A Key to Success
Success Exponents for Side-Channel Distinguishers

Sylvain Guilley[1,2], Annelie Heuser[1(✉)], and Olivier Rioul[1,3]

[1] Department Comelec, Télécom ParisTech, Institut Mines-Télécom, CNRS LTCI, 46 Rue Barrault, 75 634 Paris Cedex 13, France
{sylvain.guilley,annelie.heuser,olivier.rioul}@telecom-paristech.fr
[2] Secure-IC S.A.S., 15 Rue Claude Chappe, Bât. B, ZAC des Champs Blancs, 35 510 Cesson-Sévigné, France
[3] Applied Mathematics Department, École Polytechnique, Palaiseau, France

Abstract. The success rate is the classical metric for evaluating the performance of side-channel attacks. It is generally computed empirically from measurements for a particular device or using simulations. Closed-form expressions of success rate are desirable because they provide an explicit functional dependence on relevant parameters such as number of measurements and signal-to-noise ratio which help to understand the effectiveness of a given attack and how one can mitigate its threat by countermeasures. However, such closed-form expressions involve high-dimensional complex statistical functions that are hard to estimate.

In this paper, we define the success exponent (SE) of an arbitrary side-channel distinguisher as the first-order exponent of the success rate as the number of measurements increases. Under fairly general assumptions such as soundness, we give a general simple formula for any arbitrary distinguisher and derive closed-form expressions of it for DoM, CPA, MIA and the optimal distinguisher when the model is known (template attack). For DoM and CPA our results are in line with the literature. Experiments confirm that the theoretical closed-form expression of the SE coincides with the empirically computed one, even for reasonably small numbers of measurements. Finally, we highlight that our study raises many new perspectives for comparing and evaluating side-channel attacks, countermeasures and implementations.

Keywords: Side-Channel distinguisher · Evaluation metric · Success rate · Success exponent · Closed-form expressions

1 Introduction

Side-channel attacks analyse physical leakage that is unintentionally emitted during cryptographic operations in a device. This side-channel leakage is statistically dependent on intermediate processed values involving the secret key.

Annelie Heuser is a Google European fellow in the field of privacy and is partially founded by this fellowship.

A. Biryukov and V. Goyal (Eds.): INDOCRYPT 2015, LNCS 9462, pp. 270–290, 2015.
DOI: 10.1007/978-3-319-26617-6_15

It is then possible to retrieve the secret from the measured data by maximizing some statistical distinguisher. In the past decade, many distinguishers have been proposed: difference of means test [17] (DoM), Pearson correlation [4] (CPA), mutual information [12] (MIA), etc. Such distinguishers have different characteristics and performances, depending on the implementation, measurement noise, and assumed knowledge on how the device leaks.

To evaluate the performance of a given distinguisher for a limited number of measurements, the *average probability of success* a.k.a. *success rate* (SR) is the ideal and most common evaluation metric [30]. It provides everything one needs to know about the performance of a particular attack scenario. Ideally, one would exhibit an explicit functional relationship of the SR with the number of measurements, signal-to-noise ratio (SNR), and other important quantities determining the relationship between correct and false key hypotheses such as confusion coefficients [10]. The resulting closed-form expression would allow one to better understand how effective the attack can be under specific conditions and how one can mitigate it with appropriate countermeasures.

So far, however, it can be theoretically computed only for a very narrow range of distinguishers (DoM [10], CPA [18,29,31], Bayesian attacks [29]) and only under restrictive "ideal" scenarios (e.g., perfectly known leakage model in Gaussian noise). Moreover, the resulting exact expressions involve high dimensional functions whose dependency on the relevant parameters (such as confusion coefficients) can be very complex. For DoM and CPA under ideal scenarios, the resulting formulas involve a multivariate normal c.d.f. [28] for which no closed-form expression exists, while as was found in the case of CPA [29] the corresponding matrices are not of full rank and require heavy Monte-Carlo computation.

In this paper, we carry out a theoretical derivation of the SR for quite arbitrary distinguishers, at the first order of the exponent. More precisely, our computation yields closed-form expressions of the success exponent (SE) associated to the failure rate (1–SR) at first order as the number of measurements m increases:

$$1 - \mathrm{SR} \approx e^{-m \cdot \mathrm{SE}}. \tag{1}$$

(The precise mathematical meaning of the equivalence $\approx$ will be given in Definition 7.) Even though we obtain the derived expression for the SE under the asymptotic condition that m tends to infinity, simulations show that Eq. (1) is still accurate even for fairly small values of m.

Such an evaluation of the success rate, suitable even for a small number of traces, allows one to compare all possible distinguishers in any scenario (noise distribution, unprotected or protected implementation, etc.). A recent paper by Duc et al. [9, Theorem 2] tackles this problem and achieves a unilateral bound. Here we give both a lower and an upper bound, and as an illustration derive the exact expression of the SE for DoM, CPA, MIA and the optimal distinguisher when model is known (template attack) in terms of the appropriate relevant parameters.

The rest of this paper is organized as follows. Section 2 gives the necessary definitions about distinguishers, success and soundness. In Sect. 3, we examine the convergence of success rate and apply a central limit theorem to derive the SE (Theorem 1). Section 4 validates the SE even for relatively small number of traces, and Sect. 5 provides closed-form expressions of SE for some popular distinguishers. The conclusions and promising perspectives are in Sect. 6.

2 Preliminaries

In the sequel, we consider a standard univariate side-channel scenario as defined in [21]. Let k^* denote the secret cryptographic key, k any possible key hypothesis. Also let X be a random variable[1] representing the measured leakage and T be the (random) input or cipher text used for a given encryption request. The attacker knows some mapping f corresponding to an the internally processed variable $f(k, T)$. A common consideration is $f(T, k) = \texttt{Sbox}[T \oplus k]$ where Sbox is a substitution box. The measured leakage X can then be written as

$$X = \varphi(f(T, k^*)) + N, \tag{2}$$

where φ is a deterministic leakage function and where N is an independent—not necessarily Gaussian—additive noise with zero mean ($\mathbb{E}\{N\} = 0$). The device-specific deterministic function φ is normally unknown to the attacker but she may estimate it as $\hat{\varphi}$ and compute the *sensitive variable* $Y(k) = \hat{\varphi}(f(T, k))$ for each key hypothesis k. For later ease of notation we may drop the letter k and write $Y = Y(k)$ and $Y^* = Y(k^*)$. We do not make any particular assumption on φ or f so that our framework can be applied to any arbitrary scenario.

2.1 Distinguisher

In practice, the distinguisher is a function of m i.i.d. leakage measurements $X_1, X_2, \ldots, X_m$ and sensitive variables $Y_1(k), Y_2(k), \ldots, Y_m(k)$ whose maximization over the key hypothesis yields $\hat{k} = \arg\max_k \widehat{\mathcal{D}}(k)$, where

$$\widehat{\mathcal{D}}(k) = \widehat{\mathcal{D}}(X_1, X_2, \ldots, X_m; Y_1(k), Y_2(k), \ldots, Y_m(k)). \tag{3}$$

Definition 1 (Theoretical Distinguisher). *We assume that there is a "theoretical" value of the distinguisher*

$$\mathcal{D}(k) = \mathcal{D}(X, Y(k)) \tag{4}$$

for each k such that $\widehat{\mathcal{D}}(k)$ converges to $\mathcal{D}(k)$ as $m \to +\infty$ in the mean-squared sense, i.e., the mean-squared error

$$\mathrm{MSE}_m = \mathbb{E}\Big\{\big(\widehat{\mathcal{D}}(k) - \mathcal{D}(k)\big)^2\Big\} \to 0 \text{ as } m \to +\infty. \tag{5}$$

[1] Capitals such as X denote random variables. The corresponding lowercase x denotes realizations of these random variables. We write $\mathbb{P}\{A\}$ for the probability of an event A and $\mathbb{E}\{X\}$ for the expectation of a random variable X.

This implies that $\widehat{\mathcal{D}}(k) \to \mathcal{D}(k)$ in probability. Thus we may consider the practical distinguisher $\widehat{\mathcal{D}}(k)$ as an *estimator* of the theoretical $\mathcal{D}(k)$. The corresponding *bias* and *variance* of $\widehat{\mathcal{D}}(k)$ are

$$B_m(k) = \mathbb{E}\{\widehat{\mathcal{D}}(k)\} - \mathcal{D}(k) \tag{6}$$

$$V_m(k) = \mathrm{Var}(\widehat{\mathcal{D}}(k)). \tag{7}$$

*Example 1 (*CPA [4]*).* For correlation analysis we have

$$\widehat{\mathcal{D}}(k) = \frac{m\sum_{i=1}^m X_iY_i - \sum_{i=1}^m X_i \sum_{i=1}^m Y_i}{\sqrt{m\sum_{i=1}^m X_i^2 - (\sum_{i=1}^m X_i)^2}\sqrt{m\sum_{i=1}^m Y_i^2 - (\sum_{i=1}^m Y_i)^2}} \tag{8}$$

$$\mathcal{D}(k) = \rho(X,Y) = \frac{\mathrm{Cov}(X,Y)}{\sigma_X\sigma_Y} = \frac{\mathbb{E}\{(X-\mu_X)(Y-\mu_Y)\}}{\sigma_X\sigma_Y}. \tag{9}$$

*Example 2 (*MIA [12]*).* For mutual information

$$\mathcal{D}(k) = I(X,Y) = H(X) - H(X|Y) \tag{10}$$

can be estimated e.g. with histograms as

$$\widehat{\mathcal{D}}(k) = \sum_x \sum_y \hat{\mathbb{P}}(x,y) \log_2 \frac{\hat{\mathbb{P}}(x,y)}{\hat{\mathbb{P}}(x)\hat{\mathbb{P}}(y)}. \tag{11}$$

Lemma 1. *Bias $B_m(k)$ and variance $V_m(k)$ tend to zero as m increases.*

Proof. One has the well-known bias-variance compromise: $\mathrm{MSE}_m = \mathbb{E}\{\big(\widehat{\mathcal{D}}(k) - \mathbb{E}\{\widehat{\mathcal{D}}(k)\} + B_m(k)\big)^2\} = V_m(k) + B_m(k)^2 + 0$ where the cross-term vanishes. Since $\mathrm{MSE}_m \to 0$ it follows that $V_m(k) \to 0$ and $B_m(k) \to 0$. □

2.2 Success Rate

The success rate (SR) is the classical evaluation metric when comparing empirical side-channel distinguishers $\widehat{\mathcal{D}}(k)$. It is generally calculated empirically [8,19,21]. The exact (theoretical) value of SR [10,18,29,31] is as follows.

Definition 2 (Success Rate and Failure Rate). *The average success probability is defined by*

$$\mathrm{SR}(\widehat{\mathcal{D}}) = \mathbb{P}\{\forall k \neq k^*,\ \widehat{\mathcal{D}}(k^*) > \widehat{\mathcal{D}}(k)\}. \tag{12}$$

where k^* is the actual value of the secret key. It is sometimes convenient to consider the average failure rate *as the complementary probability*

$$\mathrm{FR}(\widehat{\mathcal{D}}) = 1 - \mathrm{SR}(\widehat{\mathcal{D}}) = \mathbb{P}\{\exists k \neq k^*,\ \widehat{\mathcal{D}}(k) \geq \widehat{\mathcal{D}}(k^*)\}. \tag{13}$$

Evaluating probabilities of events like $\{\exists k \neq k^*,\ \widehat{\mathcal{D}}(k) \geq \widehat{\mathcal{D}}(k^*)\}$ may be cumbersome. In order to pass from those to individual events $\{\widehat{\mathcal{D}}(k) \geq \widehat{\mathcal{D}}(k^*)\}$ for each k, the following lemma is convenient.

Lemma 2 (Squeezing the Failure Rate). *One can lower and upper bound the failure rate as follows:*

$$\max_{k \neq k^*} \mathbb{P}\{\widehat{\mathcal{D}}(k) \geq \widehat{\mathcal{D}}(k^*)\} \leq \mathrm{FR}(\widehat{\mathcal{D}}) \leq \sum_{k \neq k^*} \mathbb{P}\{\widehat{\mathcal{D}}(k) \geq \widehat{\mathcal{D}}(k^*)\}. \tag{14}$$

Proof. We can write $\mathrm{FR}(\widehat{\mathcal{D}}) = \mathbb{P}\{\bigcup_{k \neq k^*} \{\widehat{\mathcal{D}}(k) \geq \widehat{\mathcal{D}}(k^*)\}\}$. The upper bound follows from the union bound $\mathbb{P}\{\bigcup_k A_k\} \leq \sum_k \mathbb{P}\{A_k\}$. Now the probability of the union is not less that of any individual event $\{\widehat{\mathcal{D}}(k) \geq \widehat{\mathcal{D}}(k^*)\}$. Choosing the one with maximal probability gives the lower bound. □

Remark 1. The lower bound approximation in Eq. (14) is reminiscent of ideas developed by Whitnall and Oswald in [33] where they define a framework for the theoretical evaluation of side-channel distinguishers. Their outcome is captured by the relative behavior of the distinguisher for the correct key and its nearest rival. We leverage on this idea to prove our Theorem 1 in Sect. 3.

Lemma 2 leads us to define pairwise quantities (see e.g., [29, Eq. (13)]).

Definition 3 (Pairwise Deltas). *For any function $f(k)$ define*

$$\Delta f(k^*, k) = f(k^*) - f(k). \tag{15}$$

Thus $\Delta\widehat{\mathcal{D}}(k^*, k) = \widehat{\mathcal{D}}(k^*) - \widehat{\mathcal{D}}(k)$ and $\Delta\mathcal{D}(k^*, k) = \mathcal{D}(k^*) - \mathcal{D}(k)$. The pairwise error probability for the transition $k^* \to k$ is

$$\mathbb{P}\{\widehat{\mathcal{D}}(k) \geq \widehat{\mathcal{D}}(k^*)\} = \mathbb{P}\{\Delta\widehat{\mathcal{D}}(k^*, k) \leq 0\}. \tag{16}$$

Lemma 3. *The difference $\Delta\widehat{\mathcal{D}}(k^*, k)$ estimates $\Delta\mathcal{D}(k^*, k)$ with bias and variance*

$$B_m(k^*, k) = B_m(k^*) - B_m(k) \tag{17}$$

$$V_m(k^*, k) = \mathrm{Var}(\Delta\widehat{\mathcal{D}}(k^*, k)) \tag{18}$$

tending to zero as $m \to +\infty$.

Proof. Since $\widehat{\mathcal{D}}(k) \to \mathcal{D}(k)$ and $\widehat{\mathcal{D}}(k^*) \to \mathcal{D}(k^*)$ in the mean-square sense (Definition 1) we can deduce that $\widehat{\mathcal{D}}(k^*) - \widehat{\mathcal{D}}(k) \to \mathcal{D}(k^*) - \mathcal{D}(k)$ also in the mean-square sense. This follows from Minkowski's inequality $\sqrt{\mathbb{E}\{(X \pm Y)^2\}} \leq \sqrt{\mathbb{E}\{X^2\}} + \sqrt{\mathbb{E}\{Y^2\}}$. The proof of Lemma 1 now applies verbatim to show that $B_m(k^*, k) \to 0$ and $V_m(k^*, k) \to 0$. □

2.3 Soundness

Definition 4 (Soundness Condition). *The attack using distinguisher $\widehat{\mathcal{D}}(k)$ is* sound *if the corresponding theoretical distinguisher's values satisfy the inequalities*

$$\mathcal{D}(k^*) > \mathcal{D}(k) \qquad \text{for all } k \neq k^*. \tag{19}$$

In other words $\Delta\mathcal{D}(k^*, k) > 0$ for all bad key hypotheses k.

In [13] the authors give a proof of soundness for CPA. Note that, DoM can be seen as a special case of CPA (when $m \to \infty$) where $Y \in \{\pm 1\}$ and thus is all the more sound. MIA was proven sound for Gaussian noise in [23,26].

Proposition 1 (Soundness). *When the attack is sound, the success eventually tends to 100 % as m increases:*

$$\mathrm{SR}(\widehat{\mathcal{D}}) \to 1 \textit{ as } m \to +\infty. \tag{20}$$

This has been taken as a definition of soundness in [30, Sect. 5.1]. We provide an elegant proof.

Proof. By Lemma 2, $1 - \mathrm{SR}(\widehat{\mathcal{D}}) \leq \sum_{k \neq k^*} \mathbb{P}\{\Delta\widehat{\mathcal{D}}(k^*, k) \leq 0\}$. It suffices to show that for each $k \neq k^*$, $\mathbb{P}\{\Delta\widehat{\mathcal{D}}(k^*, k) \leq 0\} = \mathbb{P}\{\Delta\mathcal{D}(k^*, k) - \Delta\widehat{\mathcal{D}}(k^*, k) \geq \Delta\mathcal{D}(k^*, k)\}$ tends to zero. Now by the soundness assumption, $\Delta\mathcal{D} = \Delta\mathcal{D}(k^*, k) > 0$. Dropping the dependency on (k^*, k) for notational convenience, one obtains

$$\mathbb{P}\{\Delta\mathcal{D} - \Delta\widehat{\mathcal{D}} \geq \Delta\mathcal{D}\} \leq \frac{\mathbb{E}\Big\{\big(\Delta\mathcal{D} - \Delta\widehat{\mathcal{D}}\big)^2\Big\}}{\Delta\mathcal{D}^2} \to 0 \tag{21}$$

where we have used Chebyshev's inequality $\mathbb{P}\{X \geq \epsilon\} \leq \frac{\mathbb{E}\{X^2\}}{\epsilon^2}$ and the fact that $\Delta\widehat{\mathcal{D}}(k^*, k) \to \Delta\mathcal{D}(k^*, k)$ in the mean-square sense (Lemma 3). $\square$

Since $\mathrm{SR}(\widehat{\mathcal{D}}) \to 1$ as m increases we are led to investigate the rate of convergence of $\mathrm{FR}(\widehat{\mathcal{D}}) = 1 - \mathrm{SR}(\widehat{\mathcal{D}})$ toward zero. This is done next.

3 Derivation of Success Exponent

3.1 Normal Approximation and Assumption

We first prove some normal (Gaussian) behavior in the case of additive distinguishers and then generalize.

Definition 5 (Additive Distinguisher [18]). An additive distinguisher can be written in the form of a sum of i.i.d. terms:

$$\widehat{\mathcal{D}}(X_1, X_2, \ldots, X_m; Y_1(k), Y_2(k), \ldots, Y_m(k)) = \frac{1}{m}\sum_{i=1}^{m} \widehat{\mathcal{D}}(X_i; Y_i(k)). \tag{22}$$

Remark 2. DoM is additive (see e.g., [10]). Attacks maximizing scalar products $\sum_{i=1}^{m} X_i Y_i$ are clearly additive; they constitute a good approximation to CPA, and are even equivalent to CPA if one assumes that the first and second moments of $Y(k)$ are constant independent of k (see [14,27,29] for similar assumptions).

Lemma 4. *When the distinguisher is additive, the corresponding theoretical distinguisher is*

$$\mathcal{D}(X, Y(k)) = \mathbb{E}\{\widehat{\mathcal{D}}(X; Y(k))\}. \tag{23}$$

Thus $\Delta\widehat{\mathcal{D}}(k^*, k)$ is an unbiased estimator of $\Delta\mathcal{D}(k^*, k)$, whose variance is

$$V_m(k^*, k) = \frac{\mathrm{Var}\big(\widehat{\mathcal{D}}(X; Y(k^*)) - \widehat{\mathcal{D}}(X; Y(k))\big)}{m} \tag{24}$$

Proof. Letting $\mathbb{E}\{\widehat{\mathcal{D}}(X; Y(k))\} = \mathcal{D}(k)$, since the terms $\widehat{\mathcal{D}}(X_i; Y_i(k))$ are independent and identically distributed, one has

$$\mathbb{E}\Big\{\big(\widehat{\mathcal{D}}(k) - \mathcal{D}(k)\big)^2\Big\} = \tfrac{1}{m^2}\mathbb{E}\Big\{\sum\nolimits_{i=1}^{m}\big(\widehat{\mathcal{D}}(X_i; Y_i(k)) - \mathcal{D}(k)\big)^2\Big\} \tag{25}$$

$$= \tfrac{1}{m}\mathbb{E}\Big\{\big(\widehat{\mathcal{D}}(X; Y(k)) - \mathcal{D}(k)\big)^2\Big\} \to 0. \tag{26}$$

Therefore, $\frac{1}{m}\sum_{i=1}^{m}\widehat{\mathcal{D}}(X_i; Y_i(k)) \to \mathbb{E}\{\widehat{\mathcal{D}}(X; Y(k))\}$ in the mean-square sense. (This is actually an instance of the weak law of large numbers). The corresponding bias is zero: $\mathbb{E}\{\widehat{\mathcal{D}}(k)\} - \mathcal{D}(k) = 0$.

Taking differences, it follows from Lemma 3 that $\Delta\widehat{\mathcal{D}}(k^*, k) \to \Delta\mathcal{D}(k^*, k)$ in the mean-square sense with zero bias. The corresponding variance is computed as above as $\mathbb{E}\big\{\big(\Delta\widehat{\mathcal{D}}(k^*, k) - \Delta\mathcal{D}(k^*, k)\big)^2\big\} = \frac{1}{m}\mathbb{E}\big\{\big(\big(\widehat{\mathcal{D}}(X; Y(k^*)) - \widehat{\mathcal{D}}(X; Y(k))\big) - \big(\mathcal{D}(X; Y(k^*)) - \mathcal{D}(X; Y(k))\big)\big)^2\big\} = \frac{1}{m}\mathrm{Var}\big(\widehat{\mathcal{D}}(X; Y(k^*)) - \widehat{\mathcal{D}}(X; Y(k))\big)$. □

Proposition 2 (Normal Approximation). *When the distinguisher is additive, $\Delta\widehat{\mathcal{D}}(k^*, k)$ follows the normal approximation*

$$\Delta\widehat{\mathcal{D}}(k^*, k) \sim \mathcal{N}\big(\Delta\mathcal{D}(k^*, k), V_m(k^*, k)\big) \tag{27}$$

as m increases. This means that

$$\frac{\Delta\widehat{\mathcal{D}}(k^*, k) - \Delta\mathcal{D}(k^*, k)}{\sqrt{V_m(k^*, k)}} \tag{28}$$

converges to the standard normal $\mathcal{N}(0, 1)$ in distribution.

Proof. Apply the central limit theorem to the sum of i.i.d. variables $m\Delta\widehat{\mathcal{D}}(k^*, k) = \sum_{i=1}^{m}\widehat{\mathcal{D}}(X_i; Y_i(k^*)) - \widehat{\mathcal{D}}(X_i; Y_i(k))$. It follows that

$$\frac{m\Delta\widehat{\mathcal{D}}(k^*, k) - m\Delta\mathcal{D}(k^*, k)}{\sqrt{m \cdot \mathrm{Var}\left(\Delta\widehat{\mathcal{D}}(k^*, k)\right)}} = \frac{\Delta\widehat{\mathcal{D}}(k^*, k) - \Delta\mathcal{D}(k^*, k)}{\sqrt{V_m(k^*, k)}} \tag{29}$$

tends in distribution to $\mathcal{N}(0, 1)$. □

Remark 3. Notice that the normal approximation is *not* a consequence of a Gaussian noise assumption or anything actually related to the leakage model but is simply a genuine consequence of the central limit theorem.

The above result for additive distinguishers leads us to the following.

Definition 6 (Normal Assumption). *We say that a sound distinguisher follows the* normal assumption *if*

$$\Delta\widehat{\mathcal{D}}(k^*,k) \sim \mathcal{N}\big(\mathbb{E}\{\Delta\widehat{\mathcal{D}}(k^*,k)\}, V_m(k^*,k)\big) \tag{30}$$

as m increases.

Remark 4. We note that in general

$$\mathbb{E}\{\Delta\widehat{\mathcal{D}}(k^*,k)\} = \Delta\mathcal{D}(k^*,k) + \Delta B_m(k^*,k) \tag{31}$$

has a bias term (Lemma 3). By Proposition 2 any additive distinguisher follows the above normal assumption (with zero bias). We shall adopt the normal assumption even in situations where the distinguisher is not additive (as is the case of MIA) with possibly nonzero bias. The corresponding outcomes will be justified by simulations in Sect. 4.

3.2 The Main Result: Success Exponent

Recall a well-known mathematical definition that two functions are *equivalent*: $f(x) \sim g(x)$ if $f(x)/g(x) \to 1$ as $x \to +\infty$. The following defines a weaker type of equivalence $f(x) \approx g(x)$ at first order of exponent, which is required to derive the success exponent SE.

Definition 7 (First-Order Exponent [7, Chap. 11]**).** *We say that a function $f(x)$ has* first order exponent *$\xi(x)$ if $\big(\ln f(x)\big) \sim \xi(x)$ as $x \to +\infty$, in which case we write*

$$f(x) \approx \exp \xi(x). \tag{32}$$

Lemma 5. *Let $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} e^{-t^2/2}\, dt$ be the tail probability of the standard normal (a.k.a. Marcum function). Then as $x \to +\infty$,*

$$Q(x) \approx e^{-x^2/2}. \tag{33}$$

Proof. For $t > x$, we can write

$$\int_x^{+\infty} \frac{1+1/t^2}{1+1/x^2} \frac{e^{-t^2/2}}{\sqrt{2\pi}}\, \mathrm{d}t \leq Q(x) \leq \int_x^{+\infty} \frac{t}{x} \frac{e^{-t^2/2}}{\sqrt{2\pi}}\, \mathrm{d}t. \tag{34}$$

Taking antiderivative yields

$$\frac{1}{1+1/x^2} \frac{1}{\sqrt{2\pi}} \frac{e^{-x^2/2}}{x} \leq Q(x) \leq \frac{1}{x\sqrt{2\pi}} e^{-x^2/2}. \tag{35}$$

Taking the logarithm gives

$$-x^2/2 - \ln(x+1/x) - \ln(2\pi)/2 \leq \ln Q(x) \leq -x^2/2 - \ln x - \ln(2\pi)/2 \tag{36}$$

which shows that $\ln Q(x) \sim -x^2/2$. □

Lemma 6. *Under the normal assumption,*

$$\mathbb{P}\{\Delta\widehat{\mathcal{D}}(k^*,k) \le 0\} \approx \exp\Big(-\frac{\big(\Delta\mathcal{D}(k^*,k)+\Delta B_m(k^*,k)\big)^2}{2\,V_m(k^*,k)}\Big). \tag{37}$$

Proof. Noting that

$$\mathbb{P}\{\Delta\widehat{\mathcal{D}}(k^*,k) \le 0\} = \mathbb{P}\Big\{\frac{\Delta\widehat{\mathcal{D}}(k^*,k)-\mathbb{E}\{\Delta\widehat{\mathcal{D}}(k^*,k)\}}{\sqrt{V_m(k^*,k)}} \le \frac{-\mathbb{E}\{\Delta\widehat{\mathcal{D}}(k^*,k)\}}{\sqrt{V_m(k^*,k)}}\Big\} \tag{38}$$

and using the normal approximation it follows that

$$\mathbb{P}\{\Delta\widehat{\mathcal{D}}(k^*,k) \le 0\} \approx Q\Big(\frac{\mathbb{E}\{\Delta\widehat{\mathcal{D}}(k^*,k)\}}{\sqrt{V_m(k^*,k)}}\Big) \tag{39}$$

where $\mathbb{E}\{\Delta\widehat{\mathcal{D}}(k^*,k)\} = \Delta\mathcal{D}(k^*,k)+\Delta B_m(k^*,k)$. The assertion now follows from Lemma 5. □

Theorem 1. *Under the normal assumption,*

$$\mathrm{FR}(\widehat{\mathcal{D}}) = 1-\mathrm{SR}(\widehat{\mathcal{D}}) \approx \exp\Big(-\min_{k\neq k^*}\frac{\big(\Delta\mathcal{D}(k^*,k)+\Delta B_m(k^*,k)\big)^2}{2\,V_m(k^*,k)}\Big). \tag{40}$$

Proof. We combine Lemmas 2 and 6. The lower bound of $\mathrm{FR}(\widehat{\mathcal{D}})$ is

$$\approx \max_{k\neq k^*}\exp\Big(-\frac{\big(\Delta\mathcal{D}(k^*,k)+\Delta B_m(k^*,k)\big)^2}{2\,V_m(k^*,k)}\Big) \tag{41}$$

$$= \exp\Big(-\min_{k\neq k^*}\frac{\big(\Delta\mathcal{D}(k^*,k)+\Delta B_m(k^*,k)\big)^2}{2\,V_m(k^*,k)}\Big). \tag{42}$$

The upper bound is the sum of vanishing exponentials (for $k \neq k^*$) which is equivalent to the maximum of the vanishing exponentials, which yields the same expression. The result follows since the lower and upper bounds from Lemma 2 are equivalent as m increases. □

Corollary 1. *For any additive distinguisher,*

$$\mathrm{FR}(\widehat{\mathcal{D}}) = 1-\mathrm{SR}(\widehat{\mathcal{D}}) \approx e^{-m\cdot\mathrm{SE}(\widehat{\mathcal{D}})} \tag{43}$$

where

$$\mathrm{SE}(\widehat{\mathcal{D}}) = \min_{k\neq k^*}\frac{\Delta\mathcal{D}(k^*,k)^2}{2\,\mathrm{Var}\big(\widehat{\mathcal{D}}(X;Y(k^*))-\widehat{\mathcal{D}}(X;Y(k))\big)}. \tag{44}$$

Proof. Apply the above theorem using Lemma 4 and Proposition 2. □

Remark 5. We show in Sect. 5 that for non-additive distinguisher such as MIA the closed-form expression for the first-order exponent is linear in the number of measurements m so that the expression $1-\mathrm{SR} \approx e^{-m\cdot\mathrm{SE}}$ may be considered as fairly general for large m. Moreover, we experimentally show in the next section that this approximation already holds with excellent approximation for a relatively small number of measurements m.

4 Success Exponent for Few Measurements

Some devices such as unprotected 8-bit microprocessors require only a small number of measurements to reveal the secret key. As the SNR is relatively high, the targeted variable has the length of the full size, and on such processors, the pipeline is short or even completely absent. On such worst-case platforms, such as the AVR ATMega, the SNR can be has high as 7, for those instructions consisting in memory look-ups. A CPA requires $m = 12$ measurements (cf. DPA contest v4, for attacks reported in [2]).

In order to investigate the relation $\mathrm{SR} \approx 1-e^{-m\mathrm{SE}}$ for such small values of m, we target PRESENT [3], which is an SPN (Substitution Permutation Network) block cipher, with leakage model given by $Y(k) = HW(\mathtt{Sbox}(T \oplus k))$, where $\mathtt{Sbox} : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ is the PRESENT substitution box and $k \in \mathbb{F}_2^4$. We considered $N \sim \mathcal{N}(0,1)$ in our simulations applied to the following distinguishers:

- optimal distinguisher (a.k.a. template attack [6], whose formal expression is given in [15] for Gaussian noise);
- DoM [17][2] on bit #2;
- CPA (Example 1),
- MIA (Example 2), with three distinct bin widths of length $\Delta x \in \{1,2,4\}$, and two kinds of binning:
  - B1, which partitions $\mathbb{R}$ as $\bigcup_{i\in\mathbb{N}}[i\Delta x, (i+1)\Delta x[$, and
  - B2, which partitions $\mathbb{R}$ as $\bigcup_{i\in\mathbb{N}}[(i-\frac{1}{2})\Delta x, (i+\frac{1}{2})\Delta x[$.

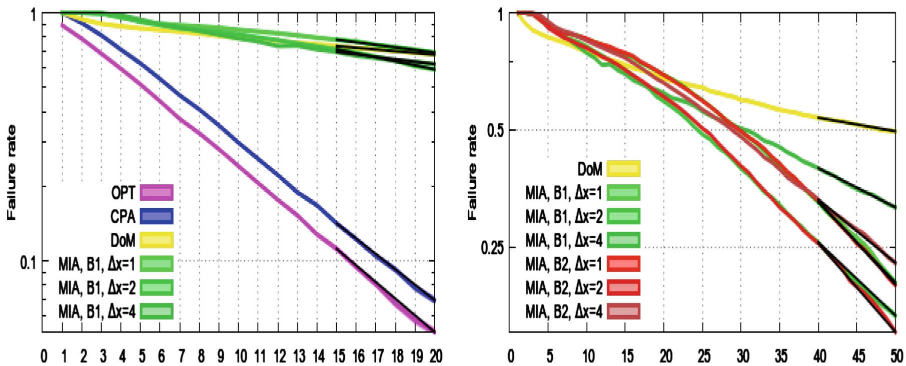


Fig. 1. Failure rate for few measurements. (a) Optimal distinguisher, CPA, DoM, and MIA. (b) Zoom out for less efficient attacks DoM and MIA.

Figure 1 shows the failure rate in a logarithmic scale for 10,000 simulations with additional error bars as described in [19]. To assess the linear dependence

[2] It is known that for bit #1, the DoM is not sound: the same distinguisher value can be obtained for the correct key $k = k^*$ and for at least one incorrect key $k = k^* \oplus \mathtt{0x9}$.

$\log(1-\mathrm{SR}) = -m\mathrm{SE}$ between the logarithm of the error rate and the number of traces, we have superimposed the linear slope $-\mathrm{SE}$ in black. We find that CPA and the optimal distinguishers behave according to the law for m as small as 2! The error rate of MIA and DoM becomes linear for $m \geq 40$. Interestingly, for MIA, the binning size has an impact (see also [12,23]). The best parameterization of the MIA corresponds to $\Delta x = 2$, for both B1 and B2.

5 Closed-Form Expressions of SE

5.1 Success Exponents for DoM and CPA

We precise our side-channel model from Eq. (2) in case of additive distinguishers. As these distinguishers are most usually used when the leakage X is linearly depend on Y^*, we assume similar to previous works [10,31] $X = \alpha Y^* + N$. To simplify the derivation, we assume that the distribution of $Y(k)$ is identical for all k. In other words, knowing the distribution of $Y(k)$ does not give any evidence about the secret (see [14,27] for similar assumptions). In particular $\mathrm{Var}\{Y(k)\}$ is constant for all k. Without loss of generality we may normalize the sensitive variable Y such that $\mathbb{E}\{Y(k)\} = 0$ and $\mathrm{Var}\{Y(k)\} = \mathbb{E}\{Y(k)^2\} = 1$. The SNR is thus equal to α^2/σ^2.

We first extend the idea of confusion similar to [31], which we call *general 2-way confusion coefficients*.

Definition 8 (General 2-way Confusion Coefficients). *For $k \neq k^*$ we define*

$$\kappa(k^*, k) = \mathbb{E}\Big\{\Big(\frac{Y(k^*) - Y(k)}{2}\Big)^2\Big\}, \tag{45}$$

$$\kappa'(k^*, k) = \mathbb{E}\Big\{Y(k^*)^2\Big(\frac{Y(k^*) - Y(k)}{2}\Big)^2\Big\}. \tag{46}$$

Remark 6. The authors of [10] defined the confusion coefficient as $\kappa(k^*, k) = \mathbb{P}\{Y(k^*) \neq Y(k)\}$. A straightforward computation gives

$$\begin{aligned}\mathbb{P}\{Y(k^*) \neq Y(k)\} &= \mathbb{P}\{Y(k^*) = -1, Y(k) = 1)\} + \mathbb{P}\{Y(k^*) = -1, Y(k) = 1\} \\ &= \mathbb{E}\{\big(\frac{Y(k^*) - Y(k)}{2}\big)^2\}. \end{aligned} \tag{47}$$

Thus our definition is consistent and a natural extension of the work in [10].

The alternative confusion coefficient introduced in [31] is defined as $\kappa^\circ(k^*, k) = \mathbb{E}\{Y(k^*)Y(k)\}$. The following relationship is easily obtained:

$$\kappa^\circ(k^*, k) = 1 - 2\kappa(k^*, k). \tag{48}$$

Proposition 3 (SE for CPA). *The success exponent for* CPA *takes the closed-form expression*

$$\mathrm{SE} = \min_{k \neq k^*} \frac{\alpha^2 \kappa^2(k^*, k)}{2(\alpha^2(\kappa'(k^*, k) - \kappa^2(k^*, k)) + \sigma^2 \kappa(k^*, k))}. \tag{49}$$

Proof. Proposition 3 is an immediate consequence of the formula in Eq. (44) and the following lemma. □

Lemma 7. *The first two moments of* $\widehat{\Delta\mathcal{D}}(k^*, k)$ *are given by*

$$\mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*, k)\} = 2\alpha\kappa(k^*, k), \tag{50}$$

$$\mathrm{Var}(\widehat{\Delta\mathcal{D}}(k^*, k)) = 4[\alpha^2(\kappa'(k^*, k) - \kappa^2(k^*, k)) + \sigma^2\kappa(k^*, k)]. \tag{51}$$

Proof. Recall from Remark 2 that $\widehat{\Delta\mathcal{D}}(k^*, k) = XY^* - XY = (\alpha Y^* + N)(Y^* - Y)$. On one hand, since we assumed that $\mathbb{E}\{(Y^*)^2\} = 1$, we obtain

$$\mathbb{E}\{Y^*(Y^* - Y)\} = 1 - \mathbb{E}\{Y^*Y\} = 2\mathbb{E}\Big\{\Big(\frac{Y^* - Y}{2}\Big)^2\Big\} = 2\kappa(k^*, k). \tag{52}$$

On the other hand, since N is independent of Y,

$$\mathbb{E}\{N(Y^* - Y)\} = \mathbb{E}\{N\} \cdot \mathbb{E}\{Y^* - Y\} = 0. \tag{53}$$

Combining we obtain $\mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*, k)\} = 2\alpha\kappa(k^*, k)$. For the variance we have

$$\begin{aligned} \mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*, k)^2\} &= \mathbb{E}\{(XY^* - XY)^2\} && (54)\\ &= \mathbb{E}\{N^2(Y^* - Y)^2\} + \alpha^2\mathbb{E}\{Y^{*2}(Y^* - Y)^2\} && (55)\\ &= 4\sigma^2\kappa(k^*, k) + \alpha^2 4\kappa'(k^*, k), && (56) \end{aligned}$$

since all cross terms with N vanish. It follows that

$$\begin{aligned} \mathrm{Var}(\widehat{\Delta\mathcal{D}}(k^*, k)) &= \mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*, k)^2\} - \mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*, k)\}^2 && (57)\\ &= 4[\alpha^2(\kappa'(k^*, k) - \kappa^2(k^*, k)) + \sigma^2\kappa(k^*, k)]. && (58) \end{aligned}$$

as announced. □

For DoM with one-bit variables $Y(k) \in \{\pm 1\}$ we can further simplify the success exponent such that it can be expressed directly through the SNR $= \alpha^2/\sigma^2$, number of measurements and 2-way confusion coefficient $\kappa(k^*, k)$:

Proposition 4 (SE for 1-bit DoM). *The success exponent for* DoM *takes the closed-form expression*

$$\mathrm{SE} = \frac{1}{\max\limits_{k \neq k^*}\Big(\dfrac{2 - 2\kappa(k^*, k)}{\kappa(k^*, k)} + \dfrac{2}{\kappa(k^*, k)\,\mathrm{SNR}}\Big)} \tag{59}$$

Proof. When $Y(k) \in \{\pm 1\}$ on has the additional simplification:

$$\kappa(k^*, k) = \mathbb{E}\Big\{\Big(\frac{Y(k^*) - Y(k)}{2}\Big)^2\Big\} = \mathbb{E}\Big\{Y(k^*)^2\Big(\frac{Y(k^*) - Y(k)}{2}\Big)^2\Big\} = \kappa'(k^*, k). \tag{60}$$

Now Proposition 4 follows directly from Proposition 3. □

Remark 7. Estimating the success rate directly from confusion coefficients includes a computation of a multivariate normal cumulative distribution function [28] for which we have found that no closed-form expression exists. Moreover, the corresponding covariance matrices $[\kappa(k^*, i, j)]_{i,j}$ and $[\kappa(k^*, i) \times \kappa(k^*, j)]_{i,j}$ that depend on the confusion coefficients are not of full rank. This effect was similarly discovered for CPA by Rivain in [29], where the author propose to use Monte-Carlo simulation to overcome this problem.

Therefore, it is difficult to rederive the expressions above for the success exponent from the exact expressions of SR in [10,29]. However, one clearly obtains the same exponential convergence behavior of SR toward 100 %.

As a result, we stress that the closed-form expressions of SE above are more convenient than the exact expressions for the SR for DoM and CPA, since in the SE, only 2-way confusion coefficients $\kappa(k^*, k), \kappa'(k^*, k)$ are involved without the need to compute multivariate distributions.

5.2 Success Exponent for the Optimal Distinguisher

Definition 9 (Optimal Distinguisher [15]**).** In case α is known and the noise is Gaussian the *optimal distinguisher* is additive and given by

$$\mathcal{D}(k) = -(X - \alpha Y)^2 \tag{61}$$

$$\widehat{\mathcal{D}}(X, Y(k)) = -(X - \alpha Y(k))^2. \tag{62}$$

Interestingly, as we show in the following proposition the optimal distinguisher involves the following confusion coefficient.

Definition 10 (Confusion Coefficient for the Optimal Distinguisher). *For $k \neq k^*$ we define*

$$\kappa''(k^*, k) = \mathbb{E}\Big\{ \Big(\frac{Y(k^*) - Y(k)}{2} \Big)^4 \Big\}. \tag{63}$$

Proposition 5 (SE for the Optimal Distinguisher). *The success exponent for the optimal distinguisher takes the closed-form expression*

$$\mathrm{SE} = \min_{k \neq k^*} \frac{\alpha^2 \kappa^2(k^*, k)}{2(\sigma^2 \kappa(k^*, k) + \alpha^2(\kappa''(k^*, k) - \kappa(k^*, k))}. \tag{64}$$

Proof. Proposition 5 is an immediate consequence of the formula in Eq. (44) and the following lemma. ☐

Lemma 8. *The first two moments of $\widehat{\Delta\mathcal{D}}(k^*, k)$ are given by*

$$\mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*, k)\} = 4\alpha^2 \kappa(k^*, k), \tag{65}$$

$$\mathrm{Var}(\widehat{\Delta\mathcal{D}}(k^*, k)) = 16\alpha^2(\sigma^2 \kappa(k^*, k) + \alpha^2(\kappa(k^*, k)'' - \kappa(k^*, k))). \tag{66}$$

Proof. Recall that $\mathbb{E}\{N\}=0$. Straightforward calculation yields

$$\mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*,k)\} = \mathbb{E}\{-(X-\alpha Y^*)^2 + (X-\alpha Y)^2\} \tag{67}$$
$$= \mathbb{E}\{2N\alpha(Y^*-Y)\} + \mathbb{E}\{\alpha^2(Y^*-Y)^2\} \tag{68}$$
$$= 4\alpha^2\kappa(k^*,k). \tag{69}$$

Next we have

$$\mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*,k)^2\} = \mathbb{E}\{(2N\alpha(Y^*-Y) + \alpha^2(Y^*-Y)^2)^2\} \tag{70}$$
$$= \mathbb{E}\{4N^2\alpha^2(Y^*-2)^2\} + \mathbb{E}\{(Y^*-Y)^4\alpha^4\} \tag{71}$$
$$= 16\alpha^2\sigma^2\kappa(k^*,k) + 16\alpha^4\kappa''(k^*,k) \tag{72}$$

which yields the announced formula for the variance. □

Corollary 2. *The closed-form expressions for* DoM*,* CPA *and for the optimal distinguisher simplify for high noise $\sigma \gg \alpha$ in a single equation:*

$$\mathrm{SE} \;\approx\; \min_{k\neq k^*} \frac{\alpha^2\kappa^2(k^*,k)}{2\sigma^2\kappa(k^*,k)} \;=\; \frac{1}{2}\cdot \mathrm{SNR}\cdot \min_{k\neq k^*}\kappa(k^*,k). \tag{73}$$

Proof. Trivial and left to the reader. □

Remark 8. Corollary 2 is inline with the findings in [15], that CPA and the optimal distinguisher become closer the lower the SNR. However, note that, in [15] CPA is the correlation of the absolute value.

Remark 9. From Corollary 2 and the relationship $1-\mathrm{SR} \approx e^{-m\cdot \mathrm{SE}}$ one can directly determine that if, e.g., the SNR is decreased by a factor of 2 the number of measurements m have to multiplied by 2 in order to achieve the same success. This verifies a well-known "rule of thumb" for side-channel attacks (see e.g., [20]).

5.3 Success Exponent for MIA

Unlike CPA or DoM, the estimation of the mutual information in MIA:

$$\mathcal{D}(k) = I(X,Y) = H(X) - H(X|Y) \tag{74}$$
$$= -\int p(x)\log p(x)\,\mathrm{d}x + \sum_y p(y)\int p(x|y)\log p(x|y)\,\mathrm{d}x \tag{75}$$

is a nontrivial problem. While Y is discrete, the computation of mutual information requires the estimation of the conditional pdfs $p(x|y)$. For a detailed evaluation of estimation methods for MIA we refer to [32].

In the following, we consider the estimation with histograms (H-MIA) in order to simplify the derivation of a closed-form expression for SE. One partitions the leakage X into h distinct bins b_i of width Δx with $i = 1,\ldots,h$.

Definition 11. *Let* $\hat{p}(x) = \frac{\#b_i}{m}$ *where* $\#b_i$ *is the number of leakage values falling into bin* b_i *and let* $\hat{p}(x|y)$ *be the estimated probability knowing* $Y = y$*. Then*

$$\widehat{\mathcal{D}}(k) = -\sum_x \hat{p}(x)\log\hat{p}(x) + \sum_y \hat{p}(y)\sum_x \hat{p}(x|y)\log\hat{p}(x|y). \tag{76}$$

To simplify the presentation that follows, we consider only the conditional negentropy $-\hat{H}(X|Y)$ as a distinguisher, since $\hat{H}(X)$ does not depend on the key hypothesis k. Additionally, we assume that the distribution of Y is known to the attacker so that she can use $p(y)$ instead of $\hat{p}(y)$. Now H-MIA simplifies to

$$\mathsf{H\text{-}MIA}(X,Y) = \sum_y p(y)\sum_x \hat{p}(x|y)\log\hat{p}(x|y) + \log\Delta x. \tag{77}$$

The additional term $\log\Delta x$ arises due to the fact that we have estimated the differential entropy $H(X)$. For more information on differential entropy and mutual information we refer to [7].

Proposition 6 (SE for H-MIA).

$$\mathrm{SE} \approx \min_{k^*\neq k}\frac{\frac{1}{2}\big(\Delta\mathcal{D}(k^*,k) + \frac{\Delta x^2}{24}\big(\Delta J(k^*,k)\big)\big)^2}{\sum_y p(y)\mathrm{Var}\{-\log p(X|Y=y)\} + \sum_{y^*} p(y^*)\mathrm{Var}\{-\log p(X|Y=y^*)\}}, \tag{78}$$

where $\Delta\mathcal{D}(k^*,k) = H(X|Y) - H(X|Y^*)$*,* $\Delta J(k^*,k) = J(X|Y) - J(X|Y^*)$*,* $J(X|Y) = \sum_y p(y)J(X|Y=y)$ *and* $J(X|Y)$ *is the Fisher information [11]:*

$$J(X|Y=y) = \int_{-\infty}^{\infty}\frac{[\frac{d}{dx}p(x|y)]^2}{p(x|y)}\,dx. \tag{79}$$

Proof. Since Y is discrete the bias only arise due to the discretization of X and the limited number of measurements m. Therefore, we use the approximations given for the bias of $\hat{H}(X)$ in [22] (3.14) to calculate $\mathbb{E}\{\widehat{\mathcal{D}}(k)\}$ and $\mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*,k)\}$ for H-MIA. To be specific, let h define the number of bins and Δx their width. Then

$$\mathbb{E}\{\widehat{\mathcal{D}}(k)\} = -\mathbb{E}\{\hat{H}(X|Y)\} = -\sum_y p(y)\mathbb{E}\{\hat{H}(X|Y=y)\}, \tag{80}$$

$$\approx -\sum_y p(y)\big[H(X|Y=y) + \frac{\Delta x^2}{24}J(X|Y=y)\big] - \frac{h-1}{2m}, \tag{81}$$

$$\mathbb{E}\{\widehat{\Delta\mathcal{D}}(k^*,k)\} \approx \sum_y p(y)\big[H(X|Y=y) + \frac{\Delta x^2}{24}J(X|Y=y)\big] - \Big(\sum_{y^*} p(y^*)\big[H(X|Y^*=y^*) + \frac{\Delta x^2}{24}J(X|Y^*=y^*)\big]\Big), \tag{82}$$

with $J(X|Y) = \sum_y p(y)J(X|Y = y)$ and $J(X|Y = y)$ being the Fisher information $\int_{-\infty}^{\infty} \frac{[\frac{d}{dx}p(x|y)]^2}{p(x|y)}\,\mathrm{d}x$ [11].

To calculate $\mathrm{Var}\{\widehat{\mathcal{D}}(k)\}$ we use the law of total variance [16] and the approximations for the variance given in [22] (4.9):

$$\mathrm{Var}\{\widehat{\mathcal{D}}(k)\} = \mathrm{Var}\{\hat{H}(X|Y)\}\} = \mathrm{Var}\{\mathbb{E}\{\hat{H}(X|Y = y)\}\} \tag{83}$$

$$\approx \mathrm{Var}\{H(X)\} - \frac{1}{m}\sum_y p(y)\mathrm{Var}\{-\log p(x|y)\} \tag{84}$$

$$\mathrm{Var}\{\widehat{\Delta\mathcal{D}}(k^*, k)\} = \mathrm{Var}\{\mathbb{E}\{\hat{H}(X|Y = y\}\} - \mathrm{Var}\{\mathbb{E}\{\hat{H}(X|Y^* = y^*\}\} \tag{85}$$

$$- 2\mathrm{Cov}(\mathbb{E}\{\hat{H}(X|Y = y\}\}, \mathbb{E}\{\hat{H}(X|Y^* = y^*\}\})$$

$$\approx \frac{1}{m}\Big(\sum_y p(y)\mathrm{Var}\{-\log p(x|y)\} + \sum_y p(y^*)\mathrm{Var}\{-\log p(x|y^*)\}\Big) \tag{86}$$

From Eqs. (82) and (86) Proposition 6 follows directly. □

Remark 10. Interestingly, even if MIA is not additive the SE is linear in the number of measurements m just like for DoM and CPA. This is also confirmed experimentally in the next subsection.

Remark 11. If N is normal distributed with variance σ^2 we can further simplify $H(X|Y^* = y^*) = \frac{1}{2}\log(2\pi e\sigma^2)$ since $p(x|y^*) = p_N(x - y^*)$. Moreover, one has $J(X|Y^* = y) = \frac{1}{\sigma^2}$ and $\mathrm{Var}\{-\log p(x|y^*)\} = \frac{1}{2m}$.

Remark 12. Remarkably, the variance term does not depend on the size of Δx except in extreme cases like $\Delta x = 1$ and $\Delta x \to \infty$ – see [22] for more information.

5.4 Validation of the SE

To illustrate the validity of the success exponent and the derived closed-form expressions, we choose the same scenario as in Sect. 4 (targeting the Sbox of PRESENT) with a higher variance of the noise. We increased the bin width Δx to 4 for MIA, which lead to the best success when comparing with other widths. To be reliable we conducted 500 independent experiments in each setting.

With the appropriate parameters (confusion coefficients, SNR, etc.), we have computed the exact values for the closed-form expressions in Eqs. (49), (59), (64), and (78) for CPA, DoM, the optimal distinguisher, and MIA which are listed in Table 1 with SE for several σ's. Additionally, we computed for CPA, DoM, and the optimal distinguisher the SE in case of low noise from Eq. (73). To show that these values are valid and reasonable, we estimated the success exponent $\widehat{\mathrm{SE}}$ from the general theoretical formula in Eq. (44) using simulations. One can observe that Corollary 2 is valid.

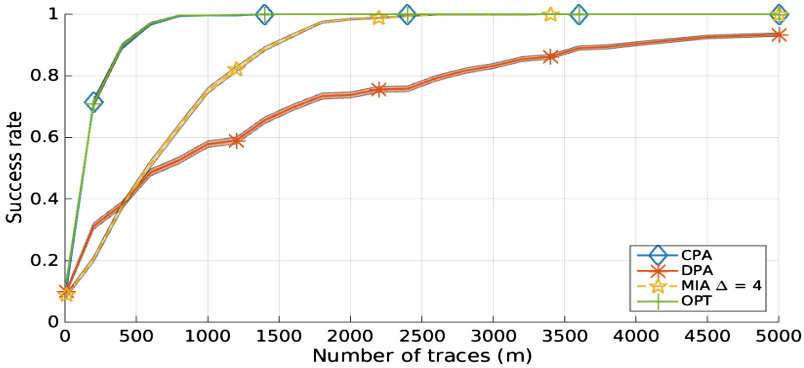
Moreover, we estimated the success exponent directly from the obtained success rate as $-\log(1 - \mathrm{SR}(\widehat{\mathcal{D}}))/m$; this was done for limited values of m to avoid

Table 1. Experimental validation of SE for several σ (values $\times 10^{-3}$)

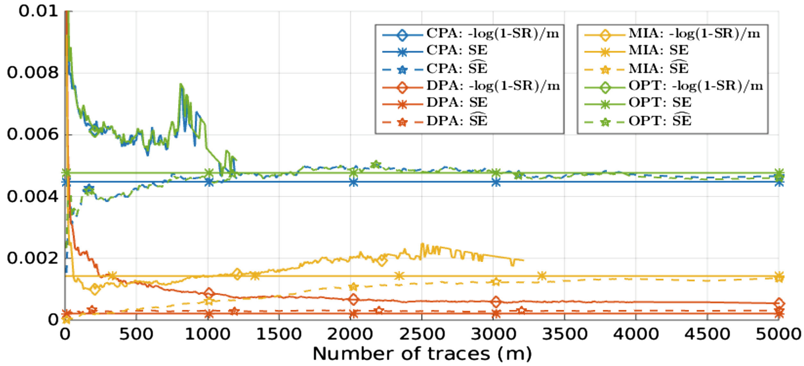
$\times 10^{-3}$	$\sigma = 5$				$\sigma = 7$				$\sigma = 10$			
	DPA	CPA	OPT	MIA	DPA	CPA	OPT	MIA	DPA	CPA	OPT	MIA
SE	0.2	4.5	4.8	1.4	0.1	2.3	2.4	0.8	0.01	1.2	1.2	0.4
SE (Eq. (73))	0.2	4.7	4.7	—	0.1	2.4	2.4	—	0.01	1.2	1.2	—
$\widehat{\text{SE}}$	0.3	4.7	4.6	1.4	0.1	2.3	2.3	0.8	0.1	1.1	1.2	0.2

the saturation effect of the $\text{SR}(\widehat{\mathcal{D}}) = 1$. Figure 2b displays the theoretical value of SE along with the estimations as a function of the number of measurements for $\sigma = 5$. For comparison we plot the success rate in Fig. 2a.

Remarkably, one can see that for all distinguishers, the two estimated values are getting closer to the theoretical SE as m increases. This confirms our theoretical study in Sect. 3 and also demonstrates that the first-order exponent of MIA is indeed linear in the number of measurements as expected.

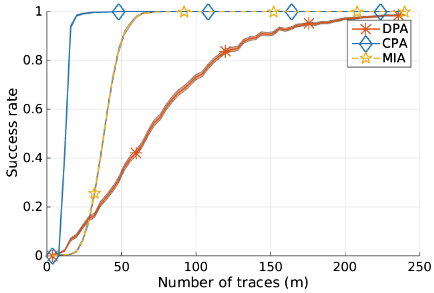


(a) Success rate

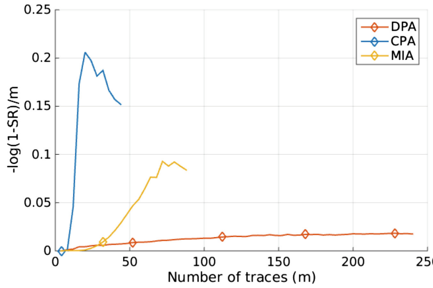


(b) Validation of the success exponent

Fig. 2. Success rate [top graph] and success exponent (SE) [bottom graph]



(a) Success rate $\mathrm{SR}(\widehat{\mathcal{D}})$



(b) $-\log(1-\mathrm{SR}(\widehat{\mathcal{D}}))/m$

Fig. 3. Empirical results using real traces (Arduino board)

Furthermore, for practical measurements we used an Arduino pro mini board with an AVR 328p micro-controller running at 16 MHz. We captured the operation of the AES Substitution box during the first round at 2 GSa/s using an EM probe. Figure 3a shows the success rate for DoM, CPA and MIA for 1600 independent retries. We plot $-\log(1-\mathrm{SR}(\widehat{\mathcal{D}}))/m$ in Fig. 3b. One can observe that DoM converges to a constant. For CPA and MIA the saturation effect of $\mathrm{SR}(\widehat{\mathcal{D}}) = 1$ is disguising the convergence.

These results raise a lot of new perspectives which we discuss next.

6 Conclusion and Perspectives for Further Applications

In this work we investigated in the first-order exponent (success exponent SE) of the success rate for arbitrary sound distinguishers under a mild normal assumption as m increases. The resulting expressions were derived under the asymptotic condition that the number of measurements m tends to infinity, but already hold accurately for reasonable low values of m. More precisely, in the investigated scenarios the approximations for CPA hold for $m \geq 2$ whereas for MIA we have $m \geq 40$. As an illustration we derived the closed-form expressions of the SE for DoM, CPA, the optimal distinguisher, and MIA and showed that they agree theoretically and empirically.

This novel first-order exponent raises many new perspectives. In particular, the resulting closed-form expressions for the SE allows one to answer questions such as: "*How many more traces?*" for achieving a given goal. For example, suppose that one has obtained SE = 90 % after m measurements. To obtain 99 % success with the same distinguisher (hence the same SE), one should approximately square $(1-\mathrm{SR})^2 = (0.1)^2 = 0.01$ which amounts to doubling m. Thus as a rule of thumb we may say that "*doubling the number of traces allows one to go from 90 % to 99 % chance of success*".

Finally, we underline that the success exponent would constitute another approach to the question of comparing substitution boxes with respect to their exploitability in side-channel analysis. It can nicely complement methods like transparency order [25] (and variants thereof [5,24]). It can also characterize, in the same framework, various countermeasures such as no masking vs. masking.

The generality of the proposed approach to derive the success exponent allows one to investigate attack performance in many different scenarios, and we feel that for this reason it is a promising tool.

Acknowledgements. The authors are grateful to Darshana Jayasinghe for the real-world validation on traces taken from the Arduino board.

References

1. Batina, L., Robshaw, M. (eds.): CHES 2014. LNCS, vol. 8731. Springer, Heidelberg (2014)
2. Belgarric, P., Bhasin, S., Bruneau, N., Danger, J.-L., Debande, N., Guilley, S., Heuser, A., Najm, Z., Rioul, O.: Time-frequency analysis for second-order attacks. In: Francillon, A., Rohatgi, P. (eds.) CARDIS 2013. LNCS, vol. 8419, pp. 108–122. Springer, Heidelberg (2014)
3. Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
4. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
5. Chakraborty, K., Sarkar, S., Maitra, S., Mazumdar, B., Mukhopadhyay, D., Prouff, E.: Redefining the transparency order. In: The Ninth International Workshop on Coding and Cryptography, WCC 2015, Paris, France, April 13–17, 2015
6. Chari, S., Rao, J.R.: Rohatgi template attacks. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 13–28. Springer, Heidelberg (2003)
7. Cover, T.M., Thomas, J.A.: Elements of Information Theory, 2nd edn. Wiley-Interscience, July 18, 2006. ISBN-10: ISBN-10: 0471241954, ISBN-13: 978–0471241959
8. Doget, J., Prouff, E., Rivain, M., Standaert, F.-X.: Univariate side channel attacks and leakage modeling. J. Cryptographic Eng. **1**(2), 123–144 (2011)
9. Duc, A., Faust, S., Standaert, F.-X.: Making masking security proofs concrete. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 401–429. Springer, Heidelberg (2015)
10. Fei, Y., Luo, Q., Ding, A.A.: A statistical model for DPA with novel algorithmic confusion analysis. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 233–250. Springer, Heidelberg (2012)
11. Ronald, A.: Statistical Methods for Research Workers. Oliver and Boyd, Edinburgh (1925)
12. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual information analysis. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 426–442. Springer, Heidelberg (2008)

13. Guilley, S., Hoogvorst, P., Pacalet, R., Schmidt, J.: Improving side-channel attacks by exploiting substitution boxes properties. In: Presse Universitaire de Rouen et du Havre (ed.), BFCA, Paris, France, pp. 1–25, May 02–04, 2007. http://www.liafa.jussieu.fr/bfca/books/BFCA07.pdf
14. Heuser, A., Kasper, M., Schindler, W., Stottinger, M.: How a symmetry metric assists side-channel evaluation - a novel model verification method for power analysis. In: Proceedings of the 2011 14th Euromicro Conference on Digital System Design, DSD 2011, pp. 674–681. IEEE Computer Society, Washington DC (2011)
15. Heuser, A., Rioul, O., Guilley, S.: Good Is not good enough - deriving optimal distinguishers from communication theory. In: Batina and Robshaw [1], pp. 55–74
16. Kardaun, O.J.W.F.: Classical Methods of Statistics. Springer, Heidelberg (2005)
17. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
18. Lomné, V., Prouff, E., Rivain, M., Roche, T., Thillard, A.: How to estimate the success rate of higher-order side-channel attacks. In: Batina and Robshaw [1], pp. 35–54
19. Maghrebi, H., Rioul, O., Guilley, S., Danger, J.-L.: Comparison between side-channel analysis distinguishers. In: Chim, T.W., Yuen, T.H. (eds.) ICICS 2012. LNCS, vol. 7618, pp. 331–340. Springer, Heidelberg (2012)
20. Mangard, S.: Hardware countermeasures against DPA – a statistical analysis of their effectiveness. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 222–235. Springer, Heidelberg (2004)
21. Mangard, S., Oswald, E., Standaert, F.-X.: One for All - All for One: Unifying Standard DPA Attacks. IET Inf. Secur. **5**(2), 100–111 (2011). doi:10.1049/iet-ifs.2010.0096. ISSN: 1751–8709
22. Moddemeijer, R.: On estimation of entropy and mutual information of continuous distributions. Signal Process. **16**(3), 233–248 (1989)
23. Moradi, A., Mousavi, N., Paar, C., Salmasizadeh, M.: A comparative study of mutual information analysis under a gaussian assumption. In: Youm, H.Y., Yung, M. (eds.) WISA 2009. LNCS, vol. 5932, pp. 193–205. Springer, Heidelberg (2009)
24. Picek, S., Mazumdar, B., Mukhopadhyay, D., Batina, L.: Modified transparency order property: solution or just another attempt. In: Chakraborty, R.S., Schwabe, P., Solworth, J. (eds.) Security, Privacy, and Applied Cryptography Engineering. LNCS, vol. 9354, pp. 210–227. Springer, Heidelberg (2015)
25. Prouff, E.: DPA attacks and S-boxes. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 424–441. Springer, Heidelberg (2005)
26. Prouff, E., Rivain, M.: Theoretical and practical aspects of mutual information based side channel analysis. In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 499–518. Springer, Heidelberg (2009)
27. Prouff, E., Rivain, M., Bevan, R.: Statistical analysis of second order differential power analysis. IEEE Trans. Comput. **58**(6), 799–811 (2009)
28. Rao, C.R.: Linear Statistical Inference and its Applications, 2nd edn. J. Wiley and Sons, New York (1973)
29. Rivain, M.: On the exact success rate of side channel analysis in the gaussian model. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 165–183. Springer, Heidelberg (2009)
30. Standaert, F.-X., Malkin, T.G., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 443–461. Springer, Heidelberg (2009)

31. Thillard, A., Prouff, E., Roche, T.: Success through confidence: evaluating the effectiveness of a side-channel attack. In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 21–36. Springer, Heidelberg (2013)
32. Veyrat-Charvillon, N., Standaert, F.-X.: Mutual information analysis: how, when and why? In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 429–443. Springer, Heidelberg (2009)
33. Whitnall, C., Oswald, E.: A fair evaluation framework for comparing side-channel distinguishers. J. Cryptographic Eng. **1**(2), 145–160 (2011)