A theoretical study of Kolmogorov-Smirnov distinguishers: Side-channel analysis vs. differential cryptanalysis

Annelie Heuser, Olivier Rioul, Sylvain Guilley

A Theoretical Study of Kolmogorov-Smirnov Distinguishers

Side-Channel Analysis vs. Differential Cryptanalysis

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

[1] TELECOM-ParisTech, COMELEC, Paris, France
{heuser,rioul,guilley}@enst.fr
[2] Secure-IC S.A.S., Rennes, France

Abstract. In this paper, we carry out a detailed mathematical study of two theoretical distinguishers based on the Kolmogorov-Smirnov (KS) distance. This includes a proof of soundness and the derivation of *closed-form expressions*, which can be split into two factors: one depending only on the *noise* and the other on the *confusion coefficient* of Fei, Luo and Ding. This allows one to have a deeper understanding of the relative influences of the signal-to-noise ratio and the confusion coefficient on the distinguisher's performance. Moreover, one is able to directly compare distinguishers based on their closed-form expressions instead of using evaluation metric that might obscure the actual performance and favor one distinguisher over the other. Furthermore, we formalize the link between the confusion coefficient and differential cryptanalysis, which shows that the stronger an S-box is resistant to differential attacks the weaker it is against side-channel attacks, and *vice versa*.

Keywords: Side-channel distinguisher · Confusion coefficient · Kolmogorov-Smirnov analysis · Closed-form expressions · S-Box differential uniformity · Constrained S-Box search

1 Introduction

Side-channel attacks consist in exploiting leakages in order to extract secrets from any kind of cryptographic devices. Studies of side-channel distinguishers have been initially empirical: they were carried out on real traces, whose characteristics in terms of signal and noise were not exactly known. This allows to compare attacks on a fair setting especially their optimizations, like for instance using the DPA contests measurements [24]. Unfortunately, this does not allow one to understand the role of the different parameters at hand (like the signal-to-noise ratio (SNR) and the impact of the leakage model) and derive conclusions for any kind of data.

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

For this reason, another approach consists in generating traces by simulations, according to some archetype leakage signal and noise. The question that now arises is how to compare attacks. Guidelines were given by Standaert et al. in [22], and a formal evaluation framework was presented in [23]. Two metrics were introduced to quantify the efficiency of attacks: *success rate* and *guessing entropy*. In [10] Maghrebi et al. introduced *error bars* on the success rate in order to determine a reliable decision whether one distinguisher is better than another. Another strategy proposed by Whitnall and Oswald in [28] consists in computing various kinds of metrics evaluating theoretical distinguishers, such as the *relative distinguishing margin*. Yet another approach consists in deriving closed-form expressions of the theoretical success rate of distinguishers. Recently, Fei et al. [7] derived a closed-form expression of the theoretical success rate for DPA (difference of means). In order to achieve this they introduced the *confusion coefficient*, which determines the relationship between the sensitive variable of the correct key and any other key hypotheses. Thanks to this concept, Thillard et al. re-derived in [26] the computation of the success rate of CPA given by Rivain in [20] in terms of the confusion coefficient.

Our Contribution. In this paper, we conduct a mathematical study on the Kolmogorov-Smirnov (KS) distinguishers, namely KSA (KS Analysis) and iKSA (interclass KSA). Following the empirical results in [10], we investigate the standard Kolmogorov-Smirnov distinguisher (i.e., KSA), and the interclass KS distinguisher (i.e., iKSA) as it was shown that iKSA outperforms KSA in simulated data using the Hamming weight leakage model [10]. In particular, our study includes the derivation of closed-form expressions as well as a proof of soundness for both KS distinguishers, where we had to focus on the one-bit leakage scenario (as for DPA).

We show that the closed-form expressions of KSA and iKSA depend on two factors: one that is a function only of the noise and another one that is a function only of the confusion coefficient. A closed-form expression having also an independent noise factor has been observed for CPA (and thus also for DPA) by Mangard et al. in [11]. Remarkably, a re-formulation of the formula in [11] in terms of the confusion coefficient shows that the closed-forms of DPA and KSA/iKSA (in short (i)KSA) only differ in the factor of the noise. As a consequence we show that, in contrast to other distinguishers like mutual information, the relative distinguishing margin of one-bit (i)KSA and DPA does *not* depend on the noise, but only on the confusion coefficients. This behavior for DPA has partially also been observed in [28].

These results highlight the relevance of a theoretical study of distinguishers and the derivation of closed-form expressions, since one is able to exactly determine the impacts of the noise and of the choice of the leakage model (e.g. S-boxes). Moreover, this allows to compare distinguishers among themselves by means of closed-form expressions, instead of using evaluation metrics obscuring relevant factors.

Finally, assuming that the leakage model depends on a substitution box (S-box), we formalize the link between the confusion coefficient and differential cryptanalysis [1] through the cryptanalytic metric called *differential uniformity*. We demonstrate that the stronger the differential resistance, the weaker the side-channel resistance and *vice versa*. This was only implicitly known so far (e.g., results of Prouff in [18]). Furthermore, we show that this behavior is not a direct consequence of the *non-linearity* of the S-box, as it is commonly believed, but rather of its resistance against differential cryptanalysis.

2 Preliminaries

2.1 Notations

Calligraphic letters (e.g., $\mathcal{X}$) denote finite sets, capital letters (e.g., X) denote random variables taking values in these sets, and the corresponding lowercase letters (e.g., x) denote their realizations. We write $\mathbb{P}\{X = x\}$ or $p(x)$ for the probability that $X = x$ and $p(x|y) = \mathbb{P}\{X = x \,|\, Y = y\}$ for conditional probabilities. Let $k^\star$ denote the secret cryptographic key, k any possible key hypothesis from the keyspace $\mathcal{K}$, and let T be the input or cipher text of the cryptographic algorithm. The mapping $g : (\mathcal{T}, \mathcal{K}) \to \mathcal{I}$ maps the input or cipher text and a key hypothesis $k \in \mathcal{K}$ to an internally processed variable in some space $\mathcal{I}$ that is assumed to relate to the leakage X. Usually, $\mathcal{T}, \mathcal{K}, \mathcal{I}$ are taken as $\mathbb{F}_2^n$, where n is the number of bits (for AES $n = 8$).

Generally it is assumed that g is known to the attacker. A common consideration is $g(T, k) = \texttt{Sbox}[T \oplus k]$ where `Sbox` is a substitution box. The measured leakage X can then be written as

$$X = \psi(g(T, k^\star)) + N, \tag{1}$$

where N denotes an independent additive noise. The device-specific deterministic function ψ is normally unknown to the attacker, which for this reason is assuming some other function ψ' modeling an exploitable part of ψ. For any key guess $k \in \mathcal{K}$ the attacker computes the *sensitive variable*

$$Y(k) = \psi'(g(T, k)). \tag{2}$$

Without loss of generality we may assume that Y is centered and normalized, i.e., $\mathbb{E}\{Y\} = 0$ and $Var\{Y\} = 1$, and that the values in $\mathcal{Y}$ are regularly spaced with step Δy. For ease of notation, we let $Y^\star = Y(k^\star)$ and $Y = Y(k)$.

2.2 Conditions

First, we assume a basic condition that when looking directly at the leakage distribution (not knowing the message or cipher) we cannot infer any secret.

Condition 1 (Secrecy condition). *The probability distribution of the leakage (see Eq. (1)) does not depend on the actual value of the secret key.*

In other words, the $Y(k)$'s are identically distributed (i.d.) for all $k \in \mathcal{K}$. Second, similarly (but not equivalently) as in [19,30] we require the following condition on the relationship between $Y^\star$ and Y to be able to distinguish between different keys $k \in \mathcal{K}$. This confusion condition will be related to the confusion coefficient later in Proposition 4.

Condition 2 (Confusion condition). *For any $k \neq k^\star$, the correspondence from $Y(k)$ to $Y(k^\star)$ is non-injective, i.e., there does* not *exist an injective (that is one-to-one) function $\xi : \mathcal{Y} \to \mathcal{Y}$ such that $Y(k^\star) = \xi\big(Y(k)\big)$ with probability one.*

Lemma 1. *The confusion condition is equivalent to the condition that for all $k \neq k^\star$ there exist $y, y^\star \in \mathcal{Y}$ such that*

$$p(y^\star|y) \text{ is neither } 0 \text{ nor } 1. \tag{3}$$

Proof. Negating the confusion condition, there is a $k \neq k^\star$ such that $\mathbb{P}\big\{Y(k^\star) = \xi(Y(k))\big\} = 1$ where ξ is some one-to-one function. This is equivalent to $\mathbb{P}\big\{Y(k^\star) = \xi(y) \,\big|\, Y(k) = y\big\} = 1$ for all $y \in \mathcal{Y}$, that is, $p(y^\star|y) = 1$ when $y^\star = \xi(y)$ and $p(y^\star|y) = 0$ otherwise. □

Thus, the confusion condition amounts to saying that knowing $Y(k) = y$ (for that particular value y satisfying the condition) does not always permit to conclude for sure about the value of $Y(k^\star)$, which depends on the secret: there is still a nonzero probability that $Y(k^\star)$ has several possible values.

2.3 Multi-bit vs One-bit Leakage Models

The existing literature on KS distinguishers [10,27,29,31] deals with multi-bit leakage models. However, a precise mathematical derivation is very much intricate in the multi-bit case. We therefore present hereafter the scenario where the sensitive variable Y is a binary variable, i.e., $\psi' : \mathcal{I} \to \mathbb{F}_2$.

Note that, we do not make the same restrictions on ψ, for example, let us consider the most common cases for ψ in practice, that have also been investigated in [28]: the Hamming weight (HW) or more generally the (unequal) weighted sum of n bits:

$$X = \sum_{i=1}^{n} \omega_i [g(T, k^\star)]_i + N, \tag{4}$$

with $[\cdot]_i : \mathbb{F}_2^n \to \mathbb{F}_2$ being the projection onto the i^{th} bit, $\omega_i \in \mathbb{R}$ and in case of a HW leakage $\omega_1 = \omega_2 = \ldots = \omega_n = 1$.

Let us assume in the following that $[g(T, k^\star)]_1, \ldots, [g(T, k^\star)]_n$ are independent and uniformly distributed, which is implied when considering a bijective S-box as for example in AES and randomly chosen plaintexts T. Consider that we concentrate on bit $b \in \{1, \ldots, n\}$, so $\psi'(\cdot) = [\cdot]_b$, then we express X in terms of the sensitive variable $Y^\star = [g(T, k^\star)]_b$ as

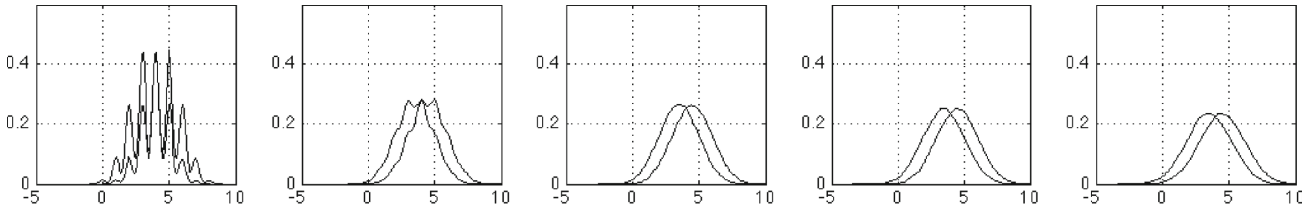
$$X = \omega_b Y^\star + \underbrace{Z + N}_{N'} \quad \text{with} \quad Z = \sum_{i \neq b} \omega_i [g(T, k^\star)]_i. \tag{5}$$

Remark 1. Note that, when ψ is the HW function ($\omega_i = 1$) Z follows a binomial law of length $n-1$ and probability $p = \frac{1}{2}$.

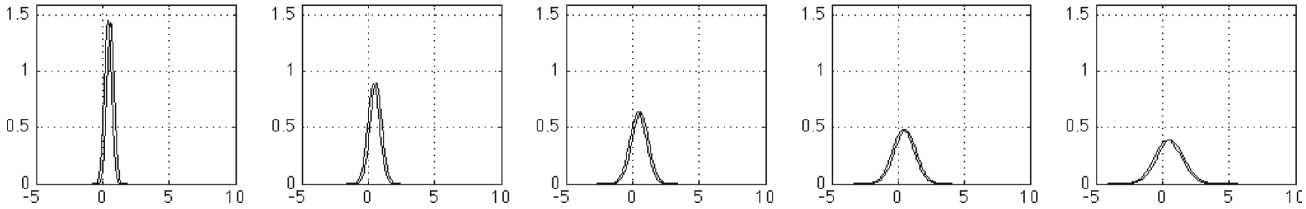
In our further analysis, we assume that $N' = Z + N$ is unimodal distributed in the sense of the following definition:

Definition 1 (Unimodal distribution). *A distribution f is called* unimodal *if there exists a mode m such that $f(x)$ is increasing for $x \leq m$ and decreasing for $x \geq m$.*

To verify this assumption empirically, we perform simulations with $N \sim \mathcal{N}(0, \sigma^2)$ for several σ^2, 10000 realisations, and $g(T, k^\star) = \texttt{Sbox}[T \oplus k^\star]$ being the result of the AES S-box (`SubBytes`) operation. Figure 1 shows the conditional distributions of $\{X|Y^\star = y_0\}$ and $\{X|Y^\star = y_1\}$ for (a) the HW model and (b) using weights ω. One can see in Fig. 1(a) that for $\sigma^2 = 0.04$, N' is clearly *not* unimodal distributed[1] , but when $\sigma^2 \geq 0.36$ the unimodality holds. Figure 1(b) illustrates that N' is unimodal distributed for all tested σ^2's. Of course, the bigger σ^2 the closer the distribution of N' will be to N. Note that, observing $\sigma^2 < 1$ is very unrealistic in practice. Moreover, when using an ATMega 163 microcontroller as used in the DPA contest v4 [25], where the signal-to-noise ratio is very high (it is *not* a security product), the condition of unimodality is fulfilled (see Fig. 2), which has also been illustrated for measurements of a microcontroller in [11] (Fig. 4.6). In the rest of the paper, to simplify the notations, we will simply denote by $N \sim \mathcal{N}(0, \sigma^2)$ the noise (sum of *algorithmic* and *measurement* noises).



(a) $\forall i\ \omega_i = 1$



(b) $\omega = [0.05, 0.2, 0.1, 0.15, 0.05, 0.05, 0.3, 0.1]$ and $b = 4$

Fig. 1. Estimated conditional distributions $\{X|Y^\star = y_0\}$ and $\{X|Y^\star = y_1\}$ using a noise level of $\sigma^2 = \{0.04, 0.16, 0.36, 0.64, 1\}$.

[1] This visual interpretation agrees with several statistical unimodality tests.

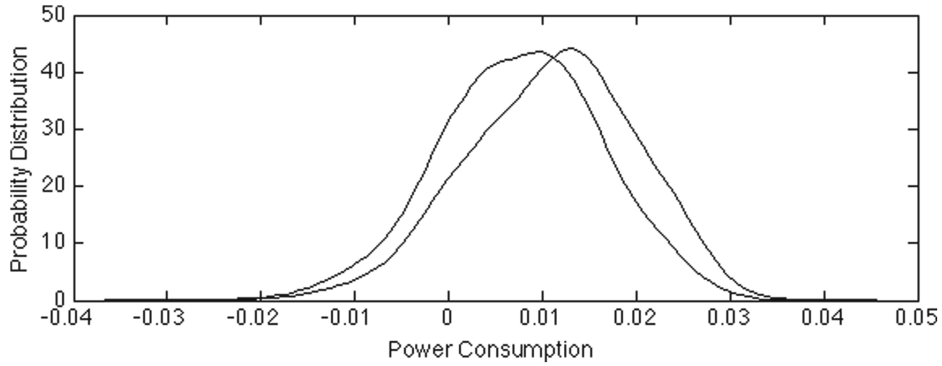


Fig. 2. Estimated conditional leakage distributions $\{X|Y^\star = y_0\}$ and $\{X|Y^\star = y_1\}$ of measurements from ATMega 163, 2nd AES S-box, 4^{th} bit.

3 Study of Theoretical KS Distinguishers

3.1 A Note on DPA/CPA

In [11] Mangard et al. showed that the theoretical CPA can be expressed as

$$\rho(X, Y) = \frac{\rho(Y^\star, Y)}{\sqrt{1 + \frac{1}{SNR}}} \quad , \tag{6}$$

where ρ is the *absolute value* of the Pearson correlation coefficient. Thus, $\rho(X, Y)$ can be factored into one part only depending on the leakage model and one depending on the SNR. Note that, CPA using one-bit models is equivalent to DPA [6] (when assuming normalized Y's), thus Eq. (6) also holds for DPA. The next proposition shows that in fact the part depending on the leakage model can be directly expressed in terms of the confusion coefficient [7], which describes the relationship between $Y(k^\star)$ and any $Y(k)$ with $k \in \mathcal{K}$ that is defined as follows.

Definition 2 (Confusion coefficient [7]). *Let $k^\star$ denote the correct key and k any key hypothesis in $\mathcal{K}$, then the* confusion coefficient *is defined as*

$$\kappa(k^\star, k) = \mathbb{P}\{Y(k^\star) \neq Y(k)\}. \tag{7}$$

Proposition 1. *For binary and normalized equiprobable Y's*

$$\rho(X, Y) = \frac{|1 - 2\kappa(k^\star, k)|}{\sqrt{1 + \frac{1}{SNR}}} = d \cdot \left|\kappa(k^\star, k) - \frac{1}{2}\right| \quad , \tag{8}$$

with $d = \frac{2}{\sqrt{1+1/SNR}}$.

Proof. As Y is normalized (i.e., $\mathbb{E}(Y) = 0$ and $Var(Y) = 1$) we re-formulate

$$\rho(Y^\star, Y) = \frac{|Cov(Y^\star, Y)|}{\sqrt{Var(Y^\star)Var(Y)}} \tag{9}$$

$$= |1 - 2\kappa(k^\star, k)|, \tag{10}$$

since $Cov(Y^\star, Y) = \mathbb{E}\{Y^\star \cdot Y\} = 1 - 2\mathbb{P}\{Y(k^\star) \neq Y(k)\} = 1 - 2\kappa(k^\star, k)$. □

3.2 KS Side-Channel Distinguishers

In this subsection we briefly sketch KS distinguishers named after Kolmogorov and Smirnov [9,21]. For more detailed information on their use in the area of side-channel analysis we refer to [27,29] for an evaluation of KS and to [10] for the comparison between KSA and iKSA, which shows that the estimated iKSA is superior to the estimated KSA using simulations for a HW leakage model.

Definition 3 (KS distinguishers). *The (standard)* Kolmogorov-Smirnov distinguisher *[27] is defined by*

$$\mathsf{KSA}(k) = \mathsf{D}_{\mathsf{KSA}}(X, Y) = \mathbb{E}_Y\big\{\|F(x|Y) - F(x)\|_\infty\big\}, \tag{11}$$

where the expectation is taken over Y's distribution, $\|\cdot\|_\infty$ is the L^∞ norm: $\|\Psi(x)\|_\infty = \sup_{x\in\mathbb{R}} |\Psi(x)|$, and $F(x) = F_X(x)$, $F(x|y) = F_{X|Y=y}(x)$ denote the cumulative distribution functions of X and X given $Y(k) = y$, respectively.

The inter-class Kolmogorov-Smirnov distinguisher *[10] is defined by*

$$\mathsf{iKSA}(k) = \mathsf{D}_{\mathsf{iKSA}}(X, Y(k)) = \frac{1}{2}\mathbb{E}_{Y,Y'}\big\{\|F(x|Y) - F(x|Y')\|_\infty\big\}, \tag{12}$$

where Y' is an independent copy of Y, and the expectation is taken over the joint distribution of Y and Y'. The $1/2$ factor makes up for double counts ($(Y, Y') \leftrightarrow (Y', Y)$).

We need the following lemma.

Lemma 2. *With the above notations and assumptions on the leakage model,*

$$\mathsf{KSA}(k) = \sum_{y\in\mathcal{Y}} p(y) \sup_{x\in\mathbb{R}} \Big| \sum_{y^\star\in\mathcal{Y}} \big(p(y^\star|y) - p(y^\star)\big) \cdot \Phi\Big(\frac{x - y^\star}{\sigma}\Big)\Big| \quad \textit{and} \tag{13}$$

$$\mathsf{iKSA}(k) = \frac{1}{2} \sum_{\substack{y,y'\in\mathcal{Y}\\ y\neq y'}} p(y)p(y') \sup_{x\in\mathbb{R}} \Big| \sum_{y^\star\in\mathcal{Y}} \big(p(y^\star|y) - p(y^\star|y')\big) \cdot \Phi\Big(\frac{x - y^\star}{\sigma}\Big)\Big|, \tag{14}$$

where $\Phi(x)$ is the c.d.f. of the standard noise N/σ (of zero *mean and* unit *variance).*

Proof. From model Eq. (1), X given $Y(k^\star) = y^\star$ has c.d.f.

$$\mathbb{P}\big\{X \le x \,\big|\, Y(k^\star) = y^\star\big\} = \Phi_N(x - y^\star) = \Phi\Big(\frac{x - y^\star}{\sigma}\Big), \tag{15}$$

where $\Phi_N(\nu) = \mathbb{P}\{N \le \nu\} = \Phi(\nu/\sigma)$ is the c.d.f. of the noise N. Indeed, we recall our notation: $X = Y(k^\star) + N$. Averaging over $Y(k^\star)$ gives

$$F(x) = \mathbb{P}\big\{X \le x\big\} = \sum_{y^\star\in\mathcal{Y}} p(y^\star)\Phi\Big(\frac{x - y^\star}{\sigma}\Big). \tag{16}$$

Now from Eq. (15) and the formula of total probability, X given $Y(k) = y$ is distributed according to the c.d.f.

$$F(x|y) = \mathbb{P}\{X \leq x \,|\, Y(k) = y\} \tag{17}$$

$$= \sum_{y^\star \in \mathcal{Y}} p(y^\star|y) \cdot \mathbb{P}\{X \leq x \,|\, Y(k^\star) = y^\star, Y(k) = y\} \tag{18}$$

$$= \sum_{y^\star \in \mathcal{Y}} p(y^\star|y) \cdot \mathbb{P}\{X \leq x \,|\, Y(k^\star) = y^\star\} \tag{19}$$

$$= \sum_{y^\star \in \mathcal{Y}} p(y^\star|y) \cdot \Phi\Big(\frac{x - y^\star}{\sigma}\Big). \tag{20}$$

Plugging Eq. (16) and Eq. (20) into Eq. (11) gives Eq. (13); plugging Eq. (20) into Eq. (12) gives Eq. (14) where it should be noted that the terms for which $y = y'$ vanish. □

Remark 2. When the noise is assumed Gaussian, Eq. (20) is the equivalent of the well-known "mixture of Gaussian" as studied in [19].

3.3 Noise Factorization

In the following we consider the scenario highlighted in Subsect. 2.3 where Y is binary and the noise follows a unimodal distribution. The next proposition shows that both KS distinguishers can be factorized as a product of one factor depending only on the noise distribution and another depending only on the sensitive variables, which has also been observed for DPA in [11] (see Subsect. 3.1), but not for any other distinguisher so far.

Proposition 2 (Noise factorization). *One has*

$$\mathsf{KSA}(k) = c \sum_{y \in \mathcal{Y}} p(y) \big| p(y^\star|y) - p(y^\star) \big| \tag{21}$$

$$\mathsf{iKSA}(k) = \frac{c}{2} \sum_{\substack{y, y' \in \mathcal{Y} \\ y \neq y'}} p(y)p(y') \big| p(y^\star|y) - p(y^\star|y') \big| \ , \tag{22}$$

where $y^\star$ denotes any of the two possible values in $\mathcal{Y}$ and where

$$c = 2\,\Phi\Big(\frac{\Delta y}{2\sigma}\Big) - 1 > 0 \ . \tag{23}$$

Proof. Since $\sum_{y^\star \in \mathcal{Y}} \big(p(y^\star|y) - p(y^\star)\big) = 1 - 1 = 0$, the two coefficients in the inner sum of Eq. (13) are opposite equal. Similarly $\sum_{y^\star} \big(p(y^\star|y) - p(y^\star|y')\big) = 1 - 1 = 0$ and the two coefficients in the inner sum of Eq. (14) are opposite equal. It follows that Eq. (21) and Eq. (22) hold with

$$c = \sup_{x \in \mathbb{R}} \Big| \Phi\Big(\frac{x - y^\star}{\sigma}\Big) - \Phi\Big(\frac{x - \widetilde{y^\star}}{\sigma}\Big) \Big| \ , \tag{24}$$

where $y^\star$ denotes any of the two possible values in $\mathcal{Y}$ and $\widetilde{y^\star}$ denotes the other one. The conclusion now follows from the following lemma. □

Lemma 3. *Let $\Phi(x)$ be the c.d.f. of random variable N/σ having even and unimodal distribution of unit variance. Then for every $y^\star \neq \widetilde{y^\star}$ with $\Delta y = |\widetilde{y^\star} - y^\star|$,*

$$\sup_{x\in\mathbb{R}} \left| \Phi\left(\frac{x-y^\star}{\sigma}\right) - \Phi\left(\frac{x-\widetilde{y^\star}}{\sigma}\right) \right| = 2\Phi\left(\frac{\Delta y}{2\sigma}\right) - 1. \tag{25}$$

Proof. Assume, without loss of generality, that $y^\star < \widetilde{y^\star}$ so that $\Delta y = \widetilde{y^\star} - y^\star$. Since Φ is continuous and nondecreasing, the above supremum is the maximum of $\Phi\left(\frac{x-y^\star}{\sigma}\right) - \Phi\left(\frac{x-\widetilde{y^\star}}{\sigma}\right)$. Since N has even and unimodal density f, the derivative of the latter expression is $f(x-y^\star) - f(x-\widetilde{y^\star})$ which is $= 0$ when $x = \frac{y^\star+\widetilde{y^\star}}{2}$ because f is even, and which is > 0 when $|x-y^\star| < |x-\widetilde{y^\star}|$ and < 0 when $|x-y^\star| > |x-\widetilde{y^\star}|$ because f is unimodal. It follows that the maximum is unique and attained when $x = \frac{y^\star+\widetilde{y^\star}}{2}$. Therefore, the desired maximum equals $\Phi\left(\frac{\widetilde{y^\star}-y^\star}{2\sigma}\right) - \Phi\left(\frac{y^\star-\widetilde{y^\star}}{2\sigma}\right) = \Phi\left(\frac{\Delta y}{2\sigma}\right) - \Phi\left(-\frac{\Delta y}{2\sigma}\right) = 2\Phi\left(\frac{\Delta y}{2\sigma}\right) - 1$. The latter equality holds since f being even, one has $\Phi(-x) = 1 - \Phi(x)$. □

As we shall see, due to this noise factorization, also KS distinguishers are very appealing theoretical objects for formal studies. The quantity $\frac{\Delta y}{2\sigma}$ receives a simple interpretation: since $\mathbb{E}\{Y(k)^2\} = (\Delta y/2)^2$, the square of $\frac{\Delta y}{2\sigma}$ is simply the leakage signal-to-noise ratio (SNR) and we can write $c = 2\Phi\left(\sqrt{\mathrm{SNR}}\right) - 1$. For Gaussian noise[2], this reduces to

$$c = \mathrm{erf}\left(\sqrt{\mathrm{SNR}/2}\right), \tag{26}$$

where $\mathrm{erf} : x \mapsto \frac{2}{\sqrt{\pi}} \int_{-\infty}^{x} \exp\left(-t^2\right) \mathrm{d}t$ is the standard error function.

3.4 Proof of Soundness

Definition 4 (Soundness). *An attack based on maximizing the values of the distinguisher $\mathsf{D}(X, Y(k))$ over k is* sound *if*

$$\mathsf{D}(X, Y(k^\star)) > \mathsf{D}(X, Y(k)) \qquad (\forall k \neq k^\star). \tag{27}$$

Several theoretical distinguishers have already been proven sound: DPA, CPA, MIA [14,19]. For KSA and iKSA the soundness conditions read

$$\mathsf{KSA}(k^\star) > \mathsf{KSA}(k) \qquad (\forall k \neq k^\star) \tag{28}$$

$$\mathsf{iKSA}(k^\star) > \mathsf{iKSA}(k) \qquad (\forall k \neq k^\star), \tag{29}$$

respectively. Recall that we assume the secrecy condition (Subsect. 2.2) which amounts to saying that the $Y(k)$'s are identically distributed (i.d.).

[2] This assumption holds for sufficiently large values of σ^2 as discussed in Subsect. 2.3, which reflects a practical scenario as illustrated e.g. in Fig. 4.6 of [11].

Proposition 3 (Soundness, i.d. case). *For binary and i.d. $Y(k)$'s, the* KSA *and* iKSA *are sound if and only if the confusion condition holds.*

Proof. Since the $Y(k)$'s are i.d., $p(y)$ does not depend on k. Let $y \neq y'$ be elements of $\mathcal{Y}$. The confusion condition Eq. (3) is equivalent to the strict inequality

$$|p(y^\star|y) - p(y^\star|y')| < 1 \qquad (\forall k \neq k^\star). \tag{30}$$

Now for $k = k^\star$, $p(y^\star|y)$ is 0 or 1 depending on whether $y = y^\star$ or $y \neq y^\star$, and therefore $|p(y^\star|y) - p(y^\star|y')| = 1$. From Eq. (22) it follows upon multiplying $|p(y^\star|y) - p(y^\star|y')|$ by $p(y)p(y')$ and summing that Eq. (30) is equivalent to Eq. (29), i.e. the soundness of iKSA.

Proving that the KSA is sound is more intricate. Again let $y \neq y'$ be elements of $\mathcal{Y}$. One has $p(y^\star) = p(y)p(y^\star|y) + p(y')p(y^\star|y')$ where $p(y) + p(y') = 1$. It follows that $p(y^\star)$ lies between $p(y^\star|y)$ and $p(y^\star|y')$. Suppose without loss of generality that $p(y^\star|y) \leq p(y^\star) \leq p(y^\star|y')$.

The confusion condition of Eq. (3) states that for any $k \neq k^\star$, one has either

$$|p(y^\star|y) - p(y^\star)| < p(y^\star) \quad \text{or} \quad |p(y^\star|y') - p(y^\star)| < 1 - p(y^\star). \tag{31}$$

the corresponding non-strict inequalities being always satisfied. It follows from Eq. (21) that this is equivalent to the single strict inequality $\mathsf{KSA}(k) < c \cdot \big(p(y)p(y^\star) + p(y')(1 - p(y^\star))\big) = c \cdot \big(p(y)p(y^\star) + (1 - p(y))(1 - p(y^\star))\big) = 2c \cdot p(y)p(y^\star)$. Since the expression for $\mathsf{KSA}(k)$ does not depend on the particular value of $y^\star$, the latter upper bound should not either. There are two possibilities:

1. either $y \neq y^\star$ and $\mathsf{KSA}(k) < 2c \cdot (1 - p(y^\star))p(y^\star)$,
2. or $y = y^\star$ and $\mathsf{KSA}(k)$ should be both $< 2c \cdot p(y^\star)^2$ and $< 2c \cdot (1 - p(y^\star))^2$. But since $\min(a, b) \leq \sqrt{ab}$ we obtain $\mathsf{KSA}(k) < 2c \cdot (1 - p(y^\star))p(y^\star)$ in both cases.

Now for $k = k^\star$, equalities hold: $|p(y^\star|y') - p(y^\star)| = 1 - p(y^\star)$ and $|p(y^\star|y) - p(y^\star)| = p(y^\star)$ (since, necessarily, $y \neq y^\star$ and $y' = y^\star$); hence $\mathsf{KSA}(k^\star) = 2c \cdot (1 - p(y^\star))p(y^\star)$. This shows that Eq. (31) is equivalent to Eq. (28). □

As a consequence, provided that the conditions on the sensitive variable in Subsect. 2.2 and 2.3 are met, KSA and iKSA are able to reveal the secret key with arbitrarily high probability as the number of measurements increases indefinitely.

3.5 Simple Closed-Form Expression

In this subsection, we study KSA and iKSA under the assumption introduced by Fei et al. in Theorem 1 of [7], which states that for a *perfectly secret encryption algorithm*, each sensitive variable is equiprobable, i.e., $p(y) = p(y^\star) = 1/2$. This requirement is stronger than our *secrecy condition* (Condition 1). Remarkably, the following proposition shows that the closed-form expressions for DPA and (i)KSA only differ in the part of the noise.

Proposition 4. *For binary and equiprobable Y's, the confusion condition in Eq. (3) reduces to the condition that*

$$\kappa(k^\star, k) \quad \text{is neither } 0 \text{ nor } 1 \qquad (\forall k \neq k^\star). \tag{32}$$

Also KSA *and* iKSA *are completely equivalent in this case, with the following closed-form expression*

$$\mathsf{KSA}(k) = 2\,\mathsf{iKSA}(k) = c \cdot \left|\kappa(k^\star, k) - \tfrac{1}{2}\right|. \tag{33}$$

Proof. Since the $Y(k)$'s are binary equiprobable, the joint distribution $\mathbb{P}\{Y(k^\star) = y^\star, Y(k) = y\}$ should be symmetric in $(y^\star, y)$ and, therefore,

$$\begin{aligned} p(y^\star|y) &= \mathbb{P}\{Y(k^\star) = y^\star \big| Y(k) = y\} \\ &= 2\mathbb{P}\{Y(k^\star) = y^\star, Y(k) = y\} \\ &= \begin{cases} \kappa(k^\star, k) & \text{if } y \neq y^\star, \\ 1 - \kappa(k^\star, k) & \text{if } y = y^\star. \end{cases} \end{aligned}$$

This proves Eq. (32). Also, $|p(y^\star|y) - p(y^\star)| = |p(y^\star|y) - 1/2| = |\kappa(k^\star, k) - 1/2|$ and if $y \neq y'$ (whence $y = y^\star$ or $y' = y^\star$), one finds $|p(y^\star|y) - p(y^\star|y')| = |2\kappa(k^\star, k) - 1|$. Plugging these expressions into Eq. (21) and Eq. (22) gives Eq. (33). □

Remark 3. Using these simple closed-form expressions it is straightforward to recover in the equiprobable case that KSA and iKSA are sound (Proposition 3): Since $\kappa(k^\star) = 0$, the confusion condition Eq. (32) is equivalent to $|\kappa(k^\star, k) - 1/2| < 1/2 = |\kappa(k^\star, k^\star) - 1/2|$ for any $k \neq k^\star$. From Eq. (33), this in turn is equivalent to Eq. (28) or Eq. (29).

Even though KSA and iKSA become equivalent if one insists on having equiprobable bits (in $\mathcal{Y}$), shows the next proposition states that KSA and iKSA are not strictly equivalent in general.

Proposition 5. *For binary $Y(k)$'s,* KSA *and* iKSA *are* not *equivalent unless the $Y(k)$'s are equiprobable (i.e. the secrecy condition holds).*

Proof. If $y \neq y'$ belong to $\mathcal{Y}$ one has $p(y^\star) = p(y)p(y^\star|y) + p(y')p(y^\star|y')$ where $p(y)+p(y') = 1$. It follows that $p(y^\star)$ lies between $p(y^\star|y)$ and $p(y^\star|y')$. Therefore, $\big|p(y^\star|y) - p(y^\star|y')\big| = \big|p(y^\star|y) - p(y^\star)\big| + \big|p(y^\star) - p(y^\star|y')\big|$ and

$$\sum_{y \neq y'} p(y)p(y')\big|p(y^\star|y) - p(y^\star|y')\big| = 2\sum_{y} p(y)(1 - p(y))\big|p(y^\star|y) - p(y^\star)\big| \tag{34}$$

so that

$$\mathsf{iKSA} = c\sum_{y} p(y)(1 - p(y))\big|p(y^\star|y) - p(y^\star)\big|. \tag{35}$$

The equivalence between KSA (Eq. (21)) and iKSA (Eq. (35)) holds only if $p(y)$ and $p(y)(1-p(y))$ are proportional, which is equivalent to the requirement that $p(y)$ is constant, i.e., the $Y(k)$'s are equiprobable. □

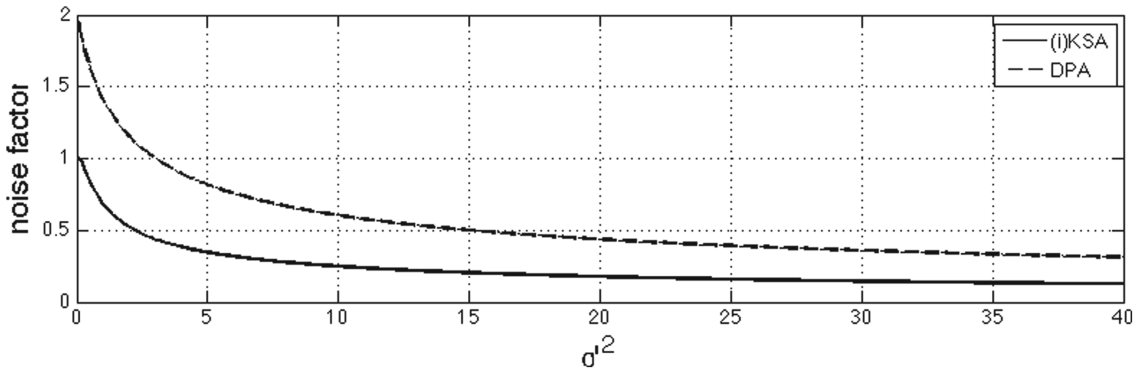


Fig. 3. Noise factor plotted as a function of σ^2.

3.6 Discussion about the Closed-Forms of DPA and (i)KSA

Note that the equality of the term related to the confusion coefficient in the closed-form expression of DPA and (i)KSA was not obvious before, since DPA distinguishes on a *proportional scale* whereas (i)KSA relies on a *nominal scale* as illustrated in [30]. It can be interpreted as follows: DPA and (i)KSA exploit equivalently the S-Box to discriminate between the correct and the incorrect key guesses.

Figure 3 illustrates the noise factor c of (i)KSA and the noise factor d of DPA as a function of σ^2 where $\mathrm{SNR} = \frac{1}{\sigma^2}$. One can see that both factors c and d tend to zero as the noise increases (SNR decreases). However, as c (resp. d) is simply a multiplicative coefficient that applies both to the distinguishers value for the correct and the incorrect key guesses, we can conclude that DPA (resp. (i)KSA) distinguishes hypotheses on the key identically, irrespective of the SNR.

4 Confusion Coefficient Versus Cryptanalytical Metrics

Now we explicitly assume that the sensitive variable Y depends on an S-box through an equation of the form $Y(k) = S(T \oplus k)$, where S is a $\mathbb{F}_2^n \to \mathbb{F}_2$ Boolean function[3], and $\mathbb{F}_2 = \{0, 1\}$ is the two-element Galois field.

4.1 Relationship between $\kappa(k^\star, k)$ and Differential Metrics

Lemma 4. *The confusion coefficient $\kappa(k^\star, k)$ can be written in terms of the Boolean function S by the following well-known quantity in Boolean functions:*

$$\frac{1}{2} - \kappa(k^\star, k) = \frac{1}{2^{n+1}} \sum_{y \in \mathbb{F}_2^n} (-1)^{S(y) \oplus S(y \oplus (k^\star \oplus k))} \in [-\tfrac{1}{2}, \tfrac{1}{2}]. \tag{36}$$

[3] This Boolean function S is typically *one component* of a substitution box with n output bits. Of course, an attacker could predict the n bits altogether. Still, a mono-bit model has the interest that it reduces the *epistemic noise*, meaning that an assumption on more than one bit certainly deviates from the actual leakage.

Proof. Using the customary interpretation of Booleans $b \in \mathbb{F}_2$ as integers: $b = \frac{1}{2}(1-(-1)^b) \in \mathbb{Z}$, one has

$$\begin{aligned}\kappa(k^\star,k) &= \mathbb{P}\{Y(k) \neq Y(k^\star)\} = \mathbb{E}\{Y(k) \oplus Y(k^\star)\} \\ &= \frac{1}{2^n}\sum_{y\in\mathbb{F}_2^n} S(y\oplus k^\star)\oplus S(y\oplus k) \\ &= \frac{1}{2^n}\sum_{y}\frac{1}{2}\left(1-(-1)^{S(y\oplus k^\star)\oplus S(y\oplus k)}\right) \\ &= \frac{1}{2} - \frac{1}{2^{n+1}}\sum_{y}(-1)^{S(y)\oplus S(y\oplus(k^\star\oplus k))} \quad . \end{aligned}$$

□

S-Boxes are characterized in cryptanalysis by two metrics called *linear* and *differential uniformity* [5,8].

Definition 5 (Linear and differential uniformity). *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be an S-Box. The linear (Λ_S) and differential (Δ_S) uniformities of S are defined as:*

$$\Lambda_S = \max_{a\in\mathbb{F}_2^n,\ k\in\mathbb{F}_2^{m*}} \left|\#\{x\in\mathbb{F}_2^n/(a\cdot x)\oplus(k\cdot S(x))=0\} - 2^{n-1}\right| \quad , \tag{37}$$

$$\Delta_S = \max_{a\in\mathbb{F}_2^m,\ k\in\mathbb{F}_2^{n*}} \#\{x\in\mathbb{F}_2^n/S(x)\oplus S(x\oplus k)=a\} \quad . \tag{38}$$

The smaller Λ_S and Δ_S, the better the S-Box from a cryptanalytical point of view, respectively against linear [12] and differential [1] cryptanalysis. Note that, in our case $m = 1$ since we restrict ourselves to one-bit of the S-Box output.

Remark 4. Note that *linear uniformity* is related to *nonlinearity*, a well-known notion in the field of vectorial Boolean functions [4]. The nonlinearity of a Boolean function S is defined as $nl(S) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\left|\widehat{(-1)^S}(a)\right|$, where $\widehat{f}(a) = \sum_z f(x)(-1)^{a\cdot z}$ is the Fourier transform of f. Again using the customary interpretation of Booleans as integers, $\Lambda_S = \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\left|\sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x\oplus S(x)}\right| = 2^{n-1} - nl(S)$. Obviously, the smaller Λ_S, the greater the nonlinearity.

Note that from Eq. (38) one has $2^{n-1} \leq \Delta_S \leq 2^n$ and therefore $0 \leq 2^{-n}\Delta_S - \frac{1}{2} \leq \frac{1}{2}$. Also recall that the confusion coefficient $\kappa(k^\star,k)$ reaches its minimal value $\kappa(k^\star,k^\star) = 0$ for $k = k^\star$, and reaches its maximal value $\kappa(k^\star,k) = 1$ if and only if there exists a key $k \neq k^\star$ such that for all $x \in \mathbb{F}_2^n$, $S(x\oplus k) = \overline{S(x\oplus k^\star)}$. We have the following relationship between Δ_S and $\kappa(k^\star,k)$:

Proposition 6 (Relationship between the differential uniformity and the confusion coefficient). *When considering a Boolean function $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ with $m = 1$, then*

$$2^{-n}\Delta_S - \frac{1}{2} = \max_{k\neq k^\star}\left|\kappa(k^\star,k) - \frac{1}{2}\right| . \tag{39}$$

Proof. From Lemma 4,

$$\#\{x \in \mathbb{F}_2^n / S(x) \oplus S(x \oplus k \oplus k^\star) = 1\} = \sum_{y \in \mathbb{F}_2^n} S(y \oplus k^\star) \oplus S(y \oplus k) = 2^n \kappa(k^\star, k)$$

and similarly $\#\{x \in \mathbb{F}_2^n / S(x) \oplus S(x \oplus k \oplus k^\star) = 0\} = 2^n - 2^n \kappa(k^\star, k)$. It follows from Eq. (38) that

$$\begin{aligned}
\Delta_S &= \max_{a \in \mathbb{F}_2,\ k \in \mathbb{F}_2^{n*}} \#\{x \in \mathbb{F}_2^n / S(x) \oplus S(x \oplus k) = a\} \\
&= \max \left\{ \begin{array}{l} \max_{k \in \mathbb{F}_2^{n*}} \#\{x \in \mathbb{F}_2^n / S(x) \oplus S(x \oplus k) = 0\}, \\ \max_{k \in \mathbb{F}_2^{n*}} \#\{x \in \mathbb{F}_2^n / S(x) \oplus S(x \oplus k) = 1\} \end{array} \right\} \\
&= \max \left\{ \begin{array}{l} \max_{k \in \mathbb{F}_2^{n*}} 2^n - \#\{x \in \mathbb{F}_2^n / S(x) \oplus S(x \oplus k) = 1\}, \\ \max_{k \in \mathbb{F}_2^{n*}} \#\{x \in \mathbb{F}_2^n / S(x) \oplus S(x \oplus k) = 1\} \end{array} \right\} \\
&= \max \left\{ \max_{k \neq k^\star} 2^n (1 - \kappa(k^\star, k)), \max_{k \neq k^\star} 2^n \kappa(k^\star, k) \right\} \\
&= 2^n \left(\frac{1}{2} + \max \left\{ \max_{k \neq k^\star} \frac{1}{2} - \kappa(k^\star, k), \max_{k \neq k^\star} \kappa(k^\star, k) - \frac{1}{2} \right\} \right) \\
&= 2^n \left(\frac{1}{2} + \max_{k \neq k^\star} \left| \kappa(k^\star, k) - \frac{1}{2} \right| \right), \qquad (40)
\end{aligned}$$

which proves the proposition. □

Therefore, minimizing Δ_S amounts in minimizing the distance between $\kappa(k^\star, k)$ for $k \neq k^\star$ and the factor $\frac{1}{2}$.

Remark 5. There is no direct link between the *linear uniformity* (Eq. (37)) and the confusion coefficient $\kappa(k^\star, k)$.

4.2 Relationship to Closed-Form Expressions

We now relate Eq. (40) to the derived closed-form expression of (i)KSA (see Eq. (33)) and DPA (see Eq. (8)). Let $\mathsf{D}(k^\star)$ be the distinguishing value of the correct key and $\mathsf{D}(k)$ be the distinguishing value of any incorrect key hypotheses. We consider two metrics, an *extensive* and a *relative* one, which provide us with a theoretical evaluation of the distinguishing power of a distinguisher.

Definition 6 (Distinguishing margin). *The* distinguishing margin $\mathrm{DM}(\mathsf{D})$ *is the minimal distance between the distinguisher for the correct key and all incorrect keys. Formally,*

$$\mathrm{DM}(\mathsf{D}) = \mathsf{D}(k^\star) - \max_{k \neq k^\star} \mathsf{D}(k). \qquad (41)$$

The following definition introduces a normalizing denominator:

Definition 7 (Relative distinguishing margin [28]). *The* relative distinguishing margin $\mathrm{RDM}(\mathsf{D})$ *is defined as*

$$\mathrm{RDM}(\mathsf{D}) = \frac{\mathsf{D}(k^\star) - \max_{k \neq k^\star} \mathsf{D}(k)}{\sqrt{Var\{\mathsf{D}(K)\}}} = \min_{k \neq k^\star} \frac{\mathsf{D}(k^\star) - \mathsf{D}(k)}{\sqrt{Var\{\mathsf{D}(K)\}}}, \qquad (42)$$

where K is the uniformly distributed random variable modeling the choice of the key k.

Remark 6. As the noise appears as a multiplicative factor c or d in the closed-form expressions of (i)KSA and DPA, it is eliminated in the relative distinguishing margin. This explains the results of Whitnall et al. in [28] where the relative distinguishing margin of DPA is constant. For KSA we cannot directly compare the results, as in [28] a multi-bit model was used. However, the relative margin of KSA is *almost* independent on the noise (one can observe only a small variation), which motivates for extension of our analysis to the multi-bit case.

Proposition 7 (Distinguishing margin of (i)KSA and DPA under the secrecy condition). *The distance to the nearest rival can be computed exactly as*

$$\mathrm{DM}(\mathsf{D}) = \lambda \cdot \left(\tfrac{1}{2} - \max_{k \neq k^\star} \left|\kappa(k^\star, k) - \tfrac{1}{2}\right|\right) = \lambda \cdot (1 - 2^{-n} \Delta_S). \tag{43}$$

Proof. Under the secrecy condition, $\mathsf{KSA}(k) = 2\mathsf{iKSA}(k) = c \cdot \left|\kappa(k^\star, k) - \frac{1}{2}\right|$ (see Eq. (33)) and $\mathsf{DPA}(k) = d \cdot \left|\kappa(k^\star, k) - \frac{1}{2}\right|$ (see Eq. (8)). Plugging this into Eq. (41) with λ being either c or d, and noting that $\kappa(k^\star, k^\star) = 0$ gives

$$\mathsf{D}(k^\star) - \max_{k \neq k^\star} \mathsf{D}(k) = \lambda \cdot \left(\tfrac{1}{2} - \max_{k \neq k^\star} \left|\kappa(k^\star, k) - \tfrac{1}{2}\right|\right), \tag{44}$$

which yields the required result from Eq. (40). □

Proposition 7 shows that if one chooses an S-box that is resistant to differential cryptanalysis (small Δ_S) the side-channel resistance is weak (high DM). Conversely, if the distinguishing margin is minimized, the differential uniformity is maximized. Therefore, there is a trade-off between the security against differential cryptanalyses and side-channel attacks. Note that, contrary to a common belief [4], the easiness to attack an S-box is not directly linked to its *non-linearity*, but rather to its *resistance against differential cryptanalysis*.

Links between cryptanalytic and side-channel metrics were already noted in the literature. However, previously published links (e.g., [3,8,18]) were *inequalities* because the goal was to highlight tendencies, whereas our result of Proposition 7 is an *equality*: the metrics are explicitly and exactly tied.

4.3 Practical Evaluation

We consider in this section three different $\mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ bijective S-boxes. They can be expressed as affine transforms of power functions [2]:

[4] More precisely, as will be made clear in the next Sect. 4.3, the key hypotheses that are the *hardest* to distinguish are those using a *linear* S-box. Indeed, they maximize *both* Λ_S (i.e. have $nl(S) = 0$) and Δ_S, which could wrongly indicate that the linearity is the relevant criteria.

1. A "bad" Sbox[·], termed S_1, of equation $y \mapsto a \odot y \oplus b$,
2. An "average" Sbox[·], termed S_{101}, of equation $y \mapsto a \odot y^{101} \oplus b$,
3. A "good" Sbox[·], termed S_{254}, of equation $y \mapsto a \odot y^{254} \oplus b$.

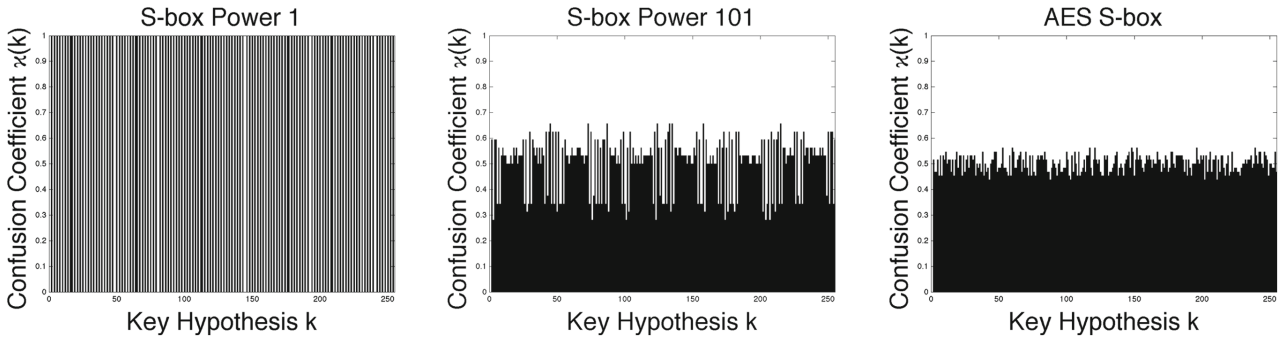


Fig. 4. Confusion coefficients for S_1, S_{101} and S_{254}

In these expressions, the operations $\oplus$ and $\odot$ are respectively the inner addition and multiplication of the Galois field $\mathbb{F}_{2^8}$ of 256 elements. The last S-Box is the one used in the AES, i.e. SubBytes, as $y^{254} = y^{-1}$ in $\mathbb{F}_{2^8}$, by Fermat's little theorem. In all three cases, the 8×8 Boolean matrix a and the 8-bit constant vector b are also those defined in the AES specification [15]; more precisely, we identify $\mathbb{F}_{2^8}$ to $\mathbb{F}_2^8$ when talking about matrices and vectors.

The values of the differential uniformity and the (relative) distinguishing margin are given in Table 1, where DM is computed without additional noise ($\sigma^2 = 0$). Figure 4 displays the confusion coefficients $\kappa(k^\star, k)$ for each S-box. It is obvious from the table and from the figure that when using S_1 (i)KSA and DPA are not able to reveal the key, which can be explained as follows: As S_1 is *linear*, both Λ_{S_1} and Δ_{S_1} are maximal (i.e. attain their upper bounds, respectively $\Lambda_{S_1} = 2^{n-1}$ and $\Delta_{S_1} = 2^n$). Thus, for all key guesses $k = k^\star \oplus \delta k$, S_1 satisfies

$$\begin{aligned} S_1(T \oplus k) &= S_1(T \oplus k^\star \oplus \delta k) = S_1(T \oplus k^\star) \oplus S_1(\delta k) \\ &= \begin{cases} S_1(T \oplus k^\star) & \text{or} \\ S_1(T \oplus k^\star) = 1 - S_1(T \oplus k^\star) \ . \end{cases} \end{aligned}$$

So, either $Y(k) = Y(k^\star)$ or $Y(k) = 1 - Y(k^\star)$, depending on $S_1(\delta k)$. In either case, the confusion condition (see Condition 2) is violated, because there exists an injective correspondence ξ (either the identity or the 1's complement) such that $Y(k^\star) = \xi(Y(k))$ with probability one. Note that, equivalently, Lemma 1 does not apply, since $\kappa(k^\star, k) \in \{0, 1\}$. Hence, (i)KSA and DPA cannot distinguish k from $k^\star$.

Moreover, one can see that the confusion coefficients for S_{254} are close to $1/2$, whereas the coefficients for S_{101} are widely spread. Thus, (i)KSA and DPA are more efficient when using S_{254} instead of S_{101}. The same effect can be seen again in Table 1 when looking at the (relative) distinguishing margin. In contrast,

Table 1. Properties of the studied S-boxes (where $\sigma^2 = 0$ for DM).

S-box	Δ_S	DM (i)KSA/DPA	RDM
S_1	256	0/0	0
S_{101}	184	0.28/0.56	2.58
S_{254}	144	0.44/0.88	9.82

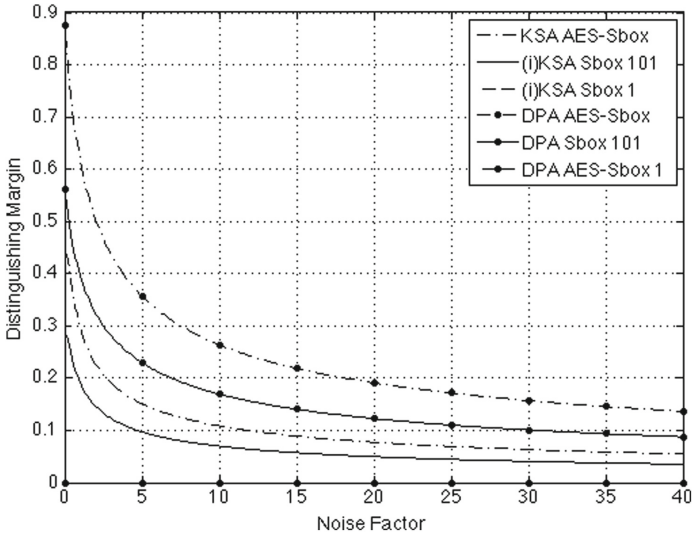


Fig. 5. Distinguishing margin for the studied S-boxes.

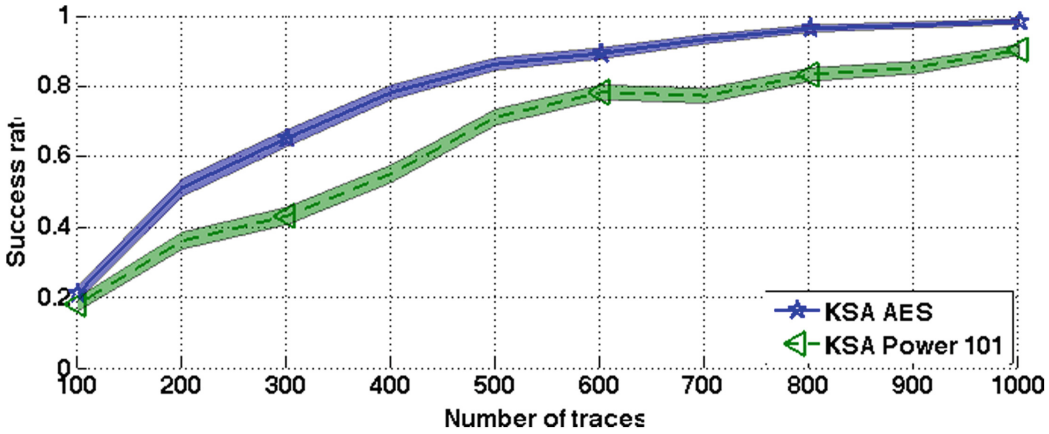


Fig. 6. Empirical success rate for S_{101} and S_{254} and $\sigma^2 = 1$ for (i)KSA.

the resistance against differential attack is less efficient (see the first column). Figure 5 displays the distinguishing margin for several values of σ^2. One can observe that the influence due to the type of S-boxes is still observable even if the noise is very large. Note that, one cannot directly compare the values of the DM of (i)KSA and DPA as it not a relative metric.

Furthermore, we conduct practical experiments using simulations and the estimated (i)KSA as defined in [10] with uniformly distributed T over 100 experiments. Figure 6 shows the empirical success rate when the leakage arises due to the Hamming weight of either S_{101} or S_{254}, where $Y(k) = [S_{101/256}(T \oplus k)]_4$. We additionally highlighted the standard deviation of the success rate by error bars as defined in [10]. As already depicted by the confusion coefficients the side channel resistance is higher for S_{101} than for S_{254}.

4.4 Research of SCA-aware S-Boxes

The traditional way to select S-Boxes is to optimize a bunch of criteria, namely *non-linearity*, *differential uniformity*, and *algebraic degree* (we refer the reader to [4], or [17, Sect. 3.1]). Actually, the algebraic degree can be seen as a less

mandatory criterion than the two others: the high-order differential attack is known to be efficient only for the second degree.

So our study shows that in order to also resist SCA, only the criterion on differential uniformity shall be relaxed, while the others can remain stringent. But we notice that building S-Boxes is difficult. One way is via stochastic algorithms (e.g., genetic algorithms). However, a random function, which has (in average) a not too bad non-linearity, has a bad differential spectrum, hence (unfortunately) a large differential uniformity Δ_S. Still, this constraint opens perspectives for the search of S-Boxes that are both cryptographically strong and less prone to the (i)KSA side-channel attacks. Indeed, our criterion is more simple than the one based on the transparency order [18], used for instance in [13,16] to design S-Boxes.

5 Conclusions and Perspectives

This paper provides a detailed theoretical analysis of KS distinguishers including soundness in case of binary sensitive variables. We showed that the closed-form expressions of KSA and iKSA are equivalent and can be expressed as a product with regard to the noise and the confusion coefficient. We show that this also holds for DPA and that even though DPA relies on a proportional scale whereas (i)KSA distinguishes nominally their closed-form only differ in the noise factor, but not in the factor regarding the confusion coefficient. These results underline the importance of theoretical studies of distinguishers as their closed-form can be directly utilized for comparisons.

Moreover, the confusion coefficient is directly related to properties of the S-box, which we further link to a differential cryptanalytic metric. In particular, we highlight that the more an S-box is resistant against side channel attacks the lesser it is secured against cryptanalytic attacks and vice versa. We have noted that the resistance against side-channel attacks is not directly linked to the *non-linearity* of the S-box as commonly believed. In our practical evaluation, we investigated three S-boxes with different power exponents 1, 101 and 254. Interestingly, the S-box of power 1 is resistant against one-bit attacks relying on the confusion coefficient (e.g. KS or DPA), whereas the S-box of power 254 (that is used in AES) is less resistant to side-channel attacks.

For future work we aim to extend our analysis to the multi-bit case and to apply the presented theoretical study as a framework to other side-channel distinguishers. We also expect to extend the study to relate the success probability of (i)KSA to the number of traces and to the S-Box properties. Additionally, the relationship between differential cryptanalytic attacks and side-channel attacks is an interesting field for future work.

Acknowledgements. The authors thank Emmanuel Prouff and Claude Carlet for sharing insights about the criteria for SCA-aware S-Boxes.

References

1. Biham, E., Shamir, A.: Differential cryptanalysis of the full 16-round DES. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 487–496. Springer, Heidelberg (1993)
2. Blondeau, C., Canteaut, A., Charpin, P.: Differential properties of power functions. In: ISIT, pp. 2478–2482. IEEE (2010)
3. Carlet, C.: On highly nonlinear S-Boxes and their inability to thwart DPA attacks. In: Maitra, S., Veni Madhavan, C.E., Venkatesan, R. (eds.) INDOCRYPT 2005. LNCS, vol. 3797, pp. 49–62. Springer, Heidelberg (2005)
4. Carlet, C.: Boolean models and methods in mathematics, computer science, and engineering. In: Crama, Y., Hammer, P. (eds.) Vectorial Boolean Functions for Cryptography, pp. 398–469. Cambridge University Press, Cambridge (2010). (Preliminary version http://www.math.univ-paris13.fr/carlet/pubs.html)
5. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 356–365. Springer, Heidelberg (1995)
6. Doget, J., Prouff, E., Rivain, M., Standaert, F.-X.: Univariate side channel attacks and leakage modeling. J. Cryptogr. Eng. **1**(2), 123–144 (2011)
7. 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)
8. Guilley, S., Hoogvorst, P., Pacalet, R.: Differential power analysis model and some results. In: Quisquater, J.-J., Paradinas, Y., Deswarte, Y., Kalam, A. (eds.) Smart Card Research and Advanced Applications VI. IFIP, vol. 153, pp. 127–142. Springer, Heidelberg (2004)
9. Kolmogorov, A.N.: Sulla determinazione empirica di una legge di distribuzione. Giorn. Ist. Ital. Attuari **4**, 83–91 (1933)
10. 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)
11. Mangard, S., Oswald, E., Popp, T.: Power analysis attacks: revealing the secrets of smart cards. Springer, December 2006. ISBN: 0-387-30857-1 (2006). http://www.dpabook.org/
12. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
13. Mazumdar, B., Mukhopadhyay, D., Sengupta, I.: Constrained search for a class of good bijective S-boxes with improved DPA resistivity. IEEE Trans. Inf. Forensics Secur. **8**(12), 2154–2163 (2013)
14. 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)
15. NIST/ITL/CSD: Advanced Encryption Standard (AES). FIPS PUB 197, Nov 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
16. Picek, S., Ege, B., Batina, L., Jakobovic, D., Papagiannopoulos, K.: Optimality and beyond: the case of 4×4 S-boxes. In: HOST, Arlington, USA. IEEE Computer Society (2014)
17. Piret, G., Roche, T., Carlet, C.: PICARO – A block cipher allowing efficient higher-order side-channel resistance. In: Bao, F., Samarati, P., Zhou, J. (eds.) ACNS 2012. LNCS, vol. 7341, pp. 311–328. Springer, Heidelberg (2012)

18. Prouff, E.: DPA attacks and S-boxes. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 424–441. Springer, Heidelberg (2005)
19. Prouff, E., Matthieu, R.: Theoretical and practical aspects of mutual information-based side channel analysis. Int. J. Appl. Cryptogr. (IJACT) **2**(2), 121–138 (2010)
20. 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)
21. Smirnov, N.V.: Tables for estimating the goodness of fit of empirical distributions. Ann. Math. Stat. **19**(2), 279–281 (1948)
22. Standaert, F.-X., Bulens, P., de Meulenaer, G., Veyrat-Charvillon, N.: Improving the rules of the DPA contest. Cryptology ePrint Archive, Report 2008/517, December 8 (2008). http://eprint.iacr.org/2008/517
23. 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)
24. TELECOM ParisTech SEN research group. DPA Contest (1st edn.), 2008–2009. http://www.DPAcontest.org/
25. TELECOM ParisTech SEN research group. DPA Contest (4th edn.), 2013–2014. http://www.DPAcontest.org/v4/
26. 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)
27. 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)
28. Whitnall, C., Oswald, E.: A fair evaluation framework for comparing side-channel distinguishers. J. Cryptogr. Eng. **1**(2), 145–160 (2011)
29. Whitnall, C., Oswald, E., Mather, L.: An exploration of the kolmogorov-smirnov test as a competitor to mutual information analysis. In: Prouff, E. (ed.) CARDIS 2011. LNCS, vol. 7079, pp. 234–251. Springer, Heidelberg (2011)
30. Whitnall, C., Oswald, E., Standaert, F.-X.: The myth of generic DPA..and the magic of learning. In: Benaloh, J. (ed.) CT-RSA 2014. LNCS, vol. 8366, pp. 183–205. Springer, Heidelberg (2014)
31. Zhao, H., Zhou, Y., Standaert, F.-X., Zhang, H.: Systematic construction and comprehensive evaluation of kolmogorov-smirnov test based side-channel distinguishers. In: Deng, R.H., Feng, T. (eds.) ISPEC 2013. LNCS, vol. 7863, pp. 336–352. Springer, Heidelberg (2013)