IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2024, No. 2, pp. 384–402. DOI:10.46586/tches.v2024.i2.384-402

Distribution of Signal to Noise Ratio and Application to Leakage Detection

Mathieu des Noes[1]

CEA - Université Grenoble Alpes, Grenoble, France, mathieu.desnoes@cea.fr

Abstract. In the context of side-channel attacks, the Signal to Noise Ratio (SNR) is a widely used metric for characterizing the information leaked by a device when handling sensitive variables. In this paper, we derive the probability density function (p.d.f.) of the signal to noise ratio (SNR) for the byte value and Hamming Weight (HW) models, when the number of traces per class is large and the target SNR is small. These findings are subsequently employed to establish an SNR threshold, guaranteeing minimal occurrences of false positives. Then, these results are used to derive the theoretical number of traces that are required to remain below pre-defined false negative and false positive rates. The sampling complexity of the T-test, ρ-test and SNR is evaluated for the byte value and HW leakage model by simulations and compared to the theoretical predictions. This allows to establish the most pertinent strategy to make use of each of these detection techniques.

Keywords: Leakage · Side-Channel · Signal to noise Ratio · Sampling Complexity

1 Introduction

Leakage detection consists in identifying the information leaked by a device when processing a sensitive data [WO19]. This information can then be employed in a second phase for template [CRR03] or machine learning [CDP17] attacks. This is particularly relevant for selecting Points of Interest (POI) in a template attack [DS16]. In this paper, we focus on detecting information leakage and do not address its exploitation. Moreover, only univariate methods that do not combine different samples from one trace are considered. Leakage detection procedures decide for one of the two hypotheses:

- $\mathcal{H}_0$: there is no evidence of leakage within the trace
- $\mathcal{H}_1$: there is some leakage

where a model is given to characterize the leakage of information and a metric is defined to decide for one of the two hypotheses.

Hamming Weight (HW) and byte value are two commonly used leakage models in the existing literature [MOP08]. The HW model assumes that the deterministic part of the leakage produced is in a linear relation with the HW of the processed data. For example, it is applied to model the signal when reading or writing data on memory via a communication bus [MOP08]. On the other hand, the byte value model assumes that the amount of leakage produced depends on the value of the processed byte and thus varies for all byte values. It is more generic than the HW model since it makes fewer assumptions.

The T-test [CdMG+13], χ^2-test [MRSS18], ρ-test (Pearson's correlation coefficient) [DS16], Signal to Noise Ratio (SNR) [Man04] and Mutual Information (MI) [MOBW13] are the most popular techniques used to detect information leakage. These detection methods have different properties and usage conditions. While T-tests and χ^2-tests indicate the

Received: 2023-10-15 Accepted: 2023-12-15 Published: 2024-03-12

presence or absence of leakage, they do not offer information on its exploitability. Leakage detection with MI is appealing because it is leakage-model-agnostic, meaning that it is robust to wrong a priori leakage model assumptions [VS09]. In addition, it is a good predictor of security against differential power analysis [SMY06] [MOS09]. However, it needs an accurate estimation of the signal's probability density function (p.d.f.) which is known to be a computational intensive task [MOBW13]. This is the reason why this technique is not addressed in this paper.

The ρ-test detects univariate linear dependency between a leakage model and the trace. SNR is also an univariate kind of test that detects dependences located at first-order statistical moment. Unlike T-test and χ^2-test, SNR provides information about exploitability of the leakage since it is linked to the mutual information through the capacity of the observation channel ($C = 1/2 \log_2(1 + SNR)$) and the success rate [dCGRP19]. Similarly, ρ-tests is also informative because it is related to the SNR [Man04]. However a mathematical leakage model must be defined before performing the computation. The SNR method is thus attractive because it is informative and does not need to make restrictive assumption on the leakage model.

Once a metric is chosen, the evaluator must interpret the results in order to decide for hypothesis $\mathcal{H}_0$ or $\mathcal{H}_1$. Practically, the result is compared to a detection threshold γ in order to decide whether or not to reject the hypothesis $\mathcal{H}_0$. The value of γ is set according to a pre-determined false positive rate (also known as false alarm rate), $\alpha = \int_{\gamma}^{\infty} p(x|\mathcal{H}_0)dx$, where $p(x|\mathcal{H}_0)$ is the probability density function (p.d.f.) of the decision metric under the hypothesis $\mathcal{H}_0$ [Poo94, Chapter 2]. Though an important performance criterion is not taken into account: the false negative rate $\beta = \int_{-\infty}^{\gamma} p(x|\mathcal{H}_1)dx$. A false negative (also known as missed detection) happens when the decision metric is smaller than γ while leakage is present ($\mathcal{H}_1$). One would like to minimize both α and β, but it is known from detection theory that a trade-off must be made. If γ is increased α will be reduced at the expense of β. Usually, the number of traces N is the parameter that allows to satisfy the two constraints. In fact, the variance of the metric is usually inversely proportional to N (e.g. sample mean variance). If γ is fixed and N is increased, the p.d.f. $p(x|\mathcal{H}_1)$ will concentrate around its mean value and β decreases. In order to estimate the false negative rate, the probability distribution $p(x|\mathcal{H}_1)$ must be known. In a nutshell, we are seeking for each detection metric a theoretical formula for $p(x|\mathcal{H}_0)$ and $p(x|\mathcal{H}_1)$.

Under the hypothesis $\mathcal{H}_0$, the p.d.f. is known for the T-test [CdMG+13], χ^2-test [MRSS18], ρ-test [Man04] and SNR for the byte value model [BDGN14] [CK14]. Under the hypothesis $\mathcal{H}_1$, the p.d.f. is known for the ρ-test [Man04] and the T-test (with equal class sizes) [WO19]. Consequently, **the p.d.f. of the SNR is unknown for the byte value model under hypothesis $\mathcal{H}_1$ and the HW model under both hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$**. The motivation of this article is thus to derive these formula and exploit them.

The **contributions** of this paper may be summarized as follows:

1. First, we exhibit the p.d.f. of the SNR for the byte value and HW models and under $\mathcal{H}_0$ and $\mathcal{H}_1$ hypotheses. To do so, we make use of a Gaussian approximation, that we mathematically and experimentally validate under a small SNR assumption. The proposed approximation allows to obtain a light and handy p.d.f. formulation which helps for instance to link in an exploitable way α, N and the number of classes. This is not possible with the F-distribution formula because it mixes all these parameters in a complex way and its inverse is not easily tractable.

2. Second, the obtained probability distributions are used to derive the theoretical number of traces that are required to remain simultaneously below the false positive and false negative rates α and β. This evaluation of the sampling complexity is made for the SNR and ρ-test methods. This is an extension of the work described in [WO19] for the T-test.

3. Third, we compare the T-test, χ^2-test, ρ-test and SNR-based detection method in terms of sampling complexity by means of simulations and experimental results. Comparisons are performed over both byte value and HW models. The sampling complexity is found minimum for the T-test and maximum for the SNR-based detection method.

4. Finally, observing that the obtained results are in accordance to the theoretical predictions, we make use of such theoretical models in order to establish the most pertinent strategy to make use of each of the T-test, χ^2-test, ρ-test and SNR-based detection techniques.

Paper organization Section 2 provides a definition of the Signal to Noise Ratio (SNR) and an explanation of the methodology used to compute various probability density functions (p.d.f.). In Section 3, we derive the p.d.f. of the signal variance S, noise variance B and SNR Z. In Section 4, these models are validated using samples obtained from both simulation and experiments conducted on traces from the ASCADv2 dataset. Subsequently, in Section 5, the optimal threshold γ, i.e. the one that minimizes the false alarms rate, is calculated for each metric. This threshold is then used to derive the theoretical sampling complexity of each detection test. These models are finally compared to simulation results and validated with traces from the ASCADv2 dataset.

Notations The device processes a sensitive random data X resulting in a leakage $T = f(X) + W$ where $f(.)$ is the leakage function and $W \sim \mathcal{N}(0, \sigma^2)$ an additive Gaussian noise. Typically, X is a 8, 16 or 32 bits word. If $f(X)$ is the Hamming weight function, 'HW8' denotes a test when X is a byte and 'HW32' when X is a 32 bits word. While acquiring the n^{th} trace, the device handles the sensitive variable x_n which is a realization of X. Traces are classified based on the values of the leakage function $f(x_n)$. A class is defined by one of the possible value of $f(x_n)$. All variables x_n having the same leakage $f(x_n)$ belong to the same class. Given the assumption made on the leakage function $f(.)$, there are K classes (e.g. $K = 9$ for the HW of a data byte). Also, as a notation abuse, we state that x_n belongs to class k if $f(x_n)$ belongs to class k. Ω_k represents the set of indices of traces that belong to class $k \in [0, K-1]$.

2 SNR as a leakage detection method

A side-channel trace is a vector of non-invasive observations, such as power consumption or electromagnetic radiation, captured while processing a sensitive variable. For our theoretical work, we assume this vector includes only one element (univariate) to simplify notations. When the device processes the sensitive random variable X_n belonging to class k, the leakage for the n^{th} trace is: $T_n = f_k + W_n$. The signal's deterministic component for class k is labeled f_k. $W_n \sim \mathcal{N}(0, \sigma^2)$ is an additive Gaussian noise. We define the subsequent random variables: the mean of the signal for all traces belonging to the same class k, denoted as $M_k = E[T_{n\in\Omega_k}]$ and its variance, denoted as $V_k = Var[T_{n\in\Omega_k}]$.
The SNR is defined by [MOP08]:

$$\begin{aligned} Z &= \frac{S}{B} \\ S &= Var\left(M_k\right) \\ B &= E\left[V_k\right] \end{aligned} \tag{1}$$

Z, S and B are random variables. The true SNR is defined by $\theta = \dfrac{var(f_k)}{\sigma^2}$.
Moreover, hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ are defined as follows:

- $\mathcal{H}_0$: $var(f_k) = 0$

- $\mathcal{H}_1$: $var(f_k) \neq 0$

In order to derive the p.d.f. of Z, the starting point of our work is the following property. If S and B are approximated by Gaussian random variables $B \sim \mathcal{N}(\mu_B, \sigma_B^2)$ and $S \sim \mathcal{N}(\mu_S, \sigma_S^2)$, then, the p.d.f. of Z is defined by [Sim02]:

$$\begin{aligned} p_Z(z) &= \frac{\sigma_B \sigma_S}{\pi(\sigma_B^2 z^2 + \sigma_S^2)} \exp\left[-\frac{1}{2}\left(\frac{\mu_B^2}{\sigma_B^2} + \frac{\mu_S^2}{\sigma_S^2}\right)\right] \\ &+ \frac{\mu_B \sigma_S^2 + \mu_S \sigma_B^2 z}{\sqrt{2\pi}(\sigma_B^2 z^2 + \sigma_S^2)^{3/2}} \exp\left(-\frac{(\mu_S - \mu_B z)^2}{2(\sigma_B^2 z^2 + \sigma_S^2)}\right) A \\ A &= \left[1 - 2\mathcal{Q}\left(\frac{\mu_B \sigma_S^2 + \mu_S \sigma_B^2 z}{\sigma_B \sigma_S (\sigma_B^2 z^2 + \sigma_S^2)^{1/2}}\right)\right] \end{aligned} \tag{2}$$

where $\mathcal{Q}(x)$ is the tail distribution function of the standard normal distribution:

$$\mathcal{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{t^2}{2}\right) dt \tag{3}$$

Our goal is to utilize the theoretical formulation of p_Z to determine the detection threshold γ and the sampling complexity of the SNR method. To do so, we will calculate the p.d.f. of S and B under hypotheses $\mathcal{H}_0$ or $\mathcal{H}_1$ and find their mean and variance. This information will be used to derive the p.d.f. of Z.

3 Approximation of the probability density function of S, B and Z

3.1 Analysis of S

3.1.1 Hypothesis $\mathcal{H}_1$

We assume that N traces have been acquired, with $|\Omega_k| = N_k$ traces per class. For the sake of generality, this number is not the same for all of the classes. Let also $P(k)$ be the probability to draw a variable belonging to class k. According to the leakage model defined in the previous section, $T_n \sim \mathcal{N}(f_k, \sigma^2)$ is i.i.d. when $n \in \Omega_k$. Under this model, M_k and S may be estimated in the following way:

$$\begin{aligned} \hat{M}_k &= \frac{1}{N_k} \sum_{n \in \Omega_k} T_n \\ \hat{S} &= \sum_{k=0}^{K-1} P(k)(\hat{M}_k - \bar{M})^2 \end{aligned} \tag{4}$$

where $\bar{M} = \sum_{k=0}^{K-1} P(k)\hat{M}_k$.

Proposition 1. *For large N_k and K, the p.d.f. of $\hat{S}$ is approximated by a Gaussian distribution $\mathcal{N}(\mu_{\hat{S}}, \sigma_{\hat{S}}^2)$ with:*

$$\begin{aligned} \mu_{\hat{S}} &= \sigma_f^2 + \sigma^2 \frac{K-1}{N} \\ \sigma_{\hat{S}}^2 &= 2\sigma^4 I_1 + 4\sigma^2 I_2 \end{aligned} \tag{5}$$

I_1 and I_2 are defined by:

$$\begin{aligned} I_1 &= \frac{K + 1 + \sum_{k=0}^{K-1} P(k)^2}{N^2} \\ I_2 &= \frac{1}{N} \sum_{k=0}^{K-1} \left(P(k) + P(k)^2\right) (f_k - \mu_f)^2 \end{aligned}$$

μ_f, σ_f^2 and N are defined by:

$$\begin{aligned}\mu_f &= \textstyle\sum_{k=0}^{K-1} P(k) f_k \\ \sigma_f^2 &= \textstyle\sum_{k=0}^{K-1} P(k) \left(f_k - \mu_f\right)^2 \\ N &= \textstyle\sum_{k=0}^{K-1} N_k\end{aligned}$$

Proof. Let us define $E_k = \hat{M}_k - \bar{M}$. It is decomposed into a sum of $\hat{M}_i$'s:

$$E_k = \left(1 - P(k)\right) \hat{M}_k - \sum_{i \neq k} P(i) \hat{M}_i$$

$\hat{M}_i$ is a sum of i.i.d. Gaussian random variable and is thus also Gaussian. Moreover, $\hat{M}_i$'s are independent since they belong to different sets of traces and classes ($\Omega_i \cap \Omega_j = \emptyset$ for $i \neq j$) and the noise variables W_n are independent. Consequently, E_k is a sum of independent Gaussian variables and thus follows a Gaussian distribution.
In addition, after some cumbersome computation, the covariance of E_k and E_j is given by:

$$cov(E_k, E_j) = \sigma^2 \left(\sum_{i=0}^{K-1} \frac{P(i)^2}{N_i} - \frac{P(k)}{N_k} - \frac{P(j)}{N_j} \right)$$

We also note that $N_k \approx P(k)N$ which leads to the following approximation: $cov(E_k, E_j) \approx -\sigma^2/N$. It converges towards zero for large N. E_k and E_j are thus asymptotically uncorrelated and consequently independent (because they are Gaussian).
If E_k's are independent random variables with finite variance, according to Lindeberg's version of the Central Limit Theorem (CLT) [AL06], $\hat{S}$ converges towards a Gaussian distribution for large K. Since the W_n's are i.i.d., according to the Central Limit Theorem (CLT), $\hat{M}_k \sim \mathcal{N}(f_k, \sigma^2/N_k)$. Consequently, we also have $\bar{M} \sim \mathcal{N}\left(\sum_{k=0}^{K-1} P(k) f_k, \sigma^2 \sum_{k=0}^{K-1} P(k)^2 \frac{1}{N_k}\right)$.
The mean $\mu_{\hat{S}}$ and variance $\sigma_{\hat{S}}^2$ are computed with the ones of $\hat{M}_k$ and $\bar{M}$. The result is given by Eq. 5. □

3.1.2 Hypothesis $\mathcal{H}_0$

When there is no leakage, it is possible to compute the probability density function of $\hat{S}$ without relying on the central limit theorem for large K.

Proposition 2. *When $var(f_k) = 0$, the p.d.f. of $\hat{S}$ is:*

$$p_{\hat{S}}(x) = C \sum_{k=0}^{\infty} \delta_k x^{(H/2+k-1)} \exp^{-x/\lambda} / \left(\Gamma\left(\frac{H}{2} + k\right) \lambda^{\rho+k} \right) \tag{6}$$

where

$$\begin{aligned}\sigma_{u_k}^2 &= \frac{\sigma^2}{N} \left(1 - P(k)\right) \\ \lambda &= 2 \min_k \sigma_{u_k}^2 \\ \delta_k &= \frac{1}{k+1} \sum_{i=1}^{k+1} i \nu_{i-1} \delta_{k+1-i} \quad \textit{with } \delta_0 = 1 \\ \nu_k &= \frac{1}{2} \sum_{i=0}^{K-1} \left(1 - \frac{\lambda}{2\sigma_{u_i}^2}\right)^{k+1} \frac{1}{k+1} \\ C &= \prod_{i=0}^{K-1} \left(\frac{\lambda}{2\sigma_{u_k}^2}\right)^{\frac{1}{2}}\end{aligned} \tag{7}$$

and $\Gamma(.)$ is the Gamma function.

Proof. $\hat{S}$ is the sum of K independent random variables with non equal variances:

$$\hat{S} = \sum_{k=0}^{K-1} U_k^2 \tag{8}$$

where $U_k = \sqrt{P(k)}E_k \sim \mathcal{N}(0, \sigma_{U_k}^2)$ with $\sigma_{U_k}^2 = \frac{\sigma^2}{N}(1 - P(k))$

If $U_k \sim \mathcal{N}(0, \sigma_{u_k}^2)$ then U_k^2 follows a gamma distribution: $U_k^2 \sim \Gamma(1/2, 2\sigma_{U_k}^2)$. The p.d.f. of a sum of independent gamma random variables with unequal variances is defined by Eq. 6, with parameters given in Eq. 7 [Mos85]. □

3.2 Analysis of B

B is estimated as follows:

$$\begin{aligned} \hat{B} &= \sum_{k=0}^{K-1} P(k)\hat{V}_k \\ \hat{V}_k &= \frac{1}{N_k - 1} \sum_{n \in \Omega_k} (T_n - \hat{M}_k)^2 \end{aligned} \tag{9}$$

where $\hat{M}_k$ is defined by Eq. 4. The analysis of $\hat{B}$ is the same under hypothesis $\mathcal{H}_1$ or $\mathcal{H}_0$ because the leakage variable f_k is eliminated in the subtraction $T_n - \hat{M}_k$.
Applying the same reasoning as in the previous section, variables $T_n - \hat{M}_k$ are Gaussian and asymptotically independent for large N_k's. By application of the CLT, $\hat{V}_k$ converges towards a Gaussian distribution. The $\hat{V}_k$'s are also independent because the T_n's are taken from different set of traces and the noise variables W_n are independent. As a result, $\hat{B}$ is a sum of K independent Gaussian random variables and is thus Gaussian itself: $\hat{B} \sim \mathcal{N}(\mu_{\hat{B}}, \sigma_{\hat{B}}^2)$. After some computations, the mean $\mu_{\hat{B}}$ and variance $\sigma_{\hat{B}}^2$ have the following expressions:

$$\begin{aligned} \mu_{\hat{B}} &= \sigma^2 \\ \sigma_{\hat{B}}^2 &= \frac{2\sigma^4}{N} \end{aligned} \tag{10}$$

3.3 Analysis of Z

3.3.1 Hypothesis $\mathcal{H}_1$

When $\hat{S}$ and $\hat{B}$ have Gaussian distributions, the p.d.f. of the SNR $\hat{Z} = \hat{S}/\hat{B}$ is defined by Eq. 2. This equation is challenging to apply in practical situations. We will demonstrate how it can be approximated by a Gaussian p.d.f. in our context (large K, large N and small SNR). Let us first focus on the first term of the Eq. 2:

$$I = \frac{\sigma_{\hat{B}}\sigma_{\hat{S}}}{\pi(\sigma_{\hat{B}}^2 z^2 + \sigma_{\hat{S}}^2)} \exp\left[-\frac{1}{2}\left(\frac{\mu_{\hat{B}}^2}{\sigma_{\hat{B}}^2} + \frac{\mu_{\hat{S}}^2}{\sigma_{\hat{S}}^2}\right)\right]$$

We replace $\mu_{\hat{B}}$ and $\sigma_{\hat{B}}^2$ by their expressions defined in Eq. 10. We thus have: $\frac{\mu_{\hat{B}}^2}{\sigma_{\hat{B}}^2} = N/2$. In practical situations, N is very large which leads to a very high value for $\frac{\mu_{\hat{B}}^2}{\sigma_{\hat{B}}^2}$. As a result, the term $\exp\left[-\frac{1}{2}\left(\frac{\mu_{\hat{B}}^2}{\sigma_{\hat{B}}^2}\right)\right]$ will force I to zero. This first component can thus be

assumed negligible.
Let now focus on the last term of Eq. 2:

$$A = \left[1 - 2\mathcal{Q}\left(\frac{\mu_{\hat{B}}\sigma_{\hat{S}}^2 + \mu_{\hat{S}}\sigma_{\hat{B}}^2 z}{\sigma_{\hat{B}}\sigma_{\hat{S}}(\sigma_{\hat{B}}^2 z^2 + \sigma_{\hat{S}}^2)^{1/2}}\right)\right]$$

Let us define the following change of variable $z = \frac{\mu_{\hat{S}}}{\mu_{\hat{B}}}(1+x)$ with $x << 1$ (small SNR region). With this modification, we obtain:

$$\frac{\mu_{\hat{B}}\sigma_{\hat{S}}^2 + \mu_{\hat{S}}\sigma_{\hat{B}}^2 z}{\sigma_{\hat{B}}\sigma_{\hat{S}}(\sigma_{\hat{B}}^2 z^2 + \sigma_{\hat{S}}^2)^{1/2}} \approx \sqrt{\frac{\mu_{\hat{B}}^2}{\sigma_{\hat{B}}^2} + \frac{\mu_{\hat{S}}^2}{\sigma_{\hat{S}}^2}} + O(x)$$

where $O(x)$ is the conventional big O notation.
As stated just above $\frac{\mu_{\hat{B}}^2}{\sigma_{\hat{B}}^2}$ is very large in practice. Moreover the $\mathcal{Q}(x)$ function vanishes for large x. As a result $A \approx 1$. This term can thus be also removed from Eq. 2. Eventually, the remaining equation is:

$$p_{\hat{Z}}(z) = \frac{\mu_{\hat{B}}\sigma_{\hat{S}}^2 + \mu_{\hat{S}}\sigma_{\hat{B}}^2 z}{\sqrt{2\pi}(\sigma_{\hat{B}}^2 z^2 + \sigma_{\hat{S}}^2)^{3/2}} \exp\left(-\frac{(\mu_{\hat{S}} - \mu_{\hat{B}} z)^2}{2(\sigma_{\hat{B}}^2 z^2 + \sigma_{\hat{S}}^2)}\right)$$

For low SNR values, a small signal approximation of $p_{\hat{Z}}(z)$ gives:

$$p_{\hat{Z}}(z) \approx \frac{\mu_{\hat{B}}}{\sqrt{2\pi}\sigma_{\hat{S}}} \exp\left(-\frac{\left(\frac{\mu_{\hat{S}}}{\mu_{\hat{B}}} - z\right)^2}{2(\sigma_{\hat{S}}^2/\mu_{\hat{B}}^2)}\right)$$

Hence, $\hat{Z}$ approximately follows a Gaussian distribution with mean $\mu_{\hat{Z}}$ and $\sigma_{\hat{Z}}^2$ defined by:

$$\begin{aligned} \mu_{\hat{Z}} &= \frac{\mu_{\hat{S}}}{\mu_{\hat{B}}} \\ \sigma_{\hat{Z}}^2 &= \frac{\sigma_{\hat{S}}^2}{\mu_{\hat{B}}^2} \end{aligned} \tag{11}$$

Under hypothesis $\mathcal{H}_1$, this gives:

$$\begin{aligned} \mu_{\hat{Z}} &= \theta + \frac{K}{N} \\ \sigma_{\hat{Z}}^2 &= \frac{4\theta}{N} + \frac{2K}{N^2} \end{aligned} \tag{12}$$

Under hypothesis $\mathcal{H}_0$, one has to set $\theta = 0$ in Eq. 12.

3.3.2 Hypothesis $\mathcal{H}_0$

Under the hypothesis $\mathcal{H}_0$, the SNR is proportional to the F-score [CK14]: $\hat{Z} = \frac{N}{K}F$ where F follows an F-distribution with $K-1$ and $N-K$ degrees of freedom. We will now derive a Gaussian approximation. From Eq. 10 we observe that $\sigma_{\hat{B}}^2$ is very small for large N. $\hat{B}$

is thus almost deterministic and $\hat{Z}$ is a scaled value of $\hat{S}$. This assumption is also valid for hypothesis $\mathcal{H}_0$ since the distribution of $\hat{B}$ is unchanged: $\hat{Z} \approx \hat{S}/\mu_{\hat{B}}$. Consequently, the p.d.f. of $\hat{Z}$ is approximated by:

$$p_{\hat{Z}}(z) \approx \mu_{\hat{B}} p_{\hat{S}}(\mu_{\hat{B}} z) \tag{13}$$

where $p_{\hat{S}}(z)$ is defined by Eq. 6.
When the number of classes K is large (e.g. $K = 256$), this p.d.f. is well approximated by a Gaussian distribution whose mean and variance are given by Eq. 11, 5 and 10, with $f_k = \mu_f$.

4 Models validation

4.1 Validation with simulations

Simulations are performed to verify the Gaussian approximation of $\hat{S}$, $\hat{B}$ and $\hat{Z}$. Two leakage models are evaluated:

- Stochastic linear leakage model [SLP05]: $f_k = \sum_{i=0}^{7} \varepsilon_i X_i$ where X_i is a random bit ('0' or '1' with probability 1/2) and $\varepsilon_i \sim \mathcal{N}(1, \sigma_a^2)$. The vector $(X_0, \cdots, X_7)$ is the binary decomposition of the class index k. In practice, the coefficients ε_i's are normalized so that $var(f_k) = 1$. Simulations are performed with $\sigma_a^2 = 0.2$.
- HW model: $f_k = HW(X)$ for X uniformly distributed in the interval $[0, 2^H - 1]$. There are $K = H + 1$ classes where H is the number of bits used for the binary decomposition of the sensitive variable X. The value of K is significantly smaller compared to the previous cases, the Central Limit Theorem (CLT) may thus lead to a inaccurate model. $N_k = 4\,10^6\, P(k)$ traces are generated for each class, where $P(k) = 2^{-H} C_H^k$ and C_H^k is the binomial coefficient.

Unless mentioned, all simulations are conducted with $\sigma^2 = 10$.

4.1.1 Stochastic linear leakage model

The probability density function for $\hat{S}$ and $\hat{B}$ is assessed using sample sets generated with the byte value linear model. This is then compared to the Gaussian approximation described in Eq. 5 and Eq. 10. The outcomes are illustrated in Figure 1, demonstrating a very good matching that validates the derived models.

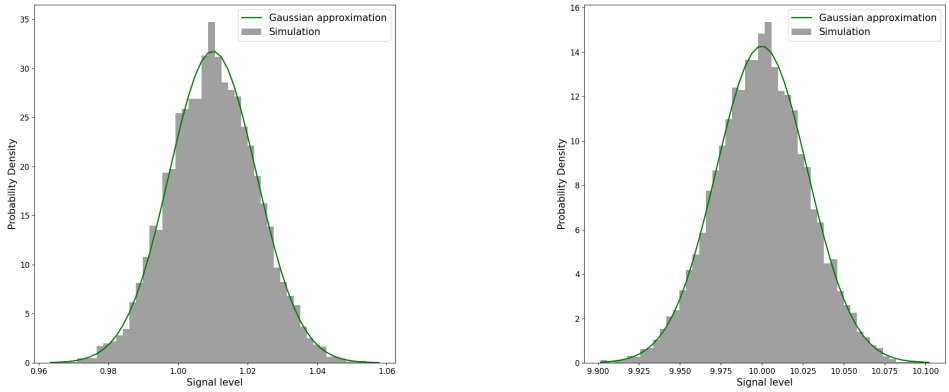

Figure 1: p.d.f. of $\hat{S}$ (left) and $\hat{B}$ (right).

The p.d.f. of $\hat{Z}$ is assessed using samples obtained from the byte value linear model. This evaluation is then compared to the probability density function provided by Equation 2 (referred to as "Model"), as well as its Gaussian approximation with mean and variance described by Equation 11 (referred to as "pdf-Gaussian approximation"). Results are presented in Figure 2 for a balanced classes configuration ($N_k = 1000\,\forall k$) and $\mu_{\hat{S}}/\mu_{\hat{B}} = 0.1$. We observe a good matching between the simulations and the two p.d.f. models. This confirms the validity of the Gaussian approximation for low SNR. Figure 2 also illustrates the p.d.f. of Z and the distribution proportional to the F-score under hypothesis $\mathcal{H}_0$ ($f_k = \mu_f$) for the byte value model. The Gaussian approximation closely approximates both the F-score distribution and the simulation results.

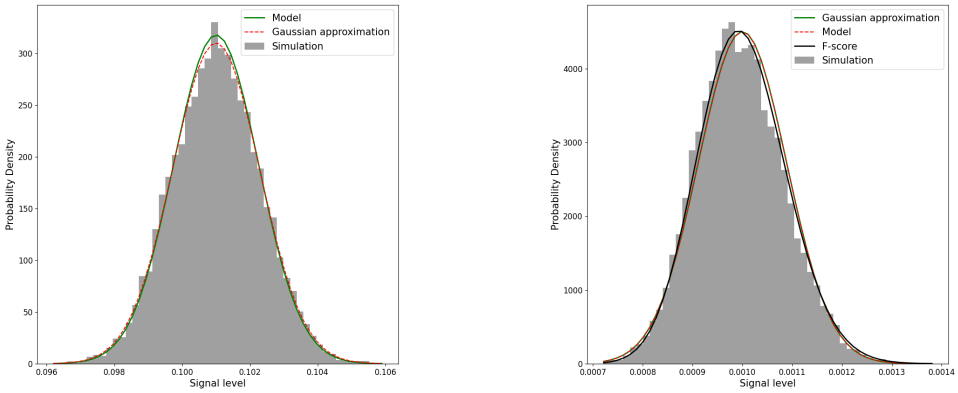

Figure 2: p.d.f. of $\hat{Z}$ with $\mu_{\hat{S}}/\mu_{\hat{B}} = 0.1$ (left) and hypothesis $\mathcal{H}_0$ (right).

4.1.2 HW leakage model

Figure 3 displays the p.d.f. of $\hat{Z}$ for $H = 8$ and 32 when the HW leakage is present. The model accurately represents the true p.d.f. even for a small number of classes ($K = 9$). The Gaussian approximation slightly overestimates the p.d.f., but remains close to the simulation results. As such, it is also suitable for a HW-based classification. Figure 4 shows the p.d.f. of $\hat{Z}$ for $H = 8$ in the absence of any leakage ($f_k = \mu_f$). The p.d.f. of the model given by Eq. 6 matches very well with simulation results.

4.2 Validation with experimental results

In this section, we experimentally validate the p.d.f. models derived under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$. The experiments use the ASCADv2 database [BPS+20]. More precisely, we use the "ascadv2-extracted" database available for download. The SNR measured with the byte value model for the first output of the masked sbox is presented in Figure 5. 500000 traces are used for the computation of the SNR. A distinguishable peak is observed at time index 5222. We assigned this time sample to hypothesis $\mathcal{H}_1$ and the time samples belonging to the interval $[0, 4000]$ to hypothesis $\mathcal{H}_0$.
Figure 6 displays the p.d.f. of $\hat{Z}$ for the byte value and HW models computed at time index 1955. The Gaussian approximation outlined in Eq. 11 is precise for the byte value model, whereas the p.d.f. provided by Eq. 6 closely matches the simulation results for the HW model.
The p.d.f. of $\hat{Z}$ for the byte value is evaluated at the time index 5222. Since the true value of θ is unknown, we assume that the model of Eq. 11 is valid and estimate it by

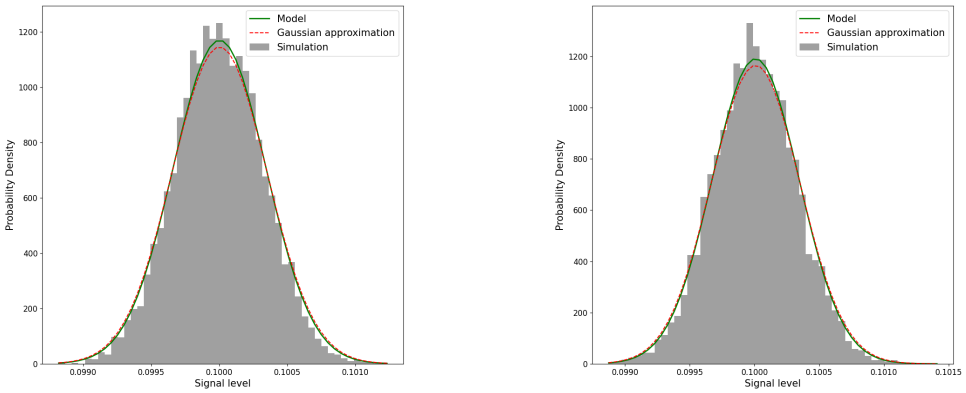

Figure 3: p.d.f. of $\hat{Z}$ for HW model under hypothesis $\mathcal{H}_1 : H = 8$ (left) and $H = 32$ (right).

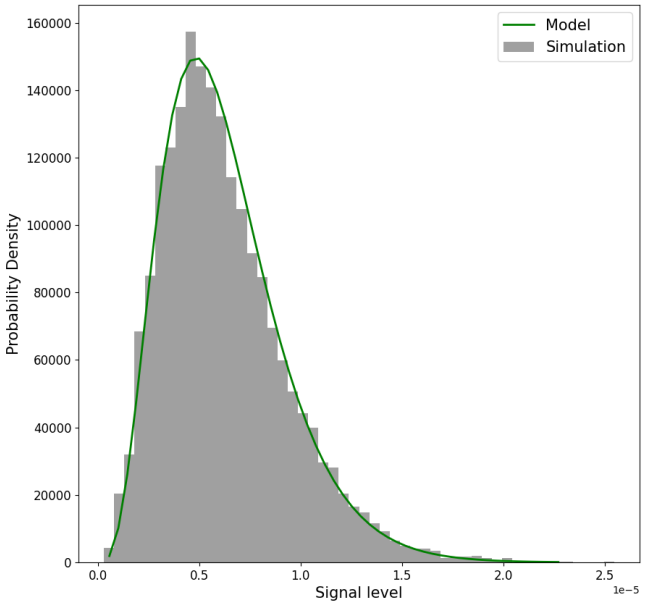

Figure 4: p.d.f. of $\hat{Z}$ under hypothesis $\mathcal{H}_0$.

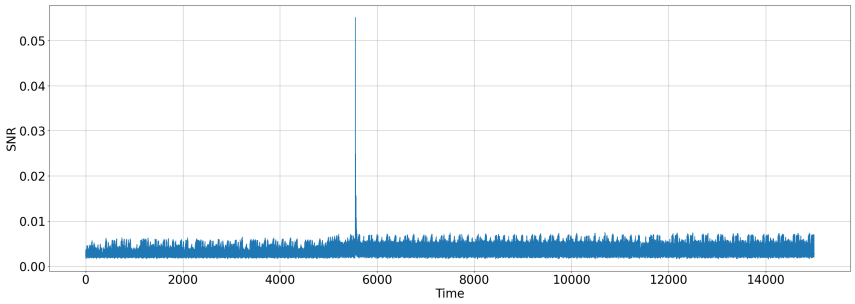

Figure 5: SNR measured with the byte value model.

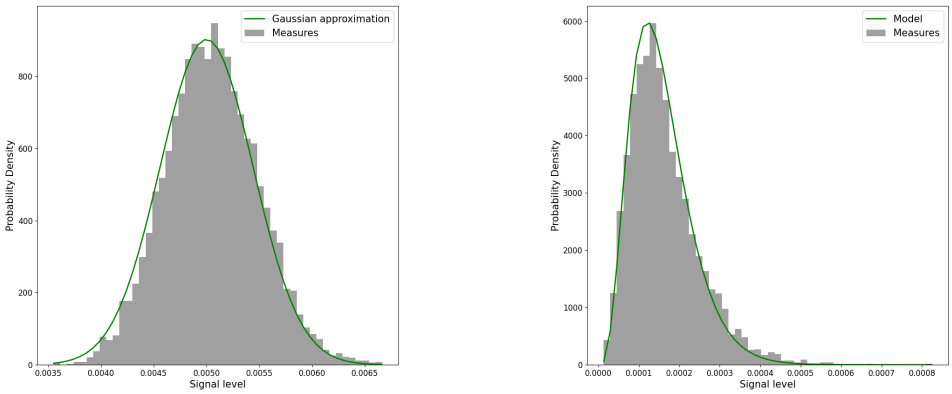

Figure 6: p.d.f. of $\hat{Z}$ - byte value model (left) and HW ($H = 8$) (right) - Hypothesis $\mathcal{H}_0$.

$\hat{\theta} = E[Z] - K/N$. This value is then inserted in Eq. 12 to compute $\mu_{\hat{Z}}$ and $\sigma^2_{\hat{Z}}$. Figure 7 displays the p.d.f. of $\hat{Z}$ for the byte value. The Gaussian approximation outlined in Eq. 11 is precise for the byte value model.

5 Detection threshold and sampling complexity

The detector computes a decision variable D (e.g. $\hat{Z}$ for SNR and correlation for the ρ-test) and must decide between two hypotheses: $\mathcal{H}_0$ or $\mathcal{H}_1$. When p.d.f. $p(D|\mathcal{H}_0)$ and $p(D|\mathcal{H}_1)$ are known, the Likelihood Ratio Test (LRT) [Poo94] is a conventional decision-making rule. It based on the ratio $\dfrac{p(D|\mathcal{H}_0)}{p(D|\mathcal{H}_1)}$. However, in our situation, this is not applicable because the LRT depends on the unknown variable we want to detect (e.g. θ for $D = \hat{Z}$). An alternative solution is to design a detector that rejects the hypothesis $\mathcal{H}_0$. This is the strategy already applied by T-test and χ^2-test. A threshold γ is pre-determined and the detector decides for hypothesis $\mathcal{H}_0$ when $D < \gamma$ and $\mathcal{H}_1$ otherwise. The performance are defined by the false positive (α) and false negative (β) rates [Poo94]:

$$\begin{aligned} \alpha &= \text{Prob}(D > \gamma|\mathcal{H}_0) \\ \beta &= \text{Prob}(D \leq \gamma|\mathcal{H}_1) \end{aligned} \tag{14}$$

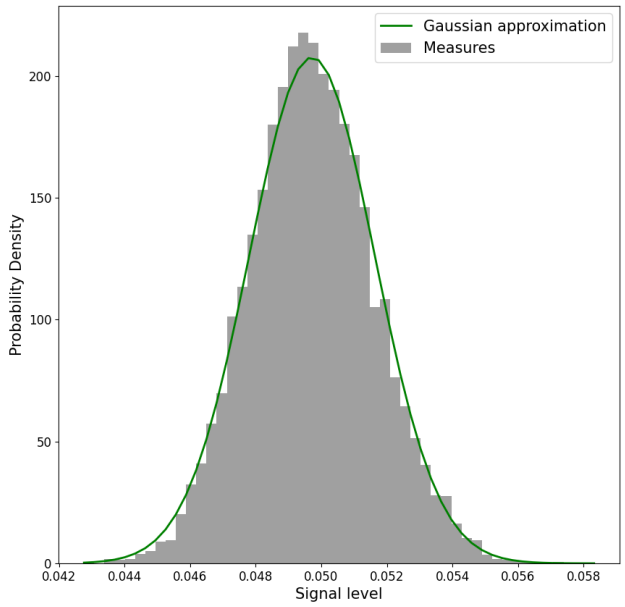

Figure 7: SNR measured with the byte value model - Hypothesis $\mathcal{H}_1$.

γ is set to ensure the false positive rate remains below α. Its depends on α, but also on the other parameters such as N and K for the SNR. This equation is then inserted in the definition of β. This provides a new equation that links N to α, β, θ and K. The p.d.f. evaluated in the previous sections are used to compute α and β. The theoretical sampling complexity N is eventually derived.

5.1 SNR

5.1.1 Byte value model

In the followings, we will denote $\hat{Z}_0$ (resp. $\hat{Z}_1$) the value of $\hat{Z}$ under hypothesis $\mathcal{H}_0$ (resp. $\mathcal{H}_1$). According to Section 3, $\hat{Z}_0$ and $\hat{Z}_1$ have Gaussian p.d.f. for small SNR. Using the Gaussian approximation for $\hat{Z}_0$:

$$\alpha = \mathcal{Q}\left(\frac{\gamma - \mu_{\hat{Z}_0}}{\sigma_{\hat{Z}_0}}\right) \tag{15}$$

where $\mathcal{Q}(x)$ is defined by Eq. 3.
Similarly,

$$\beta = 1 - \mathcal{Q}\left(\frac{\gamma - \mu_{\hat{Z}_1}}{\sigma_{\hat{Z}_1}}\right) \tag{16}$$

From Eq. 11 and 5, we have: $\mu_{\hat{Z}_1} = \theta + K/N$ and $\sigma^2_{\hat{Z}_1} = \frac{2K}{N^2} + 4\frac{\theta}{N}$. γ is set to maintain a false alarm rate smaller than α. Using Eq. 15 with $\mu_{\hat{Z}_0}$ and $\sigma_{\hat{Z}_0}$ given by Eq. 11 we obtain:

$$\gamma = \frac{K}{N} + \frac{\sqrt{2K}}{N}\mathcal{Q}^{-1}(\alpha) \tag{17}$$

Note that γ is independent from the noise variance. We will now derive the relationship between the number of trace N, α, β and the SNR value θ when all classes have the same size ($N_k = N/K$).
Inserting Eq. 17 in the definition of β in Eq. 16 gives:

$$\left(\sigma_{Z_0}\mathcal{Q}^{-1}(\alpha) - \theta\right)^2 = \sigma_{Z_1}^2\left(\mathcal{Q}^{-1}(1-\beta)\right)^2$$

Let us define the following notations: $a = \mathcal{Q}^{-1}(\alpha)$ and $b = \mathcal{Q}^{-1}(1-\beta)$. After insertion of the expression of σ_{Z_1} and σ_{Z_0}, we obtain a polynomial on the variable $x = N\theta$:

$$x^2 - \left(4b^2 + 2a\sqrt{2K}\right)x + 2K(a^2 - b^2) = 0$$

The root is eventually:

$$x_0 = N\theta = 2b^2 + a\sqrt{2K} + |b|\sqrt{2K + 4b^2 + 4a\sqrt{2K}} \tag{18}$$

The product $N\theta$ is thus constant when a, b and K are fixed.

5.1.2 HW model

For an HW leakage model, the p.d.f. of $\hat{Z}_0$ is not Gaussian anymore.
α is defined by:

$$\alpha(\gamma) = \int_{\gamma}^{\infty} \mu_{\hat{B}} p_S(\mu_{\hat{B}} x)dx \tag{19}$$

where $p_S(x)$ is given by Eq. 6.
Assuming that the assumption $\mu_{\hat{B}} \approx \sigma^2$ holds, we obtain:

$$\alpha(\gamma) = C\sum_{k=0}^{\infty} \frac{\delta_k}{\Gamma(H/2+k)} g(H/2+k, \sigma^2\gamma/\lambda) \tag{20}$$

where $g(s,x) = \int_x^{\infty} t^{s-1}e^{-t}dt$ is the upper incomplete gamma function.
From Eq. 7, we observe that λ is proportional to σ^2. Hence $\sigma^2/\lambda = N/\left(2\min_k\left(1 - P(k)\right)\right)$ does not depend on the the noise variance. Consequently, for a predefined α, the corresponding detection threshold γ is independent from σ^2 and can be pre-determined. Moreover, the variable $\sigma^2\gamma/\lambda = \gamma N/\left(2\min_k\left(1 - P(k)\right)\right)$ is constant for a fixed α. Consequently, the product $\gamma N = c_H$ is constant for a pre-determined α and a fixed value of H. Table 1 gives the values of c_H evaluated by simulations for different values of α and $H = 8$. The value $\gamma = c_H/N$ is eventually inserted in Eq. 16 which results in a polynomial on the variable $x = N\theta$:

$$x^2 - \left(4b^2 + c_H - K\right)x - 2Kb^2 + (c_H - K)^2 = 0$$

with $K = H + 1$.
The root is eventually:

$$x_0 = N\theta = 2b^2 + c_H - K + |b|\sqrt{2K + 4b^2 + 4(c_H - K)} \tag{21}$$

Table 1: Value of c_H for different false positive rates ($H = 8$).

	$\alpha = 10^{-3}$	$\alpha = 10^{-4}$	$\alpha = 10^{-5}$	$\alpha = 10^{-6}$
c_H	17.34	21.06	24.5	28.08

5.2 ρ test

Similar to the previous section, we compute the sampling complexity of the ρ-test taking into account the false negative and positive rates. To do so, we reuse some results and properties already presented in [Man04]. Let ρ be Peason's correlation coefficient computed with the acquisition samples and μ_ρ be its mean. The Fisher's Z transformation of ρ follows a Gaussian distribution:

$$\begin{aligned} Q &= \frac{1}{2}\log\left(\frac{1+\rho}{1-\rho}\right) \sim \mathcal{N}(\mu_Q, \sigma_Q^2) \\ \mu_Q &= \frac{1}{2}\log\left(\frac{1+\mu_\rho}{1-\mu_\rho}\right) \\ \sigma_Q^2 &= \frac{1}{N-3} \end{aligned}$$

If the leakage model is valid, μ_ρ is related to the SNR θ: $\mu_\rho = \sqrt{\frac{\theta}{1+\theta}}$. For low SNR and correlation values, this leads to the following approximation: $\mu_Q \approx \mu_\rho \approx \sqrt{\theta}$
From the Gaussian approximation of Q and for low correlation values, we have:

$$\begin{aligned} \alpha &= \text{Prob}(|\rho| > \gamma | \mathcal{H}_0) \approx 2\mathcal{Q}\left(\frac{\gamma}{\sigma_Q}\right) \\ \beta &= \text{Prob}(|\rho| \leq \gamma | \mathcal{H}_1) \approx 2\left(1 - \mathcal{Q}\left(\frac{\gamma - \mu_\rho}{\sigma_Q}\right)\right) \end{aligned} \tag{22}$$

Let us define the following notations: $a_1 = \mathcal{Q}^{-1}(\alpha/2)$ and $b_1 = \mathcal{Q}^{-1}(1-\beta/2)$. From the definition of α and β, we have $\gamma = a_1/\sqrt{N-3}$ and $\frac{\mu_\rho}{\sigma_Q} = a_1 - b_1$. Finally, an approximation of N is found:

$$x_0 = N\theta \approx (a_1 - b_1)^2 \tag{23}$$

5.3 T-test

When the number of traces is large, the T-test follows approximately a Gaussian distribution $\mathcal{N}(0,1)$ [DS16]. Consequently, the detection threshold is set as follows:

$$\gamma = \mathcal{Q}^{-1}(\alpha/2)$$

When $\alpha = 10^{-6}$, one finds the threshold value $\gamma = 4.9$ which is often found in the literature [CdMG+13].
The sampling complexity of the T-test has been derived and studied in [WO19]. Using an approximation of the T-test variable as a Gaussian distribution, N is derived when the number of traces is equally partitioned between the two classes:

$$x_0 = N\theta \approx \frac{(a_1 + b_2)^2}{2} \tag{24}$$

where $b_2 = \mathcal{Q}^{-1}(\beta)$.

5.4 Sampling complexity

The impact of the trace length L on the leakage detection is analyzed in [DZD+18] and [WO19]. In a multivariate setting, the overall false positive rate α_T is related to the univariate counterpart α by $\alpha_T = 1 - (1-\alpha)^L$ if the L detection tests are independent. The value assigned to α is thus set in order to limit the false positives over the entire trace:

$\alpha = 1 - (1 - \alpha_T)^{1/L}$. The value of β is set similarly. There is however a difference due to the small number of leakage points in the trace which reduces the practical value of L.

The sampling complexity of T-test and ρ-test are compared in [DS16] for the HW model under hypothesis $\mathcal{H}_1$. For a fixed SNR, the average value of the decision metric is computed as a function of the number of traces. The authors concludes that the T-test needs less traces than ρ-test to detect leakage. However, it does not provide information regarding the exploitable leakage samples. In this section, we extend this work by adding the SNR method into the comparison and also consider a stochastic leakage model in addition to the HW model. The comparison is also implemented differently. The detection threshold γ is set for a false positive rate $\alpha = 10^{-6}$. Then, we evaluate the number of traces required to provide a false negative rate below a pre-determined value $\beta = 10^{-3}$.

The sampling complexity of the T-test, χ^2-test, ρ-test and SNR is now evaluated. For the T-test and χ^2-test, the evaluation is made with the fixed-versus-random option. The fixed class is built with byte $X = 0$ and the number of traces is equally partitioned between the two classes. The χ^2-test is implemented in the same way as it is described in the original paper [MRSS18]. Since the number of column of the contingency matrix may vary from one draw to another, the detection threshold is not constant. Consequently, the p-value is computed and a false negative is declared if the p-value is larger than 10^{-6}. The estimation of the stochastic leakage model described in Section 4.1 is also considered for the ρ-test. Instead of estimating each coefficient ε_i, the leakage f_k is directly targeted. In order to optimize the number of traces used to estimate the f_k's and compute the ρ-test value, a cross-validation technique is applied. The number of traces N is split in N_c sets. The first $(N_c - 1)N/N_c$ traces are used to estimate parameters f_k. Traces are classified according to the target value (0 to 255) and f_k is estimated by averaging the traces belonging to the same class. The N_c traces of the last remaining set are used to compute their contribution to the ρ-test value. This operation is then repeated by shifting from one set at a time. In the end, all the traces are used for the estimation and the computation of the ρ-test but with disjoint sets.

The number of traces N evaluated by simulations is compared to the theoretical value predicted by Eq. 18, 21 , 23 or 24. Figure 8 shows the value of N as a function of the true SNR for the T-test, ρ-test, χ^2-test and SNR method for the stochastic linear leakage model. The T-test is the most efficient technique, followed by the ρ-test when the leakage model is perfectly estimated, the χ^2-test and the SNR method. The theoretical models are very close to the simulation results and even overlap for the T-test. This validates them. The sampling complexity of the SNR is higher because it requires a minimum amount of traces for each of the 256 classes whereas the T-test considers only two classes. When the leakage model is estimated for the ρ-test , the number of traces increases significantly and deviates from the value predicted by the theoretical model for a perfect estimation. In addition, N decreases when the number of cross-validation sets N_c increases. It converges to the same level as the SNR. The χ^2-test is not the most appropriate solution because it is not informative about the exploitability of the leakage and is less efficient than the T-test for a binary leakage detection test.

Figure 9 shows the value of N as a function of the SNR for the T-test, ρ-test and SNR method for the HW leakage model. Once again, the T-test is the most efficient technique, followed by the ρ-test and the SNR method. The theoretical model for the SNR is accurate for the HW32 leakage model. However it is not tight for the HW8 model and a very small SNR. This is probably due to the Gaussian approximation of $\hat{S}$ in Section 3.1.1 which is not fully valid for HW8. The number of classes is not large enough to apply the CLT. The error between the model and the simulations may increase with σ^2, explaining the gap observed at an SNR below -12 dB.

The validity of the theoretical models is then evaluated on real traces from the ASCADv2 data base. We reuse the same set of traces and methodology as in Section 4.2 for the

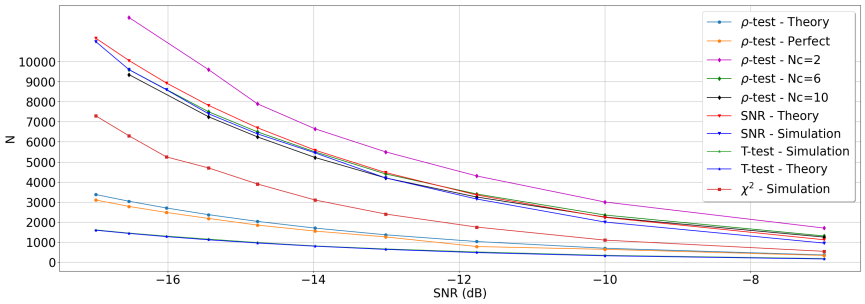

Figure 8: Sampling complexity - Stochastic model - $\alpha = 10^{-6}$ and $\beta = 10^{-3}$.

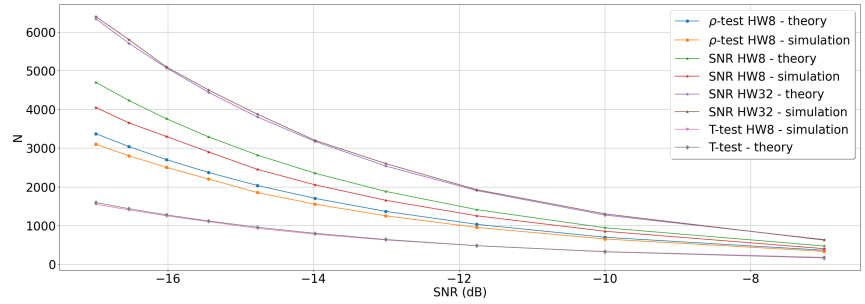

Figure 9: Sampling complexity - HW model - $\alpha = 10^{-6}$ and $\beta = 10^{-3}$.

validation of the $\mathcal{H}_1$ hypothesis. The results obtained for the SNR, T-test and ρ-test are given in Table 2. It presents the theoretical value of N for the T-test, SNR (byte value and HW8 models) and ρ-test (byte value and HW8 models), the experimental measure and the error ratio. The value provided for the ρ-test with the byte value model ($N_c = 6$ or 10) as "theory" is a simulation results obtained for $\theta = 0.044$. This value is the experimental SNR measured on the ASCADv2 dataset. This corresponds to a noise variance $\sigma^2 = 45.5$. The theoretical sampling complexity is close to the experimental results for the SNR with the byte value model, the T-test and the ρ-test. The error is larger for the SNR with the HW8 model. This may come from the relative inadequacy of the theoretical model for the HW8 leakage, as explained in the paragraph just above.

Table 2: Sampling complexity - ASCADv2 - $\alpha = 10^{-6}$ and $\beta = 10^{-3}$. (*): simulation results with $\sigma^2 = 45.5$.

	SNR (byte value)	SNR (HW8)	T-test	ρ-test ($N_c = 6$)	ρ-test ($N_c = 10$)	ρ-test (HW8)
Theory	4998	2102	712	5175 (*)	4750 (*)	1523
Experiment	4700	1800	660	5220	4700	1400
Error ratio	6%	14.4%	7.3%	0.8%	1%	8%

6 Recommendations for an evaluator

The results presented in Section 5.4 allow to draw some recommendations for the best usage of each method:

- If the evaluator is only interested by a YES/NO answer concerning the presence or absence of leakage, he/she should use the T-test method.
- If the evaluator is interested in the exploitability of the leakage, he/she should use the ρ-test method to test an HW leakage model and the SNR for the byte value model.
- The SNR method is not appropriate to test an HW leakage model.

In addition, for fixed values of α and β, two strategies are offered to the evaluator:

- The number of traces is limited to N_{max}: the minimum detectable SNR value is thus $\theta_0 = x_0/N_{max}$, where x_0 is given by either Eq. 18, 21, 23 or 24 depending on the selected detection method.
- The evaluator is only interested in detecting leakages whose SNR is greater than θ_0. The minimum number of traces that must be acquired is thus $N_{min} = x_0/\theta_0$.

If none of the previous procedure succeeds and the evaluator knows a sensitive variable is processed during the trace acquisition, the remaining solution is to implement a leakage detection test based on MI [MOBW13][CLM20].

7 Conclusion

The SNR is a widely used metric for assessing an information leakage from a device. We derived the theoretical formulation of its p.d.f. in case leakage is present or not, under a small SNR assumption. Our study covers the byte value and the HW leakage models. These p.d.f. formulations were validated through simulations and experiments on a set of traces taken from the ASCADv2 dataset. They are used to set a detection threshold that rejects false positives from the SNR measurements. These p.d.f. formulations are also used to derive the theoretical number of traces that are required to remain below pre-determined false negative and false positive rates. The sampling complexity of the T-test, ρ-test and SNR has eventually been defined and compared for the byte value and HW leakage model. The T-test is the most efficient technique for the two leakage models. The ρ-test is more efficient than the SNR method under the HW leakage model but the two techniques perform equally under the byte value model. In fact, the leakage model must be estimated from the traces in order to implement the ρ-test with the byte value model. Unfortunately, the T-test does not provide any information about the detected leakage exploitability. Consequently, the SNR method is the most appropriate method when the evaluator is interested in the exploitability of the leakage and has no prior information about the leakage model. In that case, the SNR shall be computed with the byte value model. When the evaluator wants to test the validity of the HW leakage model, the ρ-test is the most appropriate solution.

Acknowledgment

The author is very grateful to the anonymous reviewers and the shepherd for their extensive contribution in improving the paper.

References

[AL06] K.B. Athreya and S.N. Lahiri. *Measure theory and probability theory*. Springer, Heidelberg, 2006.

[BDGN14] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm. Side-channel leakage and trace compression using normalized inter-class variance. Cryptology ePrint Archive, Report 2014/1020, 2014. https://eprint.iacr.org/2014/1020.

[BPS+20] Ryad Benadjila, Emmanuel Prouff, Rémi Strullu, Eleonora Cagli, and Cécile Dumas. Deep learning for side-channel analysis and introduction to ASCAD database. *Journal of Cryptographic Engineering*, 10(2):163–188, June 2020.

[CdMG+13] J. Cooper, E. de Mulder, G. Goodwill, J. Jaffe, and G. Kenworthy. Test vector leakage assessment (TVLA) methodology in practice (extended abstract). In *ICMC*, 2013.

[CDP17] Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff. Convolutional neural networks with data augmentation against jitter-based countermeasures – profiling attacks without pre-processing –. Cryptology ePrint Archive, Report 2017/740, 2017. https://eprint.iacr.org/2017/740.

[CK14] Omar Choudary and Markus G. Kuhn. Template attacks on different devices. Cryptology ePrint Archive, Report 2014/459, 2014. https://eprint.iacr.org/2014/459.

[CLM20] Valence Cristiani, Maxime Lecomte, and Philippe Maurine. Leakage assessment through neural estimation of the mutual information. In *Applied Cryptography and Network Security Workshops: ACNS 2020 Satellite Workshops, AIBlock, AIHWS, AIoTS, Cloud S&P, SCI, SecMT, and SiMLA, Rome, Italy, October 19–22, 2020, Proceedings 18*, pages 144–162. Springer, 2020.

[CRR03] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. Template attacks. In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *CHES 2002*, volume 2523 of *LNCS*, pages 13–28. Springer, Heidelberg, August 2003.

[dCGRP19] Eloi de Cherisey, Sylvain Guilley, Olivier Rioul, and Pablo Piantanida. Best information is most successful. Cryptology ePrint Archive, Report 2019/491, 2019. https://eprint.iacr.org/2019/491.

[DS16] François Durvaux and François-Xavier Standaert. From improved leakage detection to the detection of points of interests in leakage traces. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 240–262. Springer, Heidelberg, May 2016.

[DZD+18] A Adam Ding, Liwei Zhang, François Durvaux, François-Xavier Standaert, and Yunsi Fei. Towards sound and optimal leakage detection procedure. In *Smart Card Research and Advanced Applications: 16th International Conference, CARDIS 2017, Lugano, Switzerland, November 13–15, 2017*, pages 105–122. Springer, 2018.

[Man04] Stefan Mangard. Hardware countermeasures against DPA – A statistical analysis of their effectiveness. In Tatsuaki Okamoto, editor, *CT-RSA 2004*, volume 2964 of *LNCS*, pages 222–235. Springer, Heidelberg, February 2004.

[MOBW13] Luke Mather, Elisabeth Oswald, Joe Bandenburg, and Marcin Wojcik. Does my device leak information? An a priori statistical power analysis of leakage detection tests. Cryptology ePrint Archive, Report 2013/298, 2013. https://eprint.iacr.org/2013/298.

[MOP08] S. Mangard, E. Oswald, and T. Popp. *Power analysis attacks: Revealing the secrets of smart cards*. Springer, Heidelberg, 2008.

[Mos85] P.G. Moschopoulos. The distribution of the sum of independent gamma random variables. *Annals of the Institute of Statistical Mathematics*, 37(1), 1985.

[MOS09] Stefan Mangard, Elisabeth Oswald, and Francois-Xavier Standaert. One for all - all for one: Unifying standard DPA attacks. Cryptology ePrint Archive, Report 2009/449, 2009. https://eprint.iacr.org/2009/449.

[MRSS18] Amir Moradi, Bastian Richter, Tobias Schneider, and François-Xavier Standaert. Leakage detection with the χ^2-test. *IACR TCHES*, 2018(1):209–237, 2018. https://tches.iacr.org/index.php/TCHES/article/view/838.

[Poo94] H.V. Poor. *An introduction to signal detection and estimation*. Springer, Heidelberg, 1994.

[Sim02] M.K. Simon. *Probability distributions involving Gaussian random variables: A handbook for engineers and scientists*. Springer, Heidelberg, 2002.

[SLP05] Werner Schindler, Kerstin Lemke, and Christof Paar. A stochastic model for differential side channel cryptanalysis. In Josyula R. Rao and Berk Sunar, editors, *CHES 2005*, volume 3659 of *LNCS*, pages 30–46. Springer, Heidelberg, August / September 2005.

[SMY06] Francois-Xavier Standaert, Tal G. Malkin, and Moti Yung. A unified framework for the analysis of side-channel key recovery attacks (extended version). Cryptology ePrint Archive, Report 2006/139, 2006. https://eprint.iacr.org/2006/139.

[VS09] Nicolas Veyrat-Charvillon and François-Xavier Standaert. Mutual information analysis: How, when and why? In Christophe Clavier and Kris Gaj, editors, *CHES 2009*, volume 5747 of *LNCS*, pages 429–443. Springer, Heidelberg, September 2009.

[WO19] Carolyn Whitnall and Elisabeth Oswald. A cautionary note regarding the usage of leakage detection tests in security evaluation. Cryptology ePrint Archive, Report 2019/703, 2019. https://eprint.iacr.org/2019/703.