error Function $Q(x)$ for Communications Applications," *IEEE Trans. Commun.*, vol. 27, no. 3, pp. 639–643, 1979. [Online]. Available: https://doi.org/10.1109/TCOM.1979.1094433

[3] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, and H. Maghrebi, "Orthogonal Direct Sum Masking - A Smartcard Friendly Computation Paradigm in a Code, with Builtin Protection against Side-Channel and Fault Attacks," in *Information Security Theory and Practice. Securing the Internet of Things - 8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Crete, Greece, June 30 - July 2, 2014. Proceedings*, ser. Lecture Notes in Computer Science, D. Naccache and D. Sauveron, Eds., vol. 8501. Springer, 2014, pp. 40–56. [Online]. Available: https://doi.org/10.1007/978-3-662-43826-8_4

[4] N. Bruneau, S. Guilley, A. Heuser, and O. Rioul, "Masks Will Fall Off – Higher-Order Optimal Distinguishers," in *Advances in Cryptology – ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, ser. Lecture Notes in Computer Science, P. Sarkar and T. Iwata, Eds., vol. 8874. Springer, 2014, pp. 344–365. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-45608-8_19

[5] C. Carlet, J.-L. Danger, S. Guilley, H. Maghrebi, and E. Prouff, "Achieving Side-Channel High-Order Correlation Immunity With Leakage Squeezing," *J. Cryptographic Engineering*, vol. 4, no. 2, pp. 107–121, 2014.

[6] C. Carlet and S. Guilley, "Statistical Properties of Side-Channel and Fault Injection Attacks Using Coding Theory," *Cryptography and Communications*, vol. 10, no. 5, pp. 909–933, 2018. [Online]. Available: https://doi.org/10.1007/s12095-017-0271-4

[8] W. Cheng, S. Guilley, C. Carlet, J. Danger, and S. Mesnager, "Information Leakages in Code-based Masking: A Unified Quantification Approach," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2021, no. 3, pp. 465–495, 2021. [Online]. Available: https://doi.org/10.46586/tches.v2021.i3.465-495

[7] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards Sound Approaches to Counteract Power-Analysis Attacks," in *CRYPTO*, ser. Lecture Notes in Computer Science, M. J. Wiener, Ed., vol. 1666. Springer, 1999, pp. 398–412.

[9] W. Cheng, S. Guilley, C. Carlet, S. Mesnager, and J.-L. Danger, "Optimizing Inner Product Masking Scheme by a Coding Theory Approach," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 220–235, 2021. [Online]. Available: https://doi.org/10.1109/TIFS.2020.3009609

[10] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," in *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES '01. London, UK, UK: Springer-Verlag, 2001, pp. 251–261. [Online]. Available: http://dl.acm.org/citation.cfm?id=648254.752700

[11] A. Heuser, O. Rioul, and S. Guilley, "Good Is Not Good Enough - Deriving Optimal Distinguishers from Communication Theory," in *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, ser. Lecture Notes in Computer Science, L. Batina and M. Robshaw, Eds., vol. 8731. Springer, 2014, pp. 55–74. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-44709-3_4

[12] Y. Ishai, A. Sahai, and D. Wagner, "Private Circuits: Securing Hardware against Probing Attacks," in *CRYPTO*, ser. Lecture Notes in Computer Science, vol. 2729. Springer, August 17–21 2003, pp. 463–481, Santa Barbara, California, USA.

[13] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *CRYPTO*, ser. Lecture Notes in Computer Science, M. J. Wiener, Ed., vol. 1666. Springer, 1999, pp. 388–397.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Elsevier, Amsterdam, North Holland, 1977, ISBN: 978-0-444-85193-2.

[15] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, December 2006, ISBN 0-387-30857-1, http://www.dpabook.org/.

[16] L. H. Ozarow and A. D. Wyner, "Wire-Tap Channel II," *AT&T Bell Laboratories Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[17] R. Poussier, Q. Guo, F. Standaert, C. Carlet, and S. Guilley, "Connecting and Improving Direct Sum Masking and Inner Product Masking," in *Smart Card Research and Advanced Applications - 16th International Conference, CARDIS 2017, Lugano, Switzerland, November 13-15, 2017, Revised Selected Papers*, ser. Lecture Notes in Computer Science, T. Eisenbarth and Y. Teglia, Eds., vol. 10728. Springer, 2017, pp. 123–141. [Online]. Available: https://doi.org/10.1007/978-3-319-75208-2_8

[18] P. Solé, Y. Liu, W. Cheng, S. Guilley, and O. Rioul, "Linear Programming Bounds on the Kissing Number of q-ary Codes," in *IEEE Information Theory Workshop, ITW 2021, Kanazawa, Japan, October 17-21, 2021*. IEEE, 2021, pp. 1–5. [Online]. Available: https://doi.org/10.1109/ITW48936.2021.9611478

[19] N. Veyrat-Charvillon and F. Standaert, "Mutual Information Analysis: How, When and Why?" in *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings*, ser. Lecture Notes in Computer Science, C. Clavier and K. Gaj, Eds., vol. 5747. Springer, 2009, pp. 429–443. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-04138-9_30

[20] J. Waddle and D. A. Wagner, "Towards Efficient Second-Order Power Analysis," in *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, ser. Lecture Notes in Computer Science, M. Joye and J. Quisquater, Eds., vol. 3156. Springer, 2004, pp. 1–15. [Online]. Available: https://doi.org/10.1007/978-3-540-28632-5_1

[21] W. Wang, P. Méaux, G. Cassiers, and F. Standaert, "Efficient and Private Computations with Code-Based Masking," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2020, no. 2, pp. 128–171, 2020. [Online]. Available: https://doi.org/10.13154/tches.v2020.i2.128-171

[22] V. K. Wei, "Generalized Hamming Weights for Linear Codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991. [Online]. Available: https://doi.org/10.1109/18.133259

[23] M. J. Wiener, Ed., *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, ser. Lecture Notes in Computer Science, vol. 1666. Springer, 1999.