Be my guess: Guessing entropy vs. success rate for evaluating side-channel attacks of secure chips

Julien Béguinot, Wei Cheng, Sylvain Guilley, Olivier Rioul

Be My Guess: Guessing Entropy vs. Success Rate for Evaluating Side-Channel Attacks of Secure Chips

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

***Abstract*—In a theoretical context of side-channel attacks, optimal bounds between success rate and guessing entropy are derived with a simple majorization (Schur-concavity) argument. They are further theoretically refined for different versions of the classical Hamming weight leakage model, in particular assuming a priori equiprobable secret keys and additive white Gaussian measurement noise. Closed-form expressions and numerical computation are given. A study of the impact of the choice of the substitution box with respect to side-channel resistance reveals that its nonlinearity tends to homogenize the expressivity of success rate and guessing entropy. The intriguing approximate relation $GE = 1/SR$ is observed in the case of 8-bit bytes and low noise.**

I. Introduction

Side-Channel analysis (SCA) is a well-known threat for secure chips in embedded symmetric crypto-systems. They aim at recovering the key, byte by byte in a divide-and-conquer approach, by exploiting the leakage information. The attacker guesses one key byte K from several side-channel observations Y (modeled as a random vector) knowing the corresponding plain or cipher text bytes $T = t$ and leveraging a (noiseless or noisy) leakage model.

There are two main figures of merit in order to characterize the efficiency of the secrets' recovery: *success rate* SR and *guessing entropy* GE. Roughly speaking, SR is the empirical success probability that the best ranked (most likely) key happens to be the correct one, while GE relates to the number of tries that the attacker has to make before finding the actual secret, thereby estimating the brute force effort to find the correct key by exhaustive search. On one hand, GE is more informative insofar as it depends on the whole key ranking distribution for a given number of leakage traces. On the other hand, SR computation scales easily to the whole multibyte key (the global SR being the byte-wise product of SRs) while GE is much harder to estimate in a multibyte context.

In principle, it is desirable to evaluate *both* SR and GE during the attack because it gives a trade-off between the required number of observations (traces) and the remaining effort for key enumeration. Of course, there is a clear strong correlation between SR and GE: a lower GE will generally mean higher SR and vice versa. This is true not only for a given attack on a given device as the number of traces increases, but also to compare different attacks or different devices endowed with different countermeasures against SCA. In this respect, these metrics are relevant both for the "black hat" attacker or the "white hat" evaluator, and the "blue hat" defender.

However, there remains a missing theoretical link between SR and GE that could be exploited to estimate one metric knowing the other. Obviously there is no one-to-one relation between them, but we show that one metric can be lower and upper bounded as a function of the other, which can be optimally determined for a given leakage model.

State-of-the-art: Some previous approaches attempted to bridge the gap by extending the definition of SR to the probability SR_i that the correct key belongs to the list of the first i best key guesses [1]. For instance [2] compares various key enumeration algorithms that allow to estimate SR_i based on the knowledge of the key bytes' likelihoods.

While computing GE can be intractable in practice, [3] heuristically approximates GE by considering "security graphs" summarizing both SR and GE for a given number of traces in the same visual representation.

Chérisey et al. [4] evaluate side channel attacks through SR with inequalities derived from mutual information. They also improve an inequality on GE yet the relation between the two metrics is not investigated.

A very different approach in [5] derives fairly tight mathematical bounds to estimate GE from entropy or Rényi entropy of order $1/2$. From a purely theoretical viewpoint, [6] derives optimal bounds in very generic settings for the "guessing moments" with Rényi entropies of various orders. In this respect, considering entropy of infinite order and first order guessing moment yields optimal bounds between SR and GE.

Contribution: In this paper, we first present simple and intuitive arguments to derive the optimal bounds between the two metrics SR and GE. Such bounds are all the more tighter as the key space is small. We then refine the relationship in various SCA scenarios and leakage models, providing closed-form expressions for GE in these scenarios. We observe that the bounds are all the more tight as the leakage model is nonlinear (property of an S-Box in a block cipher), which tends to explain why the expressivity of SR and GE gets similar. This accounts for their interchangeable use as an attack working factor in the SCA literature.

Outline: The remainder of this paper is organized as follows. The notions of SR and GE are introduced in Section II with emphasis on their similar properties such as data process-

ing inequalities. Section III establishes the *Schur-concavity* of GE using majorization theory which allows one to derive simple and intuitive bounds between GE and SR. The important cases of Hamming weight leakage model, with an S-Box, and with noise, are mathematically developed in Section IV. Section V concludes the paper.

II. Definitions and Basic Properties

In this section, we define success rate and guessing entropy with emphasis on their similar properties.

Basic Notations: We consider an M-ary secret $K \in \{1, 2, \ldots, M\}$ taking $M = 2^n$ values and some *side-channel observation* Y used to guess the key $\hat{K}$. Observation Y gathers several measurements with known plain or cipher text bytes $T = t$. Since $\hat{K}$ depends on the actual secret key K only through Y, the triple $K - Y - \hat{K}$ forms a Markov chain. The guess $\hat{K}$ is said to be *blind* if it does not depend on the observation Y. For any finite set A, $|A|$ denotes its cardinality.

A. Success Rate

Definition 1 (Success Rate (SR))**.** The *success rate* of $\hat{K}$ denoted $\mathbb{P}_s$ is the probability that $\hat{K}$ guesses the secret,

$$\mathbb{P}_s = \mathbb{P}(\hat{K} = K). \tag{1}$$

Theorem 1 (Optimal SR)**.** *The maximal success rate is attained with the MAP rule* $\hat{k}(y) \in \arg\max_k \mathbb{P}(K = k|Y = y)$ *and is given by*

$$\mathbb{P}_s(K|Y) = \mathbb{E}_Y\big(\max_k \mathbb{P}(K = k|Y)\big). \tag{2}$$

In particular, for a blind guess, we write

$$\mathbb{P}_s(K) = \max_k \mathbb{P}(K = k) \geq \frac{1}{M}. \tag{3}$$

Proof. Since $K-Y-\hat{K}$ is a Markov chain, $\mathbb{P}(\hat{K} = \hat{k}|Y, K) = \mathbb{P}(\hat{K} = \hat{k}|Y)$ so that

$$\begin{aligned} \mathbb{P}_s &= \mathbb{E}_Y\big(\mathbb{P}(\hat{K} = K|Y)\big) && (4)\\ &= \mathbb{E}_Y\big(\textstyle\sum_k \mathbb{P}(K = k|Y)\mathbb{P}(\hat{K} = k|Y)\big) && (5)\\ &\leq \mathbb{E}_Y\big(\max_k \mathbb{P}(K = k|Y)\big) && (6)\end{aligned}$$

with equality if and only if $\mathbb{P}(\hat{K} = \hat{k}|Y) = 1$ for some $\hat{k} \in \arg\max_k \mathbb{P}(K = k|Y)$. □

Theorem 2 (Data Processing Inequality for $\mathbb{P}_s$)**.** *One has*

$$\mathbb{P}_s(K) \leq \mathbb{P}_s(K|Y) \tag{7}$$

(observing side channel information always increases success). More generally, if $K - Y - Z$ is a Markov chain, then

$$\mathbb{P}_s(K|Z) \leq \mathbb{P}_s(K|Y) \tag{8}$$

(data processing can only reduce success).

Proof. Since $\mathbb{P}(K = k|Y) \leq \max_k \mathbb{P}(K = k|Y)$, taking the expectation over Y gives $\mathbb{E}_Y \mathbb{P}(K = k|Y) \leq \mathbb{E}_Y \max_k \mathbb{P}(K = k|Y)$ for every k, hence

$$\max_k \mathbb{E}_Y \mathbb{P}(K = k|Y) \leq \mathbb{E}_Y \max_k \mathbb{P}(K = k|Y) \tag{9}$$

which is (7). This in turn implies $\mathbb{P}_s(K|Z) \leq \mathbb{P}_s(K|Y, Z)$ by considering each fixed value $Z = z$ and taking the expectation over Z. Finally, $\mathbb{P}_s(K|Y, Z) = \mathbb{P}_s(K|Y)$ because $K|Y, Z$ is distributed as $K|Y$ since $K - Y - Z$ is a Markov chain. □

B. Guessing Entropy

In a guessing problem, keys are guessed one by one in a sequence $(1), (2), \ldots, (M)$. Such a sequence is a permutation of $\{1, 2, \ldots, M\}$ where (i) denotes the ith ranked key for $i = 1, 2, \ldots, M$. Thus, first (1) is guessed, then (2), etc. The number of key guesses before the actual secret $K = (I)$ is found is I, a random variable which depends upon the observation Y. Hence, $K - Y - I$ forms a Markov Chain.

Definition 2 (Guessing Entropy (GE))**.** The guessing entropy is the average number of guesses:

$$G = \mathbb{E}_{K,Y}(I) \tag{10}$$

Notice that some previous works define GE as I itself [5], [7].

Let $p_{(i)|y} = \mathbb{P}(K = (i)|Y = y)$ be the probability of the ith ranked key given observation $Y = y$.

Theorem 3 (Optimal GE)**.** *The minimal guessing entropy is attained with the ranking rule*

$$p_{(1)|y} \geq p_{(2)|y} \geq \cdots \geq p_{(M)|y} \tag{11}$$

and is given by

$$G(K|Y) = \mathbb{E}_Y\left(\sum_{k=1}^{M} k\, p_{(k)|Y}\right). \tag{12}$$

In particular, for a blind guess, this reduces to $G(K) = \sum_{k=1}^{M} k p_{(k)}$, where the $p_{(k)} = \mathbb{P}(K = (k))$ are in descending order.

Often $G(K)$ is simply referred to as the guessing entropy of K while $G(K|Y)$ is known as the *conditional guessing entropy* of K given Y.

Proof. By the law of total expectation,

$$G = \mathbb{E}_Y\, \mathbb{E}_K(I|Y) = \mathbb{E}_Y\left(\sum_{i=1}^{M} i \cdot \mathbb{P}(K = (i)|Y)\right). \tag{13}$$

By the rearrangement inequality [8, Thm. 368], since (i) is an increasing sequence, the minimum G is obtained when the probabilities $\mathbb{P}(K = (i)|Y)$ are in descending order. □

Theorem 4 (Data Processing Inequality)**.** *One has*

$$G(K) \geq G(K|Y) \tag{14}$$

(observing side channel information improves guessing).

More generally, if $K - Y - Z$ is a Markov chain, then

$$G(K|Z) \geq G(K|Y) \tag{15}$$

(data processing can only worsen guessing).

Proof. Without loss of generality assume that K's probability distribution is in descending order $p_1 \geq p_2 \geq \cdots \geq p_M$ so that $I = K$ and $G(K) = \mathbb{E}(K)$. Then by definition of minimum guessing, $G(K|Y = y) \leq \mathbb{E}(K|Y = y)$. Taking the

expectation over Y gives $G(K|Y) \le \mathbb{E}_Y\, \mathbb{E}(K|Y) = \mathbb{E}(K) = G(K)$ by the law of total expectation. This proves (14). This in turn implies $G(K|Z) \ge G(K|Y,Z)$ by considering each fixed value of $Z = z$ and taking the expectation over Z. Finally, $G(K|Y,Z) = G(K|Y)$ because $K|Y,Z$ is distributed as $K|Y$ since $K - Y - Z$ is a Markov chain. □

III. Bounds Derivation

A. Schur-Concavity of Guessing Entropy

First we introduce some notation for the theory of majorization [9]. Hereafter we let $p_{(1)}, p_{(2)}, \ldots, p_{(M)}$ denote the vector $p = (p_1, p_2, \ldots, p_M)$ of nonnegative elements arranged in *descending* order $p_{(1)} \ge p_{(2)} \ge \cdots \ge p_{(M)}$. We also use the *cumulative sum* notation

$$P_{(k)} = p_{(1)} + p_{(2)} + \cdots + p_{(k)} \qquad (k = 1, \ldots, M) \quad (16)$$

with the convention $P_{(0)} = 0$.

Definition 3 (Majorization)**.** We say that q *majorizes* p, and we write $p \preceq q$ if

$$P_{(k)} \le Q_{(k)} \qquad (k = 1, \ldots, M-1) \quad (17)$$

and $P_{(M)} = Q_{(M)}$. (Notice that this latter condition is always satisfied when p and q are probability distributions since $P_{(M)} = \sum_k p_k = 1$ and $Q_{(M)} = \sum_k q_k = 1$.)

The intuition behind majorization is that $p \preceq q$ means that p is more "spread out" than q. Thus in the case of a probability distribution p, the minimum spread is for a deterministic (but Dirac) distribution and the maximum spread is for a uniform distribution. Indeed, it is easily checked that

$$\big(\tfrac{1}{M}, \tfrac{1}{M}, \ldots, \tfrac{1}{M}\big) \preceq p \preceq (1, 0, 0, \ldots, 0) \quad (18)$$

for any probability distribution $p = (p_1, p_2, \ldots, p_M)$. More generally [9],

$$\big(\tfrac{P_{(M)}}{M}, \tfrac{P_{(M)}}{M}, \ldots, \tfrac{P_{(M)}}{M}\big) \preceq p \preceq (P_{(M)}, 0, 0, \ldots, 0) \quad (19)$$

for any vector $p = (p_1, p_2, \ldots, p_M)$.

Definition 4 (Schur-Concavity)**.** A function $G(p)$ is *Schur-concave* if $p \preceq q \implies G(p) \ge G(q)$.

In other words, a Schur-concave function is large for "spread out" distributions and small for "condensed" distributions.

It is well known that entropy [9], and more generally the Rényi entropy of any order [10] (e.g., min-entropy, collision entropy, etc.) is Schur-concave. Perhaps lesser known is that guessing entropy is Schur-concave:

Theorem 5 (Schur-Concavity of Guessing Entropy)**.** *Guessing entropy $G(K) = \sum_{k=1}^{M} k p_{(k)}$ is Schur-concave in p.*

Proof. Using *summation by parts*,

$$\sum_{k=1}^{M} k p_{(k)} = \sum_{k=1}^{M} k(P_{(k)} - P_{(k-1)}) \quad (20)$$

$$= M P_{(M)} - P_{(0)} + \sum_{k=1}^{M-1} \big(k - (k+1)\big) P_{(k)} \quad (21)$$

$$= M - P_{(1)} - P_{(2)} - \cdots - P_{(M-1)}. \quad (22)$$

The Schur-concavity of $G(K)$ is now obvious from the definitions. □

Remark 1. Recent works on guessing such as [11] state Schur-concavity of Rényi entropy but do not mention the same property for GE. During the review process we became aware that the Schur-concavity of GE was observed earlier by Khouzani and Malacaria [12] among many other types of entropies. They established Schur-concavity by stating (without proof) that $G(K)$ is symmetric and concave in the probability distribution of K. While symmetry is obvious here, concavity of GE is precisely established by inequality (14) above.

Remark 2. The proof of this Theorem carries over verbatim for any function of the form $\sum_{k=1}^{M} \alpha_k p_{(k)}$ where (α_k) is an increasing sequence. In particular for guessing moments [13]:

Corollary 1 (Schur-Concavity of Guessing Moments)**.** *$G_\rho(K) = \sum_{k=1}^{M} k^\rho p_{(k)}$ is Schur-concave in p.*

These results are in line with the known inequalities between guessing entropy (or guessing moments) and entropy (or Rényi entropies) as established in [13], [14].

Remark 3. Since guessing entropy is Schur-concave, it follows from (18) that guessing entropy is minimized for the deterministic distribution and maximized for the uniform distribution, which gives the trivial bounds $1 \le G(K) \le \frac{M+1}{2}$.

B. Optimal Bounds on GE for a Given SR

Theorem 6 (Optimal Lower and Upper Bounds for Blind Guess)**.** *For a fixed success rate $\mathbb{P}_s(K)$, the optimal lower and upper bound on guessing entropy $G(K)$ are*

$$\big(1 + \lfloor \tfrac{1}{\mathbb{P}_s(K)} \rfloor\big)\big(1 - \tfrac{1}{2}\lfloor \tfrac{1}{\mathbb{P}_s(K)} \rfloor \mathbb{P}_s(K)\big) \le G(K) \le 1 + \frac{M}{2}(1 - \mathbb{P}_s(K)). \quad (23)$$

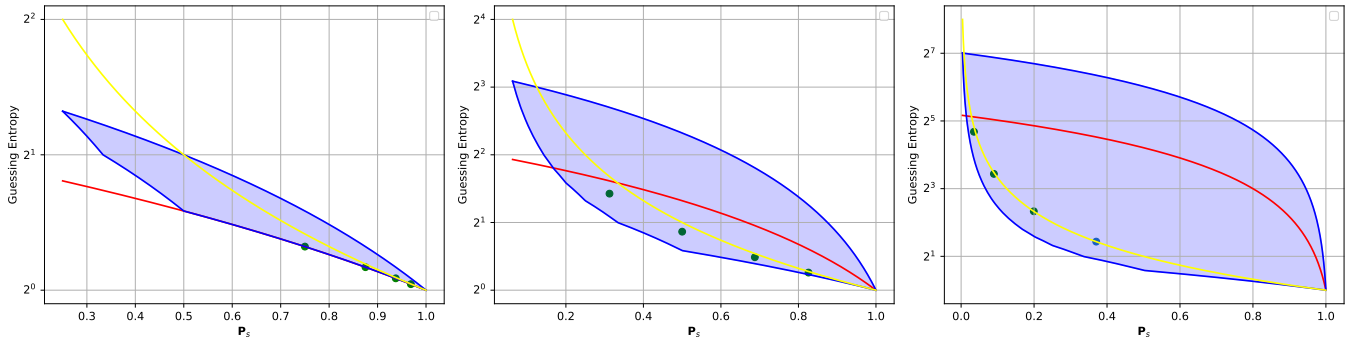
Proof. From Theorem 5, for a fixed $p_{(1)}$, $G(K) - \mathbb{P}_s(K) = \sum_{k=2}^{M} k p_{(k)}$ is Schur-concave in $(p_{(2)}, \ldots, p_{(M)})$. It follows that this quantity is maximum for the uniform distribution $(p_{(2)}, \ldots, p_{(M)}) = (\frac{1-\mathbb{P}_s}{M-1}, \frac{1-\mathbb{P}_s}{M-1}, \ldots, \frac{1-\mathbb{P}_s}{M-1})$ and minimum for the least spread out distribution $(p_{(2)}, \ldots, p_{(M)})$ with $p_{(k)} \le \mathbb{P}_s$. It is easily seen that the latter (least spread out) distribution is of the form $(p_{(2)}, \ldots, p_{(M)}) = (\mathbb{P}_s, \ldots, \mathbb{P}_s, x, 0, \ldots, 0)$ where $x < \mathbb{P}_s$ is such that $\sum_{k=2}^{M} p_{(k)} = 1$, that is, $x = 1 - \lfloor 1/\mathbb{P}_s \rfloor \mathbb{P}_s$. Plugging these values of $(p_{(1)}, p_{(2)}, \ldots, p_{(M)})$ into the expression of the guessing entropy gives the announced lower and upper bounds. □

Fig. 1 below illustrates the corresponding optimal regions (in blue) between $\mathbb{P}_s$ and G for $M = 2^n$ with $n = 2, 4, 8$.

Theorem 7 (Bounds with Side-Channel Information)**.**

$$(1 + \lfloor \tfrac{1}{\mathbb{P}_s(K|Y)} \rfloor)(1 - \lfloor \tfrac{1}{\mathbb{P}_s(K|Y)} \rfloor \frac{\mathbb{P}_s(K|Y)}{2}) \le G(K|Y) \le 1 + \frac{M}{2}(1 - \mathbb{P}_s(K|Y)). \quad (24)$$

Proof. Applying Theorem 6 to the random variable $K|Y = y$ for every value y gives $(1 + \lfloor \frac{1}{\mathbb{P}_s(K|Y=y)} \rfloor)(1 -$



(a) Regions for $M = 2^2$ (b) Regions for $M = 2^4$ (c) Regions for $M = 2^8$

Fig. 1. Regions $G(K|Y)$ vs. $\mathbb{P}_s(K|Y)$ as given by Theorem 7. The red curve is the improved upper bound (27) for the deterministic Hamming weight model. The 4 green dots are the exact values computed for $Q = 1$, 2, 3, and 4 traces. The yellow curve corresponds to the formula $G = \mathbb{P}_s^{-1}$ and seems to approximate well the actual relation for $n = 8$ bits.

$\lfloor \frac{1}{\mathbb{P}_s(K|Y=y)} \rfloor \frac{\mathbb{P}_s(K|Y=y)}{2}) \le G(K|Y=y) \le 1 + \frac{M_y}{2}(1 - \mathbb{P}_s(K|Y=y))$ where $M_y \le M$ is the number of possible keys given $Y = y$. Taking the expectation over Y we obtain lower and upper bounds on $G(K|Y) = \mathbb{E}_y\, G(K|Y=y)$. By Theorem 1, $\mathbb{P}_s(K|Y) = \mathbb{E}_y\, \mathbb{P}_s(K|Y=y)$, we obtain the announced upper bound $G(K|Y) \le 1 + \frac{M}{2}(1 - \mathbb{P}_s(K|Y))$.

The lower bound, of the form $\phi(p) = (1 + \lfloor \frac{1}{p} \rfloor)(1 - \lfloor \frac{1}{p} \rfloor \frac{p}{2})$, is piecewise linear and *convex* in $p = \mathbb{P}_s$. Indeed, its value at $p = \frac{1}{k}$ for positive integer k is $(1+k)(1 - \frac{k}{2k}) = \frac{1+k}{2}$, hence its successive slopes between $p = \frac{1}{k-1}$ and $p = \frac{1}{k}$ are $\frac{1/2}{\frac{1}{k} - \frac{1}{k-1}} = -\frac{k(k-1)}{2}$, which is increasing as $p = \frac{1}{k}$ increases. Thus, by Jensen's inequality, we have $\mathbb{E}_y[\phi(\mathbb{P}_s(K|Y=y))] \ge \phi(\mathbb{E}_y[\mathbb{P}_s(K|Y=y)]) = \phi(\mathbb{P}_s(K|Y))$, which gives the announced lower bound. □

Remark 4. It is immediate from its proof that a refinement of the upper bound of Theorem 7 is given by

$$G(K|Y) \le 1 + \frac{\max_y M_y}{2}(1 - \mathbb{P}_s(K|Y)). \tag{25}$$

This is particularly interesting for deterministic (noiseless) leakage since, as shown in the next Section, M_y decreases rapidly as the number of traces increases.

IV. Refined Bounds for Hamming Weight Leakage Model

A. Deterministic Leakage for One Observed Trace

A well-known leakage model of an embedded cryptographic device in a noiseless scenario is the *Hamming weight model*

$$Y = w_H(K \oplus t) \tag{26}$$

where w_H is the bitwise Hamming weight operator [15], $\oplus$ denotes the XOR operation and $T = t$ is given value of plain or cipher text. Let $\mathcal{Y} = \{0, 1, \ldots, n\}$ be the set of all values taken by Y and $\mathcal{K}_y$ be the set of key values k for fixed $Y = y$.

Theorem 8. *For the Hamming weight model, the region* (24) *reduces (improves) to the following values of SR and GE:*

$$G(K|Y) \le 1 + \frac{1}{2}\binom{n}{\lfloor \frac{n+1}{2} \rfloor}(1 - \mathbb{P}_s(K|Y)) \tag{27}$$

$$\mathbb{P}_s(K|Y) \ge \binom{n}{\lfloor \frac{n+1}{2} \rfloor}^{-1}. \tag{28}$$

Proof. For observed $Y = y$, $M_y = |\mathcal{K}_y|$ is the number of n-bit vectors having Hamming weight y, that is, $M_y = \binom{n}{y}$ in the improved bound (25). Since $\max_y M_y = \binom{n}{\lfloor \frac{n+1}{2} \rfloor}$, this gives (27).

Since $K|Y=y$ has M_y possible values, $\mathbb{P}_s(K|Y=y) = \max_k \mathbb{P}(K=k|Y=y) \ge \frac{1}{M_y} \ge 1/\binom{n}{\lfloor \frac{n+1}{2} \rfloor}$. Averaging over Y gives (28). Equality holds if and only if K is uniformly distributed over the largest class $\mathcal{K}_y$. □

Figure 1 illustrates the improvement for $n = 2$, 4, and 8 bits, where the red curves correspond to the reduced upper bound (27). It can be observed that the case of equality in (28) corresponds to the points where the upper bound (27) (red curve) and the lower bound in (24) (blue curve) meet. In particular for $M = 2^2$ our improved upper bound coincide with the lower bound. This proves that in this case the SR and GE are in one to one correspondence with a Hamming Weight leakage model.

B. Case of Equiprobable Keys

A usual assumption is that K is a priori uniformly distributed over M values. In this case the following exact formulas hold.

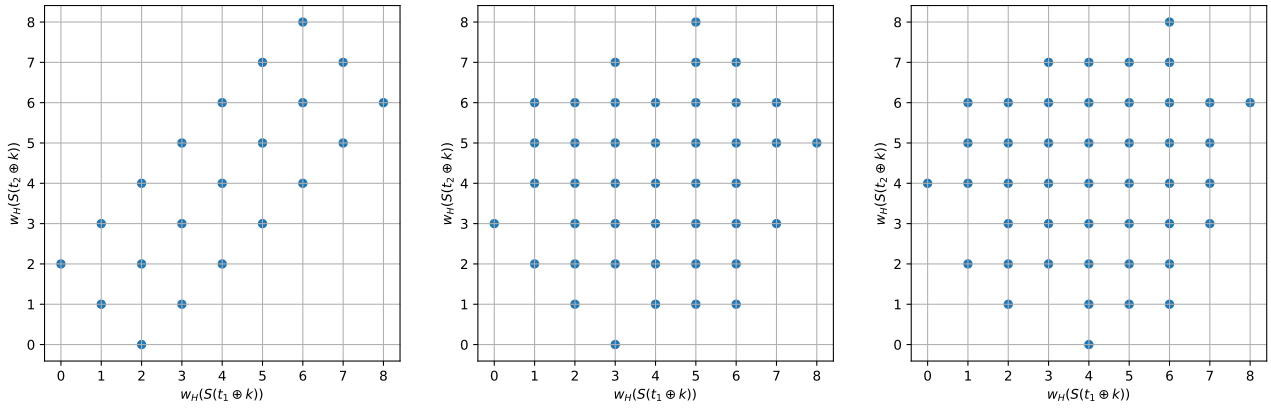
Theorem 9 (Exact Formulas of Equiprobable Keys)**.**

$$\mathbb{P}_s(K|Y) = \frac{|\mathcal{Y}|}{M} \quad \textit{and} \quad G(K|Y) = \frac{1}{2} + \frac{1}{2M}\sum_{y \in \mathcal{Y}} M_y^2. \tag{29}$$

More generally, these formulas hold when Y is any deterministic function of K. In the special case of the Hamming weight model (26)*, this gives*

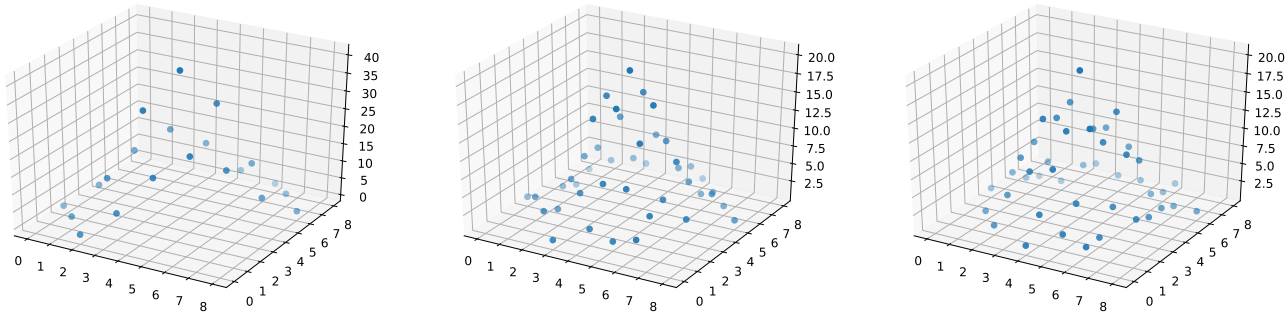
$$\mathbb{P}_s(K|Y) = (n+1)2^{-n}, \quad G(K|Y) = \frac{1 + 2^{-n}\binom{2n}{n}}{2}. \tag{30}$$

Proof. If K is equiprobable and $Y = y$ is fixed (with probability $\mathbb{P}(Y=y) = \frac{M_y}{M}$), then $K|Y=y$ is equiprobable over $M_y = |\mathcal{K}_y|$ values so that $\mathbb{P}_s(K|Y=y) = \frac{1}{M_y}$. Taking the average over Y gives $\mathbb{P}_s(K|Y) = \sum_y \frac{M_y}{M}\frac{1}{M_y}$, which yields the announced expression for SR. Similarly $G(K|Y=y) = \frac{M_y+1}{2}$ for a uniform guess, and taking the average over Y gives $G(K|Y) = \sum_y \frac{M_y}{M}\frac{M_y+1}{2}$, which yields the announced expression for GE. The Hamming weight case follows from the Vandermonde's identity $\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}$. □



(a) S_1 (linear) (b) S_7 (c) S_{254} (AES—nonlinear)

Fig. 2. Sets $\mathcal{Y}$ of deterministic Hamming weight leakage values for $t_1 = 0$ and $t_2 = 3 = (00000011)$ for different S-Boxes.



(a) S_1 (linear) (b) S_7 (c) S_{254} (AES—nonlinear)

Fig. 3. Number of keys M_y for given $Y = y$ for $t_1 = 0$ and $t_2 = 3$ for different S-Boxes. The x, y-axes represent the two coordinates of the 2-dimensional leakage $Y = y = (y_1, y_2)$. The z-axis corresponds to the number M_y of possible keys given $Y = y$, which tends to decrease as the nonlinearity of the S-Box increases. In particular, $\max_y M_y$ is respectively 40, 20, 20 thereby improving the bound (25) for nonlinear S-Boxes.

It is easily seen that we recover the well-known expressions $\mathbb{P}_s(K) = \frac{1}{M}$ and $G(K) = \frac{M+1}{2}$ for a blind guess.

C. Deterministic Leakage for Multiple Observed Traces

Consider multiple observed traces (Q queries) $Y = (Y_1, Y_2, \ldots, Y_Q)$, where

$$Y_i = w_H(K \oplus t_i) \qquad (i = 1, 2, \ldots, Q) \tag{31}$$

for fixed and distinct plain or cipher texts $t_1, t_2, \ldots, t_Q$. In this case we are faced with a combinatorial problem since letting $Y = y$ determines the intersection of Q Hamming balls.

To simplify the analysis we consider $Q = 2$ and the computation of SR. Without loss of generality we can set $t_1 = 0$ and consider variable $t_2 = t$.

Theorem 10. *Let $w = w_H(t)$. Then*

$$\mathbb{P}_s(K|Y) = \frac{(w+1)(n-w+1)}{2^n} \tag{32}$$

In particular for 8-bit bytes ($n = 8$), one obtains:

$$\mathbb{P}_s = \begin{cases} \frac{n+1}{2^n} & \text{for } w \in \{0, 8\} \\ \frac{2n}{2^n} & \text{for } w \in \{1, 7\} \\ \frac{3(n-1)}{2^n} & \text{for } w \in \{3, 6\} \\ \frac{4(n-2)}{2^n} & \text{for } w \in \{4, 5\}. \end{cases} \tag{33}$$

Proof. We show that $|\mathcal{Y}| = (w+1)(n-w+1)$ in (29) as illustrated in Fig. 2 (a), where the set $\mathcal{Y}$ of points $(y_1 = w_H(k), y_2 = w_H(k \oplus t))$ forms a (rotated) $(w+1) \times (n-w+1)$ rectangle. Indeed, let $\bar{t}$ be the binary complement of t and write the decomposition $w_H(k) = w_H(k \cdot t) + w_H(k \cdot \bar{t})$ where $\cdot$ denotes the bitwise product. For fixed $w_H(t) = w$, $w_H(k \cdot t)$ can take $w+1$ values and $w_H(k \cdot \bar{t})$ takes $(n-w)+1$ independent values. Since $w_H(k \oplus t) = w_H(k) + w_H(t) - w_H(k \cdot t) = w + w_H(k \cdot \bar{t})$, we have $(y_1, y_2) = (w_H(k \cdot t) + w_H(k \cdot \bar{t}), w + w_H(k \cdot \bar{t}))$ which takes all possible $(w+1)(n-w+1)$ values. □

More generally, the set $\mathcal{Y}$ can be determined by exhaustive enumeration of Hamming weights. We computed numerically the resulting SR and GE for $Q = 1$, 2, 3, and 4 traces. They are plotted as green dots in Fig. 1 for different values of M.

D. Role of the S-Box in the Hamming Weight Model

To prevent differential and linear cryptanalysis, block ciphers are composed with non-linear operations. This non-linearity is performed by substitution box (S-Box). We investigate different choices for the S-Box to observe its effect on SR and GE with respect to SCA resistance. We consider

$$S_i(x) = ax^i \oplus b \in \mathbb{F}_{2^n} \tag{34}$$

for exponents $i = \{1, 7, 19, 101, 254\}$, constants $a, b \in \mathbb{F}_{2^n}$.

As an illustration, Fig. 2 plots the various sets $\mathcal{Y}$ of Hamming weight leakage values for S_1 (linear), S_7, and the AES standard S_{254} (highly nonlinear). We observe that the cardinality $|\mathcal{Y}|$

increases as exponent i increases. This shows that SR (as given by Theorem 9) increases as nonlinearity increases. Fig. 3 (the 3-D extension of Fig. 2) also plots M_y as a function of $y \in \mathcal{Y}$. Here we observe that M_y tends to globally decrease as exponent i increases, which shows that GE (as given by Theorem 9) decreases as nonlinearity increases.

Therefore, the non-linearity of the S-Box diminishes the side channel resistance. The geometrical explanation of this phenomenon is that the scatter plots of Fig. 2 and 3 tend to spread out for nonlinear S-Boxes. This confirms the observation of [16] on the effect of the S-Box on the confusion coefficient, which for monobit leakage relates to both SR and GE [17].

E. Hamming Weight Leakage Model With Gaussian Noise

In this section we derive the expression of SR and GE in an Hamming Weight leakage scenario

$$Y = w_H(K \oplus t) + N \tag{35}$$

in the presence of additive white Gaussian Noise (AWGN) $N \sim \mathcal{N}(0, \sigma^2)$. Let f_Y and ϕ_σ denote the p.d.f. of Y and N, respectively. Thus $\phi_\sigma(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp(-\frac{x^2}{2\sigma^2})$. Also let Q denote the standard Q-function $Q(x) = \int_x^\infty \frac{e^{-\frac{u^2}{2}}}{\sqrt{2\pi}} du$.

Theorem 11 (Expression With Noisy Leakage)**.**

$$\mathbb{P}_s(K|Y) = \frac{n+1}{M} - \frac{2n}{M} Q\big(\frac{1}{2\sigma}\big), \tag{36}$$

$$G(K|Y) = \frac{1}{2} + \frac{\binom{2n}{n}}{2M} + \frac{2\binom{2n}{n+1}}{M} Q\big(\frac{1}{2\sigma}\big) + \sum_{i=2}^{2n} f_i(n) Q\big(\frac{i}{2\sigma}\big), \tag{37}$$

where the latter sum is negligible at first order in σ and where the f_i are rational functions in n and M.

For low noise one recovers (30).

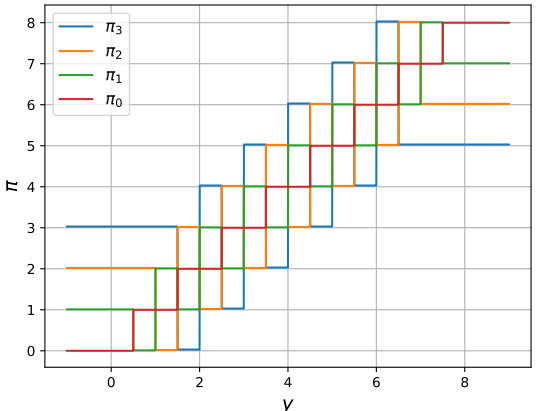


Fig. 4. $\pi_i(y)$ for $i = 0, 1, 2, 3$. We can observe that the π_i are step functions. Their are constant on the interval of the form $[\frac{p}{2}, \frac{p+1}{2})$ for all integer p.

Proof. For $j = 0, \ldots, n$ let $\pi_j(y)$ denote the $(j+1)$-th closest point to y in $\mathcal{Y}$. In particular, $\pi_0(y)$ is the closest point to y in $\mathcal{Y}$. It can be checked with the help of Fig. 4 that

$$\pi_0(y) = \begin{cases} 0 & \text{for } y \le -\frac{1}{2} \\ i & \text{for } y \in [i - \frac{1}{2}, i + \frac{1}{2}) \\ n & \text{for } y \ge n + \frac{1}{2}. \end{cases} \tag{38}$$

From (2), one has

$$\begin{aligned} \mathbb{P}_s &= \frac{1}{M} \int \phi_\sigma(y - \pi_0(y))\, \mathrm{d}y \\ &= \frac{1}{M} \Big(2Q(\frac{1}{2\sigma}) + \sum_{i=0}^{n} \int_{i-\frac{1}{2}}^{i+\frac{1}{2}} \phi_\sigma(y - i) \Big) \\ &= \frac{1}{M} \Big(2Q(\frac{1}{2\sigma}) + (n+1) \int_{-\frac{1}{2}}^{\frac{1}{2}} \phi_\sigma(y) \Big) \\ &= \frac{1}{M} (2Q(\frac{1}{2\sigma}) + (n+1)(1 - 2Q(\frac{1}{2\sigma}))) \end{aligned}$$

which after simplification proves (36).

Now from (12), one has

$$G(K|Y) = \int f_Y(y) \sum_{k=1}^{M} k\, p_{(k)|y}\, \mathrm{d}y \tag{39}$$

Since the noise is Gaussian, the $p_{(k)|y}$ are sorted by Euclidean distance. Applying Bayes' rule we obtain

$$p_{(k)|y} = \phi_\sigma(y - \pi_j(y)) \frac{1/M}{f_Y(y)}, \quad k = S_{j-1}(y) + 1, \ldots, S_j(y). \tag{40}$$

where $S_j(y) = \sum_{i=0}^{j} \binom{n}{\pi_i(y)}$ for $j = 0, \ldots, n$ with the convention $S_{-1}(y) = 0$. Therefore,

$$\begin{aligned} G(K|Y) &= \int f_Y(y) \sum_{j=0}^{n} \sum_{k=S_{j-1}(y)+1}^{S_j(y)} k\, \phi_\sigma(y - \pi_j(y)) \frac{1/M}{f_Y(y)}\, \mathrm{d}y \\ &= \frac{1}{M} \sum_{j=0}^{n} \int \sum_{k=S_{j-1}(y)+1}^{S_j(y)} k \phi_\sigma(y - \pi_j(y))\, \mathrm{d}y \\ &= \frac{1}{M} \sum_{j=0}^{n} \int C_j(y) \phi_\sigma(y - \pi_j(y))\, \mathrm{d}y \end{aligned}$$

where

$$C_j(y) = \frac{S_j(y)(S_j(y)+1) - S_{j-1}(y)(S_{j-1}(y)+1)}{2} \tag{41}$$

$$= \tfrac{1}{2} \binom{n}{\pi_j(y)} \big(2S_{j-1}(y) + \binom{n}{\pi_j(y)} + 1\big). \tag{42}$$

The $j = 0$ term can be written as

$$\int \frac{S_1(y)(1 + S_1(y))}{2} \phi_\sigma(y - w_H(\pi_1(y)))\, \mathrm{d}y \tag{43}$$

$$= \Big[2 \int_{\frac{1}{2}}^{\infty} \phi_\sigma(y) dy + \sum_{i=0}^{n} \int_{i-\frac{1}{2}}^{i+\frac{1}{2}} \frac{\binom{n}{i}(1 + \binom{n}{i})}{2} \phi_\sigma(y - i) \Big] \tag{44}$$

$$= \Big[2Q(\frac{1}{2\sigma}) + \sum_{i=0}^{n} \frac{\binom{n}{i}(1 + \binom{n}{i})}{2} (1 - 2Q(\frac{1}{2\sigma})) \Big] \tag{45}$$

$$= \frac{M}{2} + \frac{1}{2} \binom{2n}{n} - Q(\frac{1}{2\sigma})(M + \binom{2n}{n} - 2). \tag{46}$$

We now compute the $j=1$ term. It can be checked with the help of Fig. 4 that

$$\pi_1(y) = \begin{cases} 1 & \text{for } y \le -\frac{1}{2} \\ i-1 & \text{for } y \in [i-\frac{1}{2}, i) \\ i+1 & \text{for } y \in [i, i+\frac{1}{2}) \\ n-1 & \text{for } y \ge n+\frac{1}{2}. \end{cases} \tag{47}$$

In the $j=1$ term, the contribution of the integral from $\frac{1}{2}$ to ∞ and $-\infty$ to $-\frac{1}{2}$ both yields a term of value $\frac{n(n+3)}{2}Q(\frac{3\sigma}{2})$. The contribution of the integral over $[i-\frac{1}{2}, i)$ yields

$$\frac{1}{2}\binom{n}{i-1}[2\binom{n}{i}+\binom{n}{i-1}+1](Q(\frac{1}{2\sigma})-Q(\frac{1}{\sigma})). \tag{48}$$

and that over $(i, i+\frac{1}{2}]$ yields

$$\frac{1}{2}\binom{n}{i+1}[2\binom{n}{i}+\binom{n}{i+1}+1](Q(\frac{1}{2\sigma})-Q(\frac{1}{\sigma})). \tag{49}$$

Summing the contribution yields, after some calculation,

$$n(n+3)Q(\frac{3\sigma}{2})+[M-2+2\binom{2n+1}{n+1}-\binom{2n}{n}](Q(\frac{1}{2\sigma})-Q(\frac{1}{\sigma})). \tag{50}$$

Here we have used the following Vandermonde identities:

$$\sum_{i=0}^{n}\binom{n}{i+1}^2 = \sum_{i=0}^{n}\binom{n}{i-1}^2 = \binom{2n}{n}-1$$

$$\sum_{i=0}^{n}\binom{n}{i}\binom{n}{i-1} = \sum_{i=0}^{n}\binom{n}{i}\binom{n}{i+1} = \sum_{i=0}^{n}\binom{n}{i}[\binom{n+1}{i}-\binom{n}{i}]$$
$$= \binom{2n+1}{n+1}-\binom{2n}{n}.$$

Summing the $j=0$ and $j=1$ terms simplifies to the first three terms in (37).

One can go further and compute terms corresponding to $j=2,3,\ldots,n$. It is easily seen from the above derivation that splitting the integral with Chasles relation on the interval where π_i is constant yields a sum of weighted $Q(\frac{i}{2\sigma})$ as shown in (37). □

F. Validation by Simulation

We evaluated numerically the relation between SR and GE for different noise levels σ^2 and different number of traces. The evaluation has been performed by 10^3 repetitions of maximum likelihood attacks on synthetically generated leakages.

Figure 6 on next page plots the resulting values of SR and GE for various noise levels and S-Boxes. We observe that for low noise the approximation $G(K|Y) \approx \mathbb{P}_s(K|Y)^{-1}$ still holds (yellow curve). As the noise increases, for a given SR, GE increases, and the latter approximation is no longer valid. The S-Box nonlinearity accentuates this effect because it decreases the minimum distance of points in $\mathcal{Y}$ in Fig. 2 and, therefore, makes the maximum likelihood attack less robust to noise.

G. Validation on real traces from DPA Contest V4.2

Figure 5 plots the results on values of SR and GE computed on the three first folders of the DPA Contest V4.2 with a Hamming Weight template attack with known mask. As expected from the simulation the guessing entropy is lower bounded by SR^{-1}.

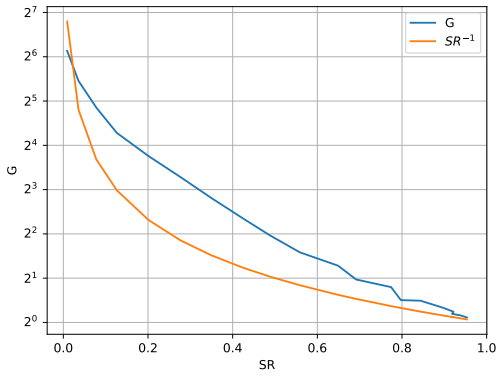


Fig. 5. Results on Traces from DPA Contest v4.2

V. Conclusion

In this paper, optimal bounds between success rate and guessing entropy are derived with a simple majorization argument, and further improved for the Hamming weight leakage model—in particular for the classical assumptions of a priori equiprobable secret keys and additive white Gaussian measurement noise. Closed-form expressions and numerical computations are given for various leakage scenarios. A study of the impact of the choice S-Box with respect to SCA resistance reveals that nonlinearity of the S-Box tends to tighten the bounds between SR and GE. The approximate relation $GE = 1/SR$ holds in the case of 8-bit bytes and low noise.

As a perspective, we notice that our methodology can be easily generalized to the definitions of the ith order success rate [1] SR_i vs. GE. However, as pointed out in [7], such theoretical work assumes perfect knowledge on the distribution of K given observation Y. This generally underestimates the practical GE for a non optimal attack because such a practical attack generally gives a suboptimal key ranking. Thus the results of this paper should yield adequate estimates only for optimal template attacks. The determination of more precise regions SR vs. GE for other types of attacks is a topic for future investigation.

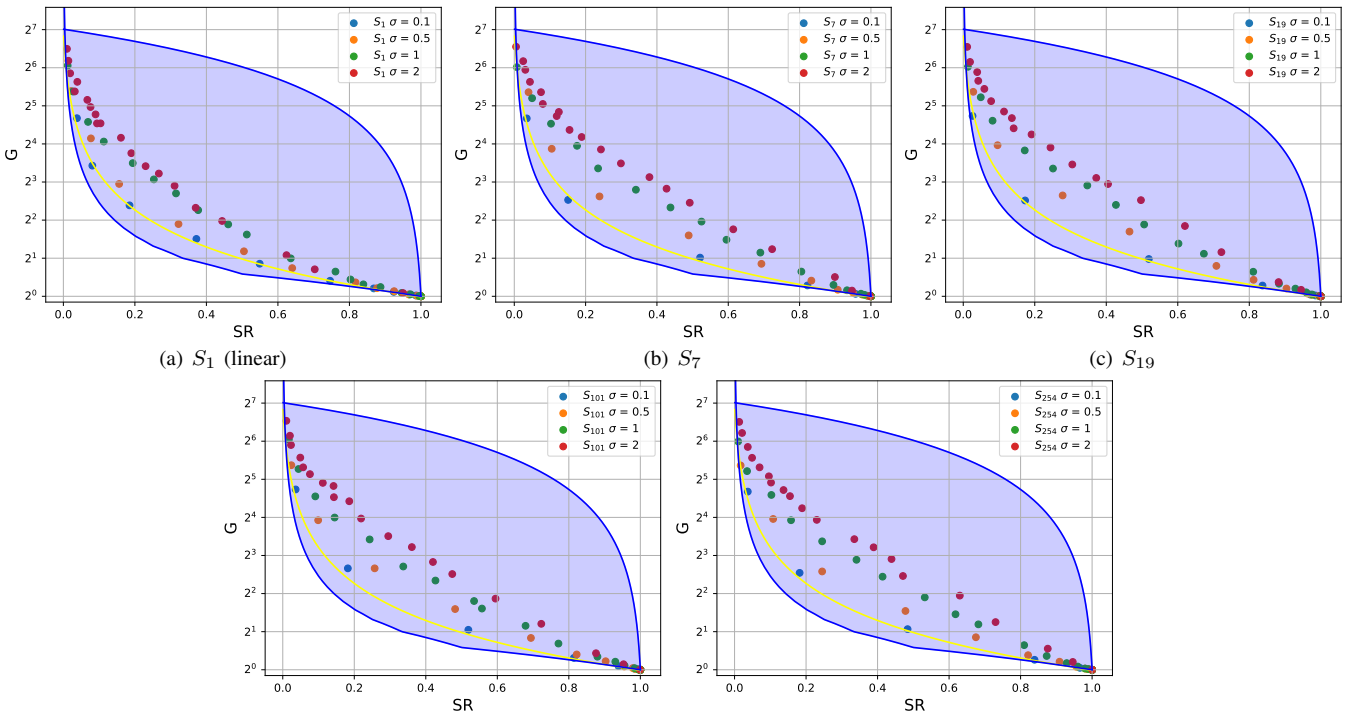
Acknowledgment: We thank anonymous reviewers for pointing out references [4], [12], [16].

References

[1] F.-X. Standaert, T. Malkin, and M. Yung, "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks," in *EUROCRYPT*, ser. LNCS, vol. 5479. Springer, April 26-30 2009, pp. 443–461, Cologne, Germany.

[2] N. Veyrat-Charvillon, B. Gérard, M. Renauld, and F.-X. Standaert, "An Optimal Key Enumeration Algorithm and Its Application to Side-Channel Attacks," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science, L. R. Knudsen and H. Wu, Eds., vol. 7707. Springer, 2012, pp. 390–406.

[3] N. Veyrat-Charvillon, B. Gérard, and F. Standaert, "Security evaluations beyond computing power," in *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, ser. Lecture Notes in Computer Science, T. Johansson and P. Q. Nguyen, Eds., vol. 7881. Springer, 2013, pp. 126–141. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-38348-9_8



(a) S_1 (linear) (b) S_7 (c) S_{19}

(d) S_{101} (e) S_{254} (AES – nonlinear)

Fig. 6. Numerical evaluation of SR and GE for various noise levels σ^2 and increasing number of traces, for various choices of S-Boxes. Each different subfigure corresponds to a choice for the S-Box. The yellow curve corresponds to GE$\approx$SR^{-1}, indicating at least for low noise, the GE is approximately the reciprocal of the SR. It can be observed that at a fixed SR the GE increases with the noise. This effect is amplified in the presence of a nonlinear S-Box.

[4] É. de Chérisey, S. Guilley, O. Rioul, and P. Piantanida, "Best Information is Most Successful — Mutual Information and Success Rate in Side-Channel Analysis," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2019, no. 2, pp. 49–79, 2019. [Online]. Available: https://doi.org/10.13154/tches.v2019.i2.49-79

[5] M. O. Choudary and P. G. Popescu, "Back to Massey: Impressively Fast, Scalable and Tight Security Evaluation Tools," in *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, ser. Lecture Notes in Computer Science, W. Fischer and N. Homma, Eds., vol. 10529. Springer, 2017, pp. 367–386. [Online]. Available: https://doi.org/10.1007/978-3-319-66787-4_18

[6] I. Sason and S. Verdú, "Improved Bounds on Lossless Source Coding and Guessing Moments via Rényi Measures," *IEEE Transactions on Information Theory*, vol. 64, no. 6, pp. 4323–4346, 2018.

[7] Z. Zhang, A. A. Ding, and Y. Fei, "A Fast and Accurate Guessing Entropy Estimation Algorithm for Full-key Recovery," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2020, no. 2, pp. 26–48, 2020. [Online]. Available: https://doi.org/10.13154/tches.v2020.i2.26-48

[8] G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*. Cambridge Univ. Press, 1934.

[9] A. W. Marshall, I. Olkin, and B. C. Arnold, *Inequalities: Theory of Majorization and Its Applications*, 2nd ed. Springer, 2011.

[10] S.-W. Ho and S. Verdú, "Convexity/Concavity of Rényi Entropy and α-Mutual Information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, China, June 14–19, 2015, pp. 745–749.

[11] R. Graczyk and I. Sason, "On Two-Stage Guessing," *Information*, vol. 12, no. 4, p. 159, 2021.

[12] M. Khouzani and P. Malacaria, "Generalized entropies and metric-invariant optimal countermeasures for information leakage under symmetric constraints," *IEEE Transactions on Information Theory*, vol. 65, no. 2, pp. 888–901, Feb. 2019.

[13] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 99–105, Jan. 1996.

[14] O. Rioul, "Variations on a theme by Massey," *IEEE Transactions on Information Theory*, vol. 68, no. 5, pp. 2813–2828, May 2022.

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

[16] A. Heuser, O. Rioul, and S. Guilley, "A Theoretical Study of Kolmogorov-Smirnov Distinguishers — Side-Channel Analysis vs. Differential Cryptanalysis," in *Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers*, ser. Lecture Notes in Computer Science, E. Prouff, Ed., vol. 8622. Springer, 2014, pp. 9–28. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-10175-0_2

[17] É. de Chérisey, S. Guilley, and O. Rioul, "Confused yet successful: - theoretical comparison of distinguishers for monobit leakages in terms of confusion coefficient and SNR," in *Information Security and Cryptology - 14th International Conference, Inscrypt 2018, Fuzhou, China, December 14-17, 2018, Revised Selected Papers*, ser. Lecture Notes in Computer Science, F. Guo, X. Huang, and M. Yung, Eds., vol. 11449. Springer, 2018, pp. 533–553. [Online]. Available: https://doi.org/10.1007/978-3-030-14234-6_28