One for All, All for One: A Unified Evaluation Framework for Univariate DPA Attacks

Jiangshan Long[1], Chenxu Wang[1], Changhai Ou[1], Zhu Wang[2], Yongbin Zhou[3], and Ming Tang[1]

[1] School of Cyber Science & Engineering, Wuhan University, Wuhan, Hubei 430072, China
longjiangshan@whu.edu.cn
wchenxu@whu.edu.cn
ouchanghai@whu.edu.cn
tangming@whu.edu.cn

[2] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
wangzhu@iie.ac.cn

[3] School of Cyber Science & Technology, Nanjing University of Science & Technology, Nanjing, Jiangsu 210094, China
zhouyongbin@njust.edu.cn

Abstract. Success Rate (SR) is one of the most popular security metrics measuring the efficiency of side-channel attacks. Theoretical expression reveals the functional dependency on critical parameters such as number of measurements and Signal-to-Noise Ratio (SNR), helping evaluators understand the threat of an attack as well as how one can mitigate it with proper countermeasures. However so far, existing works have exposed fundamental problems such as: (i) the evaluations are restricted to a very limited number of distinguishers and the methods in the literature seem specialized (i.e., hard to be extended). (ii) the evaluations assume an a-priori perfect leakage model which lacks practical relevance and ignores the fact that inaccurate profiling may lead to information loss and distorted SR. In this paper, we tackle above problems by providing an evaluation framework where different univariate DPA distinguishers are intuitively unified as linear maximum likelihood attack seeking for the closest '*distance*' between vectors in Euclidean space. We argue that this is an intrinsic property of the DPA mechanism and is independent of the leakage model. Then, we abstract the concept of SR and derive the theoretical expression in a geometric way. Finally, the theory allows a further study on leakage model where we formalize criterion explaining the impact of model errors as well as guaranteeing robust performance. We transfer the model effects to a degraded SNR parameter. Experimental results are inline with the theory, confirming that our theoretical expression coincides with the empirical ones.

Keywords: Success rate · side-channel evaluations · framework · DPA · side-channel attacks

1 Introduction

Unintentionally emitting from implementations, physical leakages such as power consumption [21, 24] and electromagnetic radiation [3, 17], break the traditional security model of cryptographic algorithms that assumes an adversary has only black box access to cryptosystem. These leakages statistically depend on intermediate values that are closely related to the secret key and therefore imply a new road for frustrating the protection. In the past decade, univariate DPA distinguishers including Bayes attack [38], Correlation Power Analysis (CPA) [37], Partition Power Analysis (PPA) [22] and Distance-of-Means (DoM) test together with its extensions [4, 21, 26, 27] have been proposed. After conquering varied cryptosystems in real world with unexpected simplicity and effectiveness, the question "to what extent my device is side-channel resistant and how to mitigate the threat?" has become a central one of concern.

For this purpose, SR is proposed as a security metric measuring the efficiency of turning leakages' information into a key recovery [35]. It comparatively evaluates how the effectiveness of side-channel attacks varies across different cryptographic algorithms, physical circuits and adversary's models, revealing which attack utilizes maximum information and which device is most vulnerable. To estimate SR, repeated experiments have been run and empirically univariate DPA attacks are found susceptible to statistical tests embedded, cryptographic properties of algorithm, characteristics of hardware implementation, number of measurements and priori knowledge on leakages. Such way comes with heavy computation loads. Hence, it raises an explicit requirement to figure out the underlying relationship among these factors theoretically so that constructive suggestions can be available for a more reasonable design of countermeasures that balances the implementation cost with the security improvement provided.

For a long time, evaluators pursued "worst case" evaluation where an hypothetical adversary can perfectly profile the leakage distribution (i.e., the leakage model accurately reflects the target device). However, practical constraints (e.g., how much time or how many measurements are allowed) indicate a critical problem that all adversaries potentially expose themselves to some biased models. This intuition was first detailed in [30] and later systematacially studied in [12] [13], putting forward the concepts of leakage certification. Weak keys from the perspective of an inaccurate model should be different from those suggested by the perfect one. So, it is still necessary to evaluate the overall security level of such more practical scenarios and quantify the information loss (an open problem in [12]). We believe they bring new perspectives for evaluators.

1.1 Related Works

Exact expressions of SR have been investigated. Under the assumption of nullity of wrong candidates' correlation coefficients and using Fisher's Z-transformation, [23] simply targeted at CPA on a candidate pair and carried out an early study against SR, which was later extended to candidate set of any size in [36]. In

subsequent works, [16] for DoM and [31] for CPA and multivariate Bayes attack argued that the assumption was not always satisfied. They launched direct analysis and found DPA attacks can be approximated using a multivariate normal cumulative distribution function. Pursuing heuristic of full-key recovery, [37] studied a variant of SR (defined as confidence) for CPA in terms of key rank evolution. Specific to distinguishers, these proposed methods suffer from a lack of generality and fail to disclose the potential relationship between DPA attacks. [15] took a logarithm of Bayes attack and by the central limit theorem suggested a statistic model. Combining the maximal likelihood estimation under linear regression model with the propositions in [10], they unified CPA and DoM as equivalent Bayes attacks with unknown system parameters. Though much more effective, the evaluations are still limited to three distinguishers and known-model scenarios. Seeking the breakthrough is challenging.

Closed-form expressions of SR based on the so called Success Exponent (SE) were given by [20]. They exhibited a more explicit functional relationship of the SR with relevant parameters meanwhile extended the evaluation from additive distinguishers (e.g., CPA and DoM) to non-additive Mutual Information Analysis (MIA) [18]. However, the built-in central limit theorem presents soundness only under the asymptotic condition that adversary tends to sample a large number of measurements. Besides, squeezing the overall SR by pairwise event (originally suggested as an evaluation framework in [40]) avoids high-dimensional complexity of interaction between incorrect keys but may become invalid when SNR is low. We will illustrate this issue in Subsection 4.2. Since the central limit theorem again leads to Gaussian distribution, similar to the exact expression of SR where no closed-form expression exists, they exploited a weak equivalence preserving the same exponential convergence behavior of SR toward 1.

Heuristic expressions of SR were developed in [41]. The author re-expressed the statistic model in [15] as a noise vector stretched in the directions of orthonormal eigenvectors of a key-dependent matrix, with the corresponding eigenvalues as factors. As a heuristic approximation, he replaced those eigenvalues by a constant that maintains the norm of the product. This allows reducing the high-dimensional complexity to a two-dimensional integral. Apparently, the method requires the eigenvalues do not vary too much. Moreover, the expressions of eigenvectors become valid only when leakages depend on the input of target cryptographic operation which may not be the case in practice.

Recent works linked SR with information theory. Authors in [9] regarded side-channel as communication channel and established a Markov chain where data processing inequality is available to bound the SR with Shannon's mutual information between leakages and model. Their result was universal but hardly concerned side-channel resistance of cryptographic algorithm as they concluded that SNR was sufficient enough to predict the security level of an implement under Gaussian noise.

1.2 Our Contributions

In this paper our contributions are as follows:

- We propose a unified framework which facilitates an in-depth discussion about to which extent different attacks share a common theoretical basis. The framework covers a total of 7 popular univariate DPA attacks (much more than existing works) and captures both profiled model and leakage distribution, meanwhile being specific enough for us to make concrete statements and sound comparison. We show that these attacks can be unified as testing vectors in Euclidean space but resorting to different easy-to-understand geometrical metrics.
- Based on the framework, we present the concepts of "*success boundary*" and "*success space*" to reveal the linear aspect of univariate DPA attacks. We demonstrate a theoretical derivation of SR where the interference of profiled model and physical leakages is decoupled. The adversary's model determines the shape of success boundary whereas the leakage distribution accounts for the probability density of the surrounded success space. It allows an easy quantification of information loss from the aspect of decayed SR.
- At last, we answer two interesting problems about the leakage model: (1) Exchanging the models of adversary and device, will it result in the same SR? (2) When model errors are enough to distort SR? Based on our theoretical expression, we formalize the criterion showing that univariate DPA attack with a profiled model is equivalent to that with a perfect one but decreased SNR. The reduction factor can be well expressed by an easy extension of the proposed confusion coefficients in the literature. It helps us explain and guarantee robust performance.

1.3 Organization

This paper is organized as follows: preliminaries including leakage model, confusion coefficient, CPA, PPA, Bayes attack, and DoM together with its extensions are introduced in Section 2. Descriptions of our evaluation framework, the intuitive expressions of univariate DPA attacks and experiments on software implementation are detailed in Section 3. We then theoretically analyze the SR in Section 4. Experiments on hardware implementation are presented in Sections 5. Finally, we conclude this paper in Section 6.

2 Preliminaries

2.1 Side-channel Leakages and Leakage Model

Following the divide-and-conquer strategy, univariate side-channel DPA attacks consider the secret as a tuple of subkeys and recover them separately. Let k^* denote the target subkey selected at random from a set $\mathcal{K} : k^* \xleftarrow{R} \mathcal{K}$, k denote any possible guessing value and $\bar{\mathcal{K}}$ denote the subset: $\bar{\mathcal{K}} = \mathcal{K} \backslash \{k^*\} = \{k^{[1]}, \cdots, k^{[S]}\}$. Let t denote the plaintext byte selected at random from another set $\mathcal{T} : t \xleftarrow{R} \mathcal{T}$. Cryptographic algorithm keeps to group operation for closure property (e.g., all computations in AES take place on Galois field $\mathbb{F}_2^8$). Let $\mathbf{Im} = \mathcal{G}(t, k^*)$ denote

such operation and **Im** is the n-bit key-dependent intermediate variable whose distribution over $\mathcal{T}$ is identical for any $k \in \mathcal{K}$ which gives no evidence about the secret k^* (see [10, 20, 25, 29] for similar observations). The leakage function $\mathcal{F}$ is a discrete function describing the physical signal (e.g., voltage for power consumption leakage) leaked during the computation of $\mathcal{G}$. Let x denote the leakage measurement and it can be expressed as:

$$x = \mathcal{F} \circ \mathcal{G}(t, k^*) + \mathsf{N} = \varphi\left(t, k^*\right) + \mathsf{N}. \tag{1}$$

Composite function φ is the leakage model and N is the independent Gaussian noise with $\mathbb{D}\{\mathsf{N}\} = \sigma_N^2$. Both the cryptographic property of algorithm and the physical characteristic of underlying hardware circuits determine the resistance of an implement against univariate side-channel attacks. This intuition is captured by $\mathcal{G}$ and $\mathcal{F}$ respectively in this paper and we do not assume any restrictions on them to make our results well applied to any scenario. At last, let $\hat{\varphi}$ denote the adversary's counterpart in real attack which may be biased by model errors.

2.2 Confusion Coefficient

Cryptographic algorithms are designed to be robust against cryptanalysis with two well-known statistical properties [33]: confusion and diffusion. Confusion makes the statistical relation between the ciphertext and secret key as complex as possible while diffusion makes the statistical relation between the ciphertext and plaintext as complex as possible. Proposed in [16] and latter refined in [15], confusion coefficient generalizes the confusion property to the field of side-channel attack by coupling $\mathcal{G}$ and $\mathcal{F}$. That is, for two subkey candidates (k_i,k_j), outputs of $\varphi\left(t, k_i\right)$ and $\varphi\left(t, k_j\right)$ behave differently over the same plaintext byte t. We abbreviate these variables as $\varphi|k_i$ and $\varphi|k_j$ and the extent to which they are different from each other determines the difficulty of distinguishing them using side-channel leakages. For this purpose, the general two-way confusion coefficient is defined as the averaged squared distance:

$$\kappa(k_i, k_j) = \mathbb{E}_t\{(\varphi(t, k_i) - \varphi(t, k_j))^2\} = \mathbb{E}\{(\varphi|k_i - \varphi|k_j)^2\}. \tag{2}$$

2.3 Difference-of-Means Attack

Abbreviated as DoM, Difference-of-Means attack targeting a single bit of **Im** is the first proposed univariate side-channel attack [21]. It is soon extended to multiple bits in two ways: the *all-or-nothing* DoM and the *generalized* DoM [26,27], to overcome some algebraic property that leads to failure in the mono-bit setting. Referring to [10], we denote these strategies as SB-DoM, AON-DoM and G-DoM respectively. DoM classifies measurements into two categories according to a partition of the range of $\hat{\varphi}$. We denote the partition by $\mathbf{\Omega_{DoM}} = \{\Omega_0, \Omega_1\}$. Leakages bundled together are deemed to share the same distribution. Difference of means is calculated to verify k since incorrect candidates will lead to misclassifications where measurements assigned to the same category actually approach

random. Let Q denote the total number of measurements and q denote a certain encryption. Let $\mathbf{Im}[i]$ denote the i-th bit. The distinguishers $\mathbf{D}_{\mathsf{SB-DoM}}(\mathbf{Im}[i])$, $\mathbf{D}_{\mathsf{AON-DoM}}(\mathbf{Im}[1:n])$ and $\mathbf{D}_{\mathsf{G-DoM}}(\mathbf{Im}[1:n])$ can be written uniformly:

$$\begin{aligned}&\mathbf{D}_{\mathsf{SB-DoM}}(\mathbf{Im}[i]) \simeq \mathbf{D}_{\mathsf{AON-DoM}}(\mathbf{Im}[1:n]) \simeq \mathbf{D}_{\mathsf{G-DoM}}(\mathbf{Im}[1:n])\\ &= \hat{\mathbb{E}}\{x_{q|\hat{\varphi}(t_q,k)\in\Omega_1}\} - \hat{\mathbb{E}}\{x_{q|\hat{\varphi}(t_q,k)\in\Omega_0}\} = \frac{\sum_{q|\hat{\varphi}(t_q,k)\in\Omega_1}^{Q} x_q}{\sum_{q|\hat{\varphi}(t_q,k)\in\Omega_1}^{Q} 1} - \frac{\sum_{q|\hat{\varphi}(t_q,k)\in\Omega_0}^{Q} x_q}{\sum_{q|\hat{\varphi}(t_q,k)\in\Omega_0}^{Q} 1}.\end{aligned} \tag{3}$$

Taking Hamming weight leakage function and $i = n$ (i.e., the least significant bit) as an example, the range $R(\hat{\varphi}) = \{0, 1, \cdots, n\}$. The partition is typically chosen as: $\mathbf{\Omega_{SB-DoM}} = \{\{\hat{\varphi}|\mathbf{Im}\%2 = 0\}, \{\hat{\varphi}|\mathbf{Im}\%2 = 1\}\}$, $\mathbf{\Omega_{AON-DoM}} = \{0, n\}$, $\mathbf{\Omega_{G-DoM}} = \{\{0, \cdots, \lfloor \frac{n}{2} \rfloor\}, \{\lceil \frac{n}{2} \rceil, \cdots, n\}\}$. Referring to the central-limit theorem, it is not hard to find that if SNR of the leakage x is decreased to $1/\beta$, Q has to be multiplied by β for DoM to achieve the same performance.

2.4 Correlation Power Analysis and Partition Power Analysis

Abbreviated as CPA, correlation power analysis is a popular side-channel distinguisher identifying k^* by assessing the linear fitting rate between the model and measurements. It implicitly extends the binary classification of DoM to a multiple one by incorporating the well-known Pearson's correlation coefficient:

$$\begin{aligned}&\mathbf{D}_{\mathsf{CPA}}(\mathbf{Im}[1:n]) = \arg\max_{k\in\mathcal{K}} \ \rho(x_{q=1,\ldots,Q}, \hat{\varphi}(k, t_{q=1,\ldots,Q}))\\ &= \arg\max_{k\in\mathcal{K}} \ \frac{\hat{\mathbb{E}}\{x_q \times \hat{\varphi}(t_q,k)\} - \hat{\mathbb{E}}\{x_q\} \times \hat{\mathbb{E}}\{\hat{\varphi}(t_q,k)\}}{\sqrt{\hat{\mathbb{D}}\{x_q\}} \times \sqrt{\hat{\mathbb{D}}\{\hat{\varphi}(t_q,k)\}}}.\end{aligned} \tag{4}$$

This notion of multi-classification was latter explicitly formalized in [22] by introducing the partition power analysis (abbreviated as PPA):

$$\begin{aligned}&\mathbf{D}_{\mathsf{PPA}}(\mathbf{Im}[1:n]) = \arg\max_{k\in\mathcal{K}} \ \sum_{i}^{m} \alpha_i \times \hat{\mathbb{E}}\{x_{q|\hat{\varphi}(t_q,k)\in\Omega_i}\}\\ &= \arg\max_{k\in\mathcal{K}} \ \sum_{i}^{m} \alpha_i \times \frac{\sum_{q|\hat{\varphi}(t_q,k)\in\Omega_i}^{Q} x_q}{\sum_{q|\hat{\varphi}(t_q,k)\in\Omega_i}^{Q} 1},\end{aligned} \tag{5}$$

where $m \geq 2$ denotes the number of partitions and $\mathbf{\Omega_{PPA}} = \{\Omega_0, \Omega_1, \cdots, \Omega_m\}$. Coefficients α_i's are real constants to be determined. Once again taking Hamming weight leakage function as an example, the parameters above can be chosen as (see Equ.(7) in [22]): $\mathbf{\Omega_{PPA}} = \{0, 1, \cdots, n\}, \alpha_i = \frac{C_n^i}{2^n} \times (i - \sum_{j=0}^{n} \frac{C_n^j}{2^n} \times j)$. It is further argued in [10] that CPA and PPA are asymptotically equivalent.

2.5 Bayes Attack and Summing DoM

Adopting the maximum likelihood method, Bayes attack calculates a probability density function with k serving as the parameter to be estimated. It is regarded as

optimal in general whenever a-priori knowledge about the leakage is available [7, 8, 19]. Given measurement set, selecting the most likely subkey candidate can be expressed by the following conditional probability:

$$\mathbf{D}_{\mathsf{Bayes}}(\mathbf{Im}[1:n]) = \arg\max_{k\in\mathcal{K}} \prod_{q=1}^{Q} \mathbb{P}\{k|x_q\} = \arg\max_{k\in\mathcal{K}} \prod_{q=1}^{Q} \mathbb{P}\{x_q|k\}. \tag{6}$$

The proof is given in [34] by stripping off the key-independent terms from the Bayes formula. At last, the idea of summing distinguishers to define a new one has been proposed in [4] where the authors performed the SB-DoM for each bit of $\mathbf{Im}$ and then summed the results. We denote this attack as M-DoM and it is straightforwardly defined as:

$$\mathbf{D}_{\mathsf{M-DoM}}(\mathbf{Im}[1:n]) = \arg\max_{k\in\mathcal{K}} \sum_{i=1}^{n} \mathbf{D}_{\mathsf{SB-DoM}}(\mathbf{Im}[i]). \tag{7}$$

Contrary to the other DoM-s, M-DoM implicitly applies a multi-classification just like CPA, PPA and Bayes attack, which will be detailed in Subsection 3.4.

3 Geometrical Framework for Univariate DPA Attacks

In this section, we propose a framework to present an intuitive explanation of the mathematical foundation behind univariate DPA attacks, putting understanding of their differences and relationship to a higher degree.

3.1 Leakage Space

Geometrical system is an ideal tool for complexity reduction. Based on this, we introduce leakage space $\mathcal{V}$ as a framework and intuitively unifies univariate DPA distinguishers as maximum likelihood attack (ML-attack).

Definition 1. *The leakage space $\mathcal{V}$ is an Euclidean space of real number whose dimension equals to the number of measurements, i.e., $\mathcal{V} = \mathbf{R}^Q$. The measurement set X is represented by a random point $\mathcal{X} = (x_1, x_2, \ldots, x_Q)$. The mathematical expectation of $\mathcal{X}$ is mapped to a fixed point $\Theta = (\varphi(t_1, k^*), \ldots, \varphi(t_Q, k^*))$.*

Lemma 1. *Since the Gaussian noise N adding to each dimension of $\mathcal{X}$ is identical and mutually independent, the probability density function ϕ in $\mathcal{V}$ becomes:*

$$\begin{aligned} \phi(\mathcal{X}) &= \left(\frac{1}{\sqrt{2\pi}\times\sigma_N}\right)^Q \times \exp\left(-\frac{1}{2\times\sigma_N^2} \times \textstyle\sum_{q=1}^{Q} (x_q - \varphi(t_q, k^*))^2\right) \\ &= \left(\frac{1}{\sqrt{2\pi}\times\sigma_N}\right)^Q \times \exp\left(-\frac{r^2}{2\times\sigma_N^2}\right), \end{aligned} \tag{8}$$

which turns out to be a univariate function of the L2 norm $r = ||\vec{\mathcal{X}} - \vec{\Theta}||$.

Let $\mathcal{D}(A, B)$ denote some kind of distance metric between A and B in $\mathcal{V}$. The procedure of univariate DPA attacks is intuitive: To achieve the goal of key recovery, the adversary samples an instance $\hat{\mathcal{X}}$. By Lemma 1 and Chebyshev's inequality, he knows that $\hat{\mathcal{X}}$ isotropically centers around its expectation Θ and won't be too far from it (i.e., $\mathcal{D}(\hat{\mathcal{X}}, \Theta)$ is short). Specifically, $\forall 1 \leq q \leq Q, \mathbb{P}\{|x_q - \varphi(t_q, k^*)| \geq c\} \leq (\frac{\sigma_N}{c})^2$. Hence, the adversary then gets an estimation of Θ with his profiled model $\hat{\varphi}$ as $\xi(k) = (\hat{\varphi}(t_1, k), \ldots, \hat{\varphi}(t_Q, k))$ whose confidence level naturally relates to the distance metric $\mathcal{D}(\hat{\mathcal{X}}, \xi(k))$. In the following, we will show that such metric in the DoM family, CPA, PPA and Bayes attack amount to vector projection, vector cosine, vector projection and Euclidean distance respectively. Anyhow, the behavior of seeking the closest distance $\arg\min_{k \in \mathcal{K}} \mathcal{D}(\hat{\mathcal{X}}, \xi(k))$ unambiguously suggests that all univariate DPA attacks are ML-attack. In the rest of paper, descriptions of target (e.g., $\mathbf{Im}[i]$) will be omitted when not necessary.

3.2 Bayes attack

In leakage space $\mathcal{V}$, Bayes distinguisher measures the distance metric:

$$\mathcal{D}_{\mathsf{Bayes}}(\mathcal{X}, \xi(k)) = \prod_{q=1}^{Q} \mathbb{P}\{x_q | k\} = \prod_{q=1}^{Q} f_{\hat{\sigma}_N^2}(x_q - \hat{\varphi}(t_q, k)) = ||\vec{\mathcal{X}} - \vec{\xi}(k)||^2. \quad (9)$$

Here $f_{\hat{\sigma}_N^2}$ is the Gaussian density function with a zero mean and estimated standard deviation $\hat{\sigma}_N$.

Lemma 2. *Bayes distinguisher is a ML-attack selecting candidates according to the Euclidean distance geometrical metric. Candidate k that corresponds to the minimum distance $||\vec{\mathcal{X}} - \vec{\xi}(k)||$ will be regarded as the secret subkey.*

From the adversary's aspect, $\mathcal{X}$ mostly takes a random walk in neighborhood $U(\xi(k^*))$. The probability that $\mathcal{X}$ happens to reach and be observed in another neighborhood $U(\xi(k^\circ))$, and thereafter is closer to $\xi(k^\circ)$, is relatively low. Regarded as "optimal", Bayes distinguisher captures the nature of $\mathcal{X}$ (i.e., the L2 norm in Lemma 1). We provide Fig. 1 for illustration which leaves us an intuitive impression of what the effectiveness of Bayes attack rests with and how. Specifically, the overlapped parts between neighborhoods confuse and mislead the distinguisher. Factors affecting this overlapped space are the size of neighborhood determined by variance of the electronic noise (i.e., σ_N^2) and the Euclidean distance between neighborhood centers $||\vec{\xi}(k^*) - \vec{\xi}(k^\circ)||$. For the latter, confusion coefficient on (k^*, k°), also illustrated in Fig. 1, quantifies its extent (averaged to one dimension): $\hat{\kappa}(k^*, k^\circ) = \mathbb{E}\{(\hat{\varphi}|k^* - \hat{\varphi}|k^\circ)^2\} = \mathbb{E}\{\frac{||\vec{\xi}(k^*) - \vec{\xi}(k^\circ)||^2}{Q}\}$.

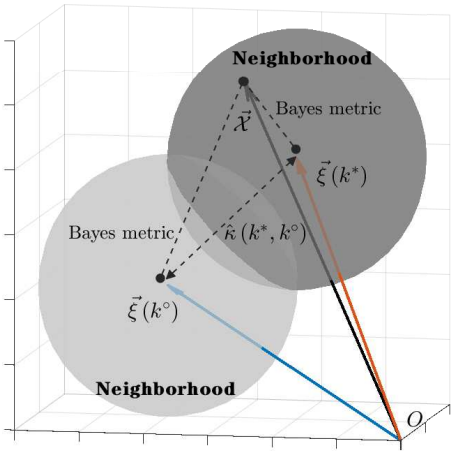

Fig. 1: A sketch map of Bayes metrics.

3.3 CPA and PPA

Let $a = \frac{||\vec{\mathcal{X}}||_1}{||\vec{\mathcal{X}}||_2}$ and $b(k) = \frac{||\vec{\xi}(k)||_1}{||\vec{\xi}(k)||_2}$, Pearson's correlation coefficient presents a linear relation with Salton's cosine measure (i.e., see Equ.(13) in [14]):

$$\begin{aligned}\mathcal{D}_{\mathsf{CPA}}(\mathcal{X}, \xi(k)) &= \rho(x_{q=1,\ldots,Q}, \hat{\varphi}(k, t_{q=1,\ldots,Q})) \\ &= \frac{Q}{\sqrt{Q-a^2} \times \sqrt{Q-b^2(k)}} \times (cos < \vec{\mathcal{X}}, \vec{\xi}(k) > - \frac{a \times b(k)}{Q}).\end{aligned} \tag{10}$$

Due to the closure property of $\mathcal{G}$, the leakage model $\varphi|k$ maintains the same distribution over plaintext byte for any $k \in \mathcal{K}$, i.e., $\mathbb{E}\{\varphi|k^*\} = \mathbb{E}\{\varphi|k \in \bar{\mathcal{K}}\}$, $\mathbb{D}\{\varphi|k^*\} = \mathbb{D}\{\varphi|k \in \bar{\mathcal{K}}\}$. Thus, we ignore the subtle statistical differences between sample moments, from which no information can be extracted, and simplify CPA distinguisher as:

$$\mathcal{D}_{\mathsf{CPA}}(\mathcal{X}, \xi(k)) = cos < \vec{\mathcal{X}}, \vec{\xi}(k) > . \tag{11}$$

Lemma 3. *CPA distinguisher is a ML-attack selecting candidates according to the vector cosine geometrical metric. Candidate k that corresponds to the maximum cosine $cos < \vec{\mathcal{X}}, \vec{\xi}(k) >$ will be regarded as the secret subkey.*

Owing to the relationship with CPA, the distance metric in PPA is easily derived and simplified in the same way (i.e., by getting rid of the effect of the sample moments in correlation coefficient):

$$\mathcal{D}_{\mathsf{PPA}}(\mathcal{X}, \xi(k)) = \hat{\mathbb{E}}\{x_q \times \hat{\varphi}(t_q, k)\} = \mho < \vec{\mathcal{X}}, \vec{\xi}(k) >, \tag{12}$$

where $\mho < \vec{\mathcal{X}}, \vec{\xi}(k) >$ denotes the vector projection of $\vec{\xi}(k)$ on $\vec{\mathcal{X}}$.

Lemma 4. *PPA distinguisher is a ML-attack selecting candidates according to the vector projection geometrical metric. Candidate k that corresponds to the maximum projection $\mho < \vec{\mathcal{X}}, \vec{\xi}(k) >$ will be regarded as the secret subkey.*

3.4 DoM and Summing DoM

Inspired from [25], we rewrite Equ.(3) and re-express DoM as follows:

$$\mathbf{D}_{\mathsf{SB-DoM}}(\mathbf{Im}[i]) \simeq \mathbf{D}_{\mathsf{AON-DoM}}(\mathbf{Im}[1:n]) \simeq \mathbf{D}_{\mathsf{G-DoM}}(\mathbf{Im}[1:n]) = \frac{\sum_{q=1}^{Q} x_q \times \mathbf{Sgnx}(|\prod_{\lambda\in\Omega_0}(\hat{\varphi}(t_q,k)-\lambda)|)}{\sum_{q=1}^{Q}\mathbf{Sgnx}(|\prod_{\lambda\in\Omega_0}(\hat{\varphi}(t_q,k)-\lambda)|)} - \frac{\sum_{q=1}^{Q} x_q \times \mathbf{Sgnx}(|\prod_{\lambda\in\Omega_1}(\hat{\varphi}(t_q,k)-\lambda)|)}{\sum_{q=1}^{Q}\mathbf{Sgnx}(|\prod_{\lambda\in\Omega_1}(\hat{\varphi}(t_q,k)-\lambda)|)}. \tag{13}$$

The step function $\mathbf{Sgnx}(.)$ is defined as:

$$\mathbf{Sgnx}(y) = \begin{cases} 0, & \text{if } y \le 0 \\ \\ 1, & \text{else} \end{cases} \tag{14}$$

Due to the diffusion property of cryptographic algorithm, each bit in the ciphertext approaches purely random [16]. As a consequence, the number of measurements in each category of the binary classification is close and tends to be the same as Q increases. Ignoring the trivial discrepancies and let $\hat{\psi}(t_q,k) = \mathbf{Sgnx}(|\prod_{\lambda\in\Omega_0}(\hat{\varphi}(t_q,k)-\lambda)|) - \mathbf{Sgnx}(|\prod_{\lambda\in\Omega_1}(\hat{\varphi}(t_q,k)-\lambda)|)$ be the profiled model of the three discussed DoM-s, we withdraw vector $\vec{\epsilon}(k) = (\hat{\psi}(t_1,k), \cdots, \hat{\psi}(t_Q,k))$ from Equ.(13) to have the distance metric:

$$\mathcal{D}_{\mathsf{SB-DoM}}(\mathcal{X}, \xi(k)) \simeq \mathcal{D}_{\mathsf{AON-DoM}}(\mathcal{X}, \xi(k)) \simeq \mathcal{D}_{\mathsf{G-DoM}}(\mathcal{X}, \xi(k)) = \mho < \vec{\mathcal{X}}, \vec{\epsilon}(k) > . \tag{15}$$

Apparently, $\hat{\psi}$ takes integers ± 1 for SB-DoM and G-DoM which corresponds to their non-overlapping binary partition. In contrast, AON-DoM divides $R(\hat{\varphi})$ into three partitions (i.e., the maximum value, the minimum value and the rest). Those medium values contribute no measurements to the difference-of-means test so their corresponding outputs of the step function remain 0 all the time. In this case, $\hat{\psi}$ takes integers within $\{-1, 0, 1\}$. For convenience, in this paper we only use the maximum and minimum values to represent the partition of AON-DoM. At last, the distance metric of the summing distinguisher M-DoM is easily obtained by extending Equ.(13) to multiple bits:

$$\mathcal{D}_{\mathsf{M-DoM}}(\mathcal{X}, \xi(k)) = \mho < \vec{\mathcal{X}}, \vec{\epsilon'}(k) > . \tag{16}$$

Here $\vec{\epsilon'}(k) = (\hat{\psi}'(t_1,k), \cdots, \hat{\psi}'(t_Q,k))$ and $\hat{\psi}'(t_q,k) = \sum_{\mathbf{Im}[i]} \hat{\psi}(t_q,k)$ is the profiled model of M-DoM which is the simple sum of mono-bit models of SB-DoM. The model $\hat{\psi}'$ takes integers within $[-n, n]$ because of the positive and negative interference of the same leakage sample for different bits of $\mathbf{Im}$, indicating that M-DoM in itself classifies the leakages into at most $2n+1$ categories.

Lemma 5. *DoM is ML-attack selecting candidates according to the vector projection geometrical metric. Candidate k that corresponds to the maximum projection $\mho < \vec{\mathcal{X}}, \vec{\epsilon}(k) >$ ($\mho < \vec{\mathcal{X}}, \vec{\epsilon}^{'}(k) >$) will be regarded as the secret subkey.*

For CPA, PPA and Bayes attack, large cosine or small distance leads to large projection, agreeing with their close performance in practice. We offer Fig. 2 as a summary. By contrast, the DoM family shares a same projection metric. From these perspectives, the DoM family is in essence equivalent to the others except for replacing the concrete model values in $\xi(k)$ by some integers. In other words, the DoM-s additionally map $\xi(k)$ to a simplified counterpart $\epsilon(k)$ ($\epsilon^{'}(k)$) through the step function **Sgnx**. In the next subsection, we will experimentally verify the similar behaviors of the three distance metrics on real leakages and elaborate how to partition the range of leakage model $\hat{\varphi}$ to determine the profiled model of the DoM family (i.e., $\hat{\psi}$ and $\hat{\psi}'$) straightforwardly.

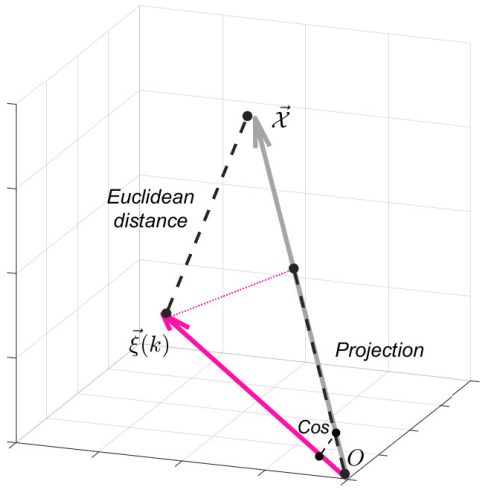

Fig. 2: The three distance metrics in univariate DPA attack.

3.5 Univariate DPA Attacks against Software Implementation

We sampled real leakages from a PRESENT algorithm implemented on an ATMega328p micro-controller whose clock frequency is 16 MHz. We applied a WaveRunner 8104 oscilloscope with a sampling rate of 1 GS/s. As a preliminary, we performed the HW ρ-test [11] to select the time sample named Point-Of-Interest (POI) which is illustrated in Fig. 3. It corresponds to the first S-box

($\mathbb{F}_2^4 \to \mathbb{F}_2^4$) of the first round encryption. The adversary was assumed to have $16 \times m$ measurements for model profiling and estimate the leakage model as $\hat{\varphi}(y) = \hat{\mathbb{E}}\{x_{q|\mathrm{Sbox}(k\oplus t_q)=y}\}$ which had been argued in [24,29] that maximized the attack efficiency. In the experiments, we controlled model errors by adjusting m.

In our first experiment, we set m to 1, 5 and 10000 consecutively to examine whether CPA, PPA and Bayes attack always approach each other (i.e., this property of distance metrics is independent of the leakage model). For convenience, we list the values of model $\hat{\varphi}$ in Table 1 by the order of intermediate variable $\mathbf{Im} = \mathrm{Sbox}(t \oplus k^*)$ to exhibit some possible rule of the power consumption. As we can see, the leakages in overall decrease with the Hamming weight of **Im** which accords with the negative spike of the selected POI. Experimental results are displayed in Fig.4. The cosine, projection and Euclidean distance metric show very similar performance even if the profiled model of adversary becomes terrible (e.g., for $m = 1$ the profiled model losses its proper prediction of the real leakages and the distorted success rates decrease with the number of measurements Q). Capturing the behaviors by a unified expression is well founded.

In our second experiment, we first partition the range of leakage model $\hat{\varphi}$ by looking at Table 1 to obtain the profiled model $\hat{\psi}$ ($\hat{\psi}'$) of the DoM family. We take the fewest profiling measurement case (i.e., largest model errors) as the example (i.e., $m = 1$ the first row of Table 1) and list the partition results in Table 2,3. For SB-DoM, the target is chosen as the least significant bit so we just have to partition $\hat{\varphi}$ in terms of odd and even number of **Im** and then compare the averaged model values. Those corresponding to the smaller mean will all be mapped to -1 while the rest are left to $+1$. For AON-DoM and G-DoM, we sort the model values. AON-DoM only cares about the maximum and minimum values which are the two partitions and mapped to integers ± 1. The others are set to 0. By contrast, G-DoM splits the sorted model values in half from the middle. All the eight maximum values are mapped to $+1$ whereas all the eight minimum values are mapped to -1. The model of the multi-classification M-DoM is the sum of SB-DoM's binary model values on every bit of **Im**.

Then, we apply the DoM-s to the same measurement set as our first experiment and the results are given in Fig.5. To better understanding the relationship of univariate DPA distinguishers and in view of the popularity of CPA, we conduct the DoM-s in two ways: (i) The original way of performing difference-of-means where leakages are classified based on the partitions of Table 2 (M-DoM is instantiated with 4 SB-DoM-s). (ii) Calculating Pearson's correlation coefficient using model $\hat{\psi}$ ($\hat{\psi}'$) in Table 3. The latter is marked with superscript "†" in the figure. As shown, the two schemes achieve almost the same performance in all cases, backing up our reasoning that the DoM family is essentially identical to CPA, PPA and Bayes attack except for replacing the concrete model values by some integers. It's also worth noting that M-DoM seem more robust in the experiment because only one of the four SB-DoM's profiled models goes wrong.

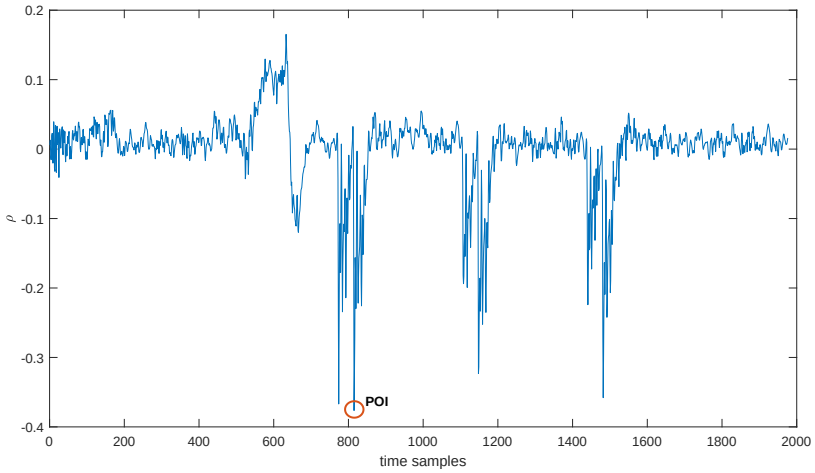

Fig. 3: The selected POI from the real leakages of the ATmega328p micro-controller.

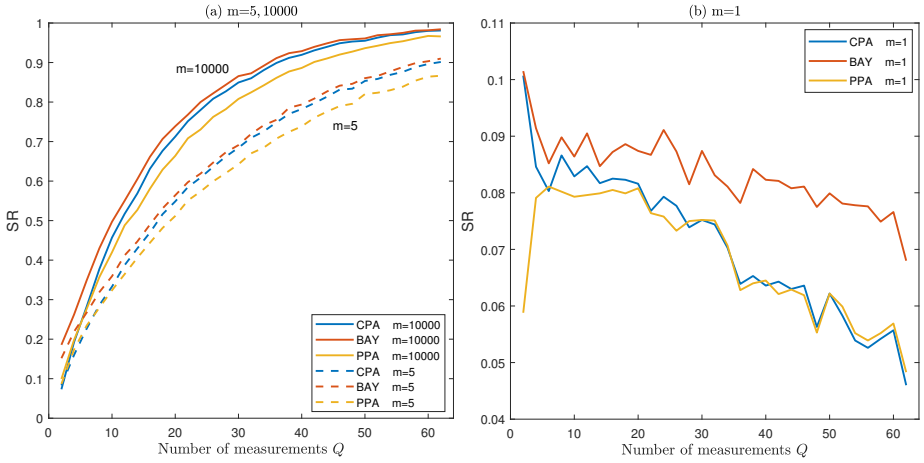

Fig. 4: CPA, PPA and Bayes attack on the ATMega328p micro-controller.

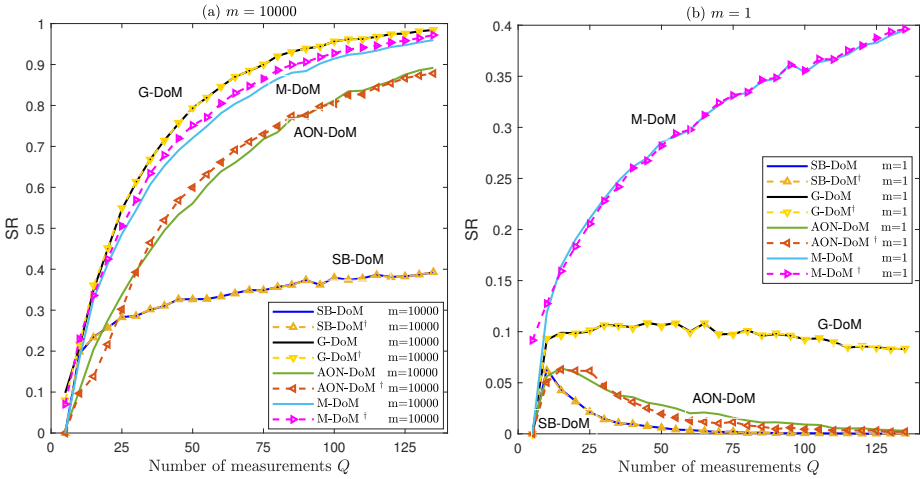

Fig. 5: Performance of the DoM family on the ATMega328p micro-controller.

Table 1: Leakage models (10^{-2}) on different number of profiling measurements.

$\hat{\varphi}$ \ **Im** / m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1.68	1.73	1.55	1.73	1.59	1.73	1.55	1.64	1.68	1.55	1.55	1.55	1.46	1.37	1.55	1.51
5	1.66	1.67	1.57	1.56	1.64	1.59	1.57	1.54	1.55	1.55	1.58	1.59	1.52	1.51	1.59	1.45
10000	1.63	1.63	1.59	1.54	1.61	1.57	1.56	1.51	1.51	1.56	1.59	1.54	1.57	1.56	1.55	1.48

Table 2: Partitions of $R(\hat{\varphi})$ under $m = 1$.

	Ω
SB-DoM	{{1.68,1.55,1.59,1.55,1.68,1.55,1.46,1.55}, {1.73,1.73,1.73,1.64,1.55,1.55,1.37,1.51}}
AON-DoM	{{1.37},{1.73}}
G-DoM	{{1.37,1.46,1.51,1.55,1.55,1.55,1.55,1.55}, {1.55,1.59,1.64,1.68,1.68,1.73,1.73,1.73}}
M-DoM	{{1.55},{1.55,1.55,1.46,1.51},{1.55,1.59,1.64,1.68,1.55,1.37}, {1.68,1.73,1.73,1.55},{1.73}}

Table 3: Leakage models (10^{-2}) of the DoM family under $m = 1$.

$\hat{\psi}(\hat{\psi}')$ \ **Im** / DoM	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
SB-DoM	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1
AON-DoM	0	0	0	0	0	1	0	0	0	0	0	0	0	-1	0	0
G-DoM	1	1	-1	1	1	1	-1	1	1	-1	-1	-1	-1	-1	1	-1
M-DoM	2	4	0	2	0	2	-2	0	0	2	-2	0	-2	0	-4	-2

4 Geometrical Evaluation of Univariate DPA Attacks

In the last section, we concluded that univariate DPA attacks boiled down to ML-attack. In this section, we reveal the linear aspect of them and derive a theoretical expression of success rate. For presentation purpose, we use the notation $\hat{\Psi}(t,k)$ that equals to $\hat{\varphi}(t,k)$ for CPA, PPA and Bayes attack, $\hat{\psi}(t,k)$ for SB-DoM, AON-DoM and G-DoM, and $\hat{\psi}'(t,k)$ for M-DoM. Then, vectors $\vec{\xi}(k)$, $\vec{\epsilon}(k)$ and $\vec{\epsilon'}(k)$ can all be represented by $\vec{\hat{\Psi}}(k)$.

4.1 Success Boundary

Recalling the analysis in Section 3, a natural next step is to identify a subspace $\mathcal{W} \subseteq \mathcal{V}$ that fulfills $\forall \mathcal{X} \in \mathcal{W}, k^* = \arg\min_{k \in \mathcal{K}} \mathcal{D}(\mathcal{X}, \hat{\Psi}(k))$ and hence gives rise to success of univariate DPA attack. We refer to it as "success space". In the following, we first consider the simplest case involving only a candidate pair (k^*, k°). By Lemmas 2,3,4,5, when the distinguisher can not tell which candidate

is more likely to be the secret subkey, we have:

$$\begin{aligned}
&\mathbf{D}_{\mathsf{Bayes}} : ||\vec{\mathcal{X}} - \vec{\xi}(k^\circ)|| = ||\vec{\mathcal{X}} - \vec{\xi}(k^*)|| \\
&\mathbf{D}_{\mathsf{CPA}} : cos < \vec{\mathcal{X}}, \vec{\xi}(k^\circ) >= cos < \vec{\mathcal{X}}, \vec{\xi}(k^*) > \\
&\mathbf{D}_{\mathsf{PPA}} : \mho < \vec{\mathcal{X}}, \vec{\xi}(k^\circ) >= \mho < \vec{\mathcal{X}}, \vec{\xi}(k^*) > \\
&\mathbf{D}_{\mathsf{SB-DoM}} \simeq \mathbf{D}_{\mathsf{AON-DoM}} \simeq \mathbf{D}_{\mathsf{G-DoM}} : \mho < \vec{\mathcal{X}}, \vec{\epsilon}(k^\circ) >= \mho < \vec{\mathcal{X}}, \vec{\epsilon}(k^*) > \\
&\mathbf{D}_{\mathsf{M-DoM}} : \mho < \vec{\mathcal{X}}, \vec{\epsilon^{'}}(k^\circ) >= \mho < \vec{\mathcal{X}}, \vec{\epsilon^{'}}(k^*) >
\end{aligned} \tag{17}$$

The general formulas of above equations are:

$$\begin{aligned}
&\mathbf{D}_{\mathsf{Bayes}} : \left(\vec{\xi}(k^\circ) - \vec{\xi}(k^*)\right)\vec{\mathcal{X}} - \frac{1}{2}\left(||\vec{\xi}(k^\circ)||^2 - ||\vec{\xi}(k^*)||^2\right) = 0 \\
&\mathbf{D}_{\mathsf{CPA}} : \left(\vec{\xi}(k^\circ)/||\vec{\xi}(k^\circ)|| - \vec{\xi}(k^*)/||\vec{\xi}(k^*)||\right)\vec{\mathcal{X}} = 0 \\
&\mathbf{D}_{\mathsf{PPA}} : \left(\vec{\xi}(k^\circ) - \vec{\xi}(k^*)\right)\vec{\mathcal{X}} = 0 \\
&\mathbf{D}_{\mathsf{SB-DoM}} \simeq \mathbf{D}_{\mathsf{AON-DoM}} \simeq \mathbf{D}_{\mathsf{G-DoM}} : (\vec{\epsilon}(k^\circ) - \vec{\epsilon}(k^*))\vec{\mathcal{X}} = 0 \\
&\mathbf{D}_{\mathsf{M-DoM}} : \left(\vec{\epsilon^{'}}(k^\circ) - \vec{\epsilon^{'}}(k^*)\right)\vec{\mathcal{X}} = 0.
\end{aligned} \tag{18}$$

It turns out that for all univariate DPA distinguishers there is a hyperplane $\mathcal{H}(k^\circ, k^*)$, whose expressions are given in Equ.(18), that linearly divides $\mathcal{V}$ into two parts. We refer to it as "success boundary" and the corresponding normal vector is denoted as $\vec{\eta}(k^\circ, k^*)$. Such linear property of univariate DPA attacks makes it easy to recognize the success space $\mathcal{W}(k^\circ, k^*)$ we are looking for since $\hat{\Psi}(k^*) \in \mathcal{W}(k^\circ, k^*)$. A sketch map is offered in Fig. 6 for illustration. Specifically, let $\triangle\, \hat{\Psi}(k^*)\, O \hat{\Psi}(k^\circ)$ denote the triangle in the figure with O the origin of $\mathcal{V}$. Combined with the geometric meanings of DPA distinguishers, one can immediately realize that for Euclidean distance metric the success boundary is the perpendicular bisecting plane of the side $\hat{\Psi}(k^*)\hat{\Psi}(k^\circ)$, for cosine distance metric it becomes the angular bisecting plane of the angle $< \hat{\Psi}(k^*) O \hat{\Psi}(k^\circ)$, and for projection distance metric it turns to the height plane of the side $\hat{\Psi}(k^*)\hat{\Psi}(k^\circ)$. Based on these, the statistically close performance of univariate DPA distinguishers can be naturally backed up by the fact that when the triangle approaches an isosceles one, its three lines are rapidly in one. Approximating the performance with a unified expression seems well founded. Owing to the arbitrariness of k°, it directly leads to the following theorem for the entire candidate set $\mathcal{K}$:

Theorem 1. *The success boundary on set $\mathcal{K}$ is the union of hyperplanes: $\boldsymbol{Bnd} = \bigcup_{k \in \bar{\mathcal{K}}} \mathcal{H}(k, k^*)$. The success space is the intersection: $\mathcal{W} = \bigcap_{k \in \bar{\mathcal{K}}} \mathcal{W}(k, k^*)$.*

Theorem 1 directly contributes a refined definition of the success rate whose calculation takes the intuitive form of space integral.

Definition 2. *In leakage space $\mathcal{V}$, the success rate of univariate DPA attacks is the probability of $\mathcal{X}$ staying in the success space $\mathcal{W}$ without crossing the success boundary **Bnd**, i.e, $SR = \mathbb{P}\{\mathcal{X} \in \mathcal{W}\}$.*

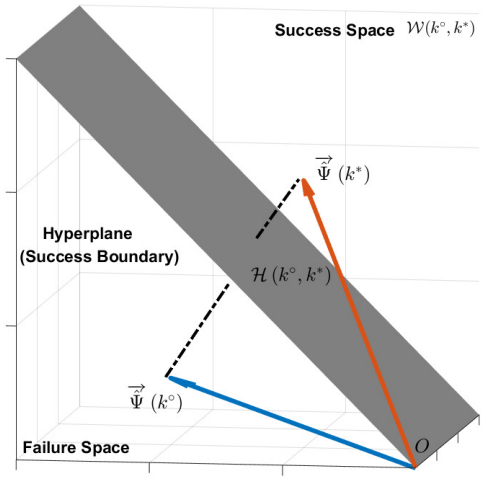

Fig. 6: A sketch map of success boundary and success space.

4.2 Success Rate on Candidate Pair (k^*, k°)

So far, the interaction of the profiled model $\hat{\varphi}$ with the true leakage distribution φ is now explicitly decoupled in terms of SR: the former determines the shape of the success space $\mathcal{W}$ (i.e., Equ.(18)) whereas the latter accounts for its probability density (i.e., Equ.(8)). In this subsection, we derive the success rate under candidate pair (k^*, k°). As disscussed, univariate DPA attacks potentially incorporate the same metric to distinguish the secret subkey. Capturing this feature, we offer a unified expression of SR and further figure out what it depends on and how. Without loss of generality, we launch a normalization and exploit the following three extensions of confusion coefficient:

$$\begin{aligned}
\kappa(k_i, k_j) &= \mathbb{E}\{(\frac{\varphi|k_i - \mu}{\sigma_E} - \frac{\varphi|k_j - \mu}{\sigma_E})^2\}, \\
\hat{\kappa}(k_i, k_j) &= \mathbb{E}\{(\frac{\hat{\Psi}|k_i - \hat{\mu}}{\hat{\sigma}_E} - \frac{\hat{\Psi}|k_j - \hat{\mu}}{\hat{\sigma}_E})^2\}, \\
\tilde{\kappa}(k_i, k_j) &= \mathbb{E}\{(\frac{\hat{\Psi}|k_i - \hat{\mu}}{\hat{\sigma}_E} - \frac{\varphi|k_j - \mu}{\sigma_E})^2\}.
\end{aligned} \tag{19}$$

Here Ψ is the counterpart for the true leakage distribution φ. The notations $\mu\,(\hat{\mu})$ and $\sigma_E\,(\hat{\sigma}_E)$ represent the corresponding mean and standard deviation.

Theorem 2. *The SR on candidate pair (k^*, k°) takes the unified expression:*

$$SR(k^\circ, k^*) = 0.5 + \frac{1}{2}\,\mathrm{erf}\left(\frac{\tilde{\kappa}(k^*, k^\circ) - \tilde{\kappa}(k^*, k^*)}{\sqrt{\hat{\kappa}(k^*, k^\circ) \times \kappa(k^*, k^\circ)}} \times \sqrt{\frac{1}{8} \times SNR \times Q \times \kappa\,(k^*, k^\circ)}\right). \tag{20}$$

The error function is defined as: $erf(x) = \frac{2}{\sqrt{\pi}} \times \int_{-\infty}^{x} e^{-t^2/2} dt$.

Remark. In view of representativeness, this expression is derived based on the projection metric but can be valid for any other distance metrics because of the statistically close performance which have been verified in Subsection 3.5

Proof. The success boundary **Bnd** in this case is a hyperplane: $H(k^\circ; x) = \left(\vec{\hat{\Psi}}\left(k^\circ\right) - \vec{\hat{\Psi}}\left(k^*\right)\right) x$. Having the fact that $\hat{\Psi}\left(k^*\right) \in \mathcal{W}(k^\circ, k^*)$, we now check out whether Θ is at the same side of the success boundary:

$$\begin{aligned} H(k^\circ; \hat{\Psi}\left(k^*\right)) &= \left(\vec{\hat{\Psi}}\left(k^\circ\right) - \vec{\hat{\Psi}}\left(k^*\right)\right) \vec{\hat{\Psi}}\left(k^*\right) = Q \times \sigma_E^2 \times \left(-\frac{\hat{\kappa}(k^*, k^\circ)}{2}\right) \leq 0 \\ H(k^\circ; \Theta) &= \left(\vec{\hat{\Psi}}\left(k^\circ\right) - \vec{\hat{\Psi}}\left(k^*\right)\right) \vec{\Theta} = Q \times \hat{\sigma}_E \times \sigma_E \times \left(\frac{-\tilde{\kappa}(k^*, k^\circ) + \tilde{\kappa}(k^*, k^*)}{2}\right). \end{aligned} \tag{21}$$

For generality, we do not make any assumptions on the profiled function $\hat{\varphi}$ so that it can be arbitrarily wrong. Therefore, the sign of $H(k^\circ; \Theta)$ is uncertain but it appears that $\Theta \in \mathcal{W}(k^\circ, k^*)$ if and only if $H(k^\circ; \Theta) \leq 0$. To obtain the success rate $\mathbb{P}\{\mathcal{X} \in \mathcal{W}(k^\circ, k^*)\} = \frac{\mathbb{P}\{\mathcal{X} \in \mathcal{W}(k^\circ, k^*)\}}{\mathbb{P}\{\mathcal{X} \in \mathcal{V}\}}$, we first consider a straight line γ perpendicular to **Bnd** and address the subproblem $\frac{\mathbb{P}\{\mathcal{X} \in \bar{\gamma}\}}{\mathbb{P}\{\mathcal{X} \in \gamma\}}$ with $\bar{\gamma}$ represents the part in failure space. Let $\theta = ||\gamma - \Theta||$ and $\mathfrak{L} = ||\Theta - \mathbf{Bnd}||$, then we have:

$$\mathfrak{L} = \frac{|H(k^\circ; \Theta)|}{||\vec{\hat{\Psi}}\left(k^\circ\right) - \vec{\hat{\Psi}}\left(k^*\right)||} = \frac{\sigma_E \times \sqrt{Q}}{\sqrt{\hat{\kappa}(k^*, k^\circ)}} * |-\frac{\tilde{\kappa}(k^*, k^\circ)}{2} + \frac{\tilde{\kappa}(k^*, k^*)}{2}|. \tag{22}$$

The operator $|\cdot|$ denotes getting absolute value. According to Equ.(8) and assuming $\Theta \in \mathcal{W}(k^\circ, k^*)$, we can get:

$$\frac{\mathbb{P}\{\mathcal{X} \in \bar{\gamma}\}}{\mathbb{P}\{\mathcal{X} \in \gamma\}} = \frac{\int_{\mathfrak{L}}^{+\infty} \phi\left(\sqrt{r^2 + \theta^2}\right) dr}{\int_{-\infty}^{+\infty} \phi\left(\sqrt{r^2 + \theta^2}\right) dr}. \tag{23}$$

It is noteworthy that:

$$\phi\left(\sqrt{r^2 + \theta^2}\right) = \left(\frac{1}{\sqrt{2\pi} \times \sigma_N}\right)^Q \exp\left(-\frac{r^2 + \theta^2}{2 \times \sigma_N^2}\right) = \hbar\left(\theta\right) \cdot \phi\left(r\right) \tag{24}$$

where $\hbar\left(\theta\right) = \exp\left(-\frac{\theta^2}{2\sigma_N^2}\right)$. Based on this, we further acquire:

$$\frac{\mathbb{P}\{\mathcal{X} \in \bar{\gamma}\}}{\mathbb{P}\{\mathcal{X} \in \gamma\}} = \frac{\int_{\mathfrak{L}}^{+\infty} \phi\left(r\right) dr}{\int_{-\infty}^{+\infty} \phi\left(r\right) dr} = 1 - \Phi_{\sigma_N}\left(\mathfrak{L}\right) = 1 - \Phi_{\sigma_N}\left(\frac{-H(k^\circ; \Theta)}{||\vec{\hat{\Psi}}\left(k^\circ\right) - \vec{\hat{\Psi}}\left(k^*\right)||}\right), \tag{25}$$

which is found independent of θ. For the other case $H(k^\circ; \Theta)) > 0$, we have:

$$\frac{\mathbb{P}\{\mathcal{X} \in \bar{\gamma}\}}{\mathbb{P}\{\mathcal{X} \in \gamma\}} = \frac{\int_{-\mathfrak{L}}^{+\infty} \phi\left(r\right) dr}{\int_{-\infty}^{+\infty} \phi\left(r\right) dr} = 1 - \Phi_{\sigma_N}\left(-\mathfrak{L}\right) = 1 - \Phi_{\sigma_N}\left(\frac{-H(k^\circ; \Theta)}{||\vec{\hat{\Psi}}\left(k^\circ\right) - \vec{\hat{\Psi}}\left(k^*\right)||}\right). \tag{26}$$

Interestingly, above results are completely the same. Hence, we do not distinguish them afterward. In a word, the normal vector $\vec{\eta}(k^\circ, k^*)$ spans a one-dimensional straight line, but together with the hyperplane $\mathcal{H}(k^\circ, k^*)$ itself, which is essentially a subspace of $Q-1$ dimensions, span the whole leakage space $\mathcal{V}$. At last, the success rate on candidate pair (k^*, k°) is:

$$\begin{aligned} SR(k^\circ, k^*) &= \frac{\mathbb{P}\{\mathcal{X} \in \mathcal{W}(k^\circ, k^*)\}}{\mathbb{P}\{\mathcal{X} \in \mathcal{V}\}} = 1 - \frac{\mathbb{P}\{\mathcal{X} \in \bar{\gamma}\}}{\mathbb{P}\{\mathcal{X} \in \gamma\}} \\ &= 0.5 + \frac{1}{2}\operatorname{erf}\left(\frac{\tilde{\kappa}(k^*, k^\circ) - \tilde{\kappa}(k^*, k^*)}{\sqrt{\hat{\kappa}(k^*, k^\circ) \times \kappa(k^*, k^\circ)}} \times \sqrt{\frac{1}{8} \times SNR \times Q \times \kappa\left(k^*, k^\circ\right)}\right), \end{aligned} \tag{27}$$

where $SNR = \sigma_E^2 / \sigma_N^2$. The equation brings us significant conclusions:

(1) It verifies the prior deduction in Subsection 3.2 that SR is determined by the overlapped space of the two neighbourhoods. Factors involved are the size of each neighbourhood which is reflected by σ_N^2 and the Euclidean distance between their centers $||\hat{\Psi}(k^*) - \hat{\Psi}(k^\circ)|| = \sqrt{Q \times \sigma_E^2 \times \kappa(k^*, k^\circ)}$.
(2) $SR(k^\circ) \geq 0.5$. Conducting a univariate DPA attack is always better than a random guess (whose success rate is exactly 0.5) even for small SNR and inadequate Q. The term $\frac{1}{2}\operatorname{erf}\left(\frac{\tilde{\kappa}(k^*,k^\circ)-\tilde{\kappa}(k^*,k^*)}{\sqrt{\hat{\kappa}(k^*,k^\circ)\times\kappa(k^*,k^\circ)}} \times \sqrt{\frac{1}{8} \times SNR \times Q \times \kappa\left(k^*, k^\circ\right)}\right)$ is the gain of effectiveness.
(3) The upper bound approximation in [20, 40] may become inaccurate for low SNR. This method was designed to squeeze the success rate on set $\mathcal{K}$ with success rate on certain pair (k^*, k). Using our notations, it is expressed as:

$$SR(\mathcal{K}) \leq \min_{k \in \bar{\mathcal{K}}} SR(k, k^*). \tag{28}$$

By the second conclusion, this upper bound is always greater than 0.5 which may disagree with the fact that SR in practice can be much more lower.

Corollary 1. *If the adversary exploits the perfect leakage model (i.e., $\hat{\Psi} = \Psi = \varphi$), then $\tilde{\kappa}(k^*, k^*) = 0$ and $\kappa(k^*, k^\circ) = \hat{\kappa}(k^*, k^\circ) = \tilde{\kappa}(k^*, k^\circ)$. The success rate on candidate pair (k^*, k°) becomes:*

$$SR(k^\circ, k^*) = 0.5 + \frac{1}{2}\operatorname{erf}\left(\sqrt{\frac{1}{8} \times SNR \times Q \times \kappa\left(k^*, k^\circ\right)}\right). \tag{29}$$

Model errors are damaging that decay SR. Comparing Equ.(29) with (20) gives rise to the following criteria judging robustness of $SR(k^\circ, k^*)$:

Corollary 2. *Let $C(k^\circ) = \frac{\tilde{\kappa}(k^*,k^\circ)-\tilde{\kappa}(k^*,k^*)}{\sqrt{\hat{\kappa}(k^*,k^\circ)\times\kappa(k^*,k^\circ)}}$ whose value serves as the criteria:*
(1) *$C(k^\circ) \leq 0$. The success rate $SR(k^\circ, k^*)$ will be distorted by model errors and turn to a monotonously decreasing function of the number of measurements Q.*
(2) *$C(k^\circ) > 0$. Applying a profiled model is equivalent to applying the perfect one but reducing* SNR *by factor $C^2(k^\circ)$.*

4.3 Success Rate on Candidate Set $\mathcal{K}$

Now we extend the success rate of univariate DPA attack to the whole candidate set $\mathcal{K}$. By Theorem 1, the success boundary in this case is made up of $|\mathcal{K}|-1$ hyperplanes: $\mathbf{Bnd} = \cup_{k\in\bar{\mathcal{K}}}\mathcal{H}(k,k^*)$. Recalling Equ.(21) and the fact that $\hat{\Psi}(k^*) \in \mathcal{W}$, the condition $\mathcal{X} \in \mathcal{W}$ will be satisfied if we restrict $\mathcal{X}$ by a constraint set $\left\{H(k^{[1]};\mathcal{X}) \le 0, \cdots, H(k^{[S]};\mathcal{X}) \le 0\right\}$ which states that it cannot cross any hyperplane and must stay at the same side with $\hat{\Psi}(k^*)$.

Lemma 6. *The success rate of univariate DPA attack on set $\mathcal{K}$ is expressed as:*

$$SR(\mathcal{K}) = \mathbb{P}\left\{H(k^{[1]};\mathcal{X}) \le 0, \cdots, H(k^{[S]};\mathcal{X}) \le 0\right\}. \tag{30}$$

Significantly, for each constraint $H(k;\mathcal{X}) \le 0$, it corresponds to the case of candidate pair (k^*,k) analysed in Subsection 4.2 which takes a Gaussian form of expression. As a result, one can infer that the whole constraint set follows a multivariate Gaussian distribution with a $1\times S$ mean vector as $\mu_H = \{H(k^{[1]};\Theta),\ldots,H(k^{[S]};\Theta)\}$. A Gaussian distribution is totally determined by its first two moments and to obtain the covariance matrix Σ_H, we first reveal the more complicated confusion relationship among three subkey candidates in an intuitive way: randomly selecting two of the hyperplanes from **Bnd** denoted as $\mathcal{H}(k^{[i]},k^*)$ and $\mathcal{H}(k^{[j]},k^*)$, we plot them with solid lines in Fig. 7. The intersection of the hyperplanes can be measured by cosine of the included angle δ that is easily calculated through their normal vectors (plotted in dotted lines):

$$\hat{\kappa}(k^*,k^{[i]},k^{[j]}) = \frac{\vec{\eta}(k^{[i]},k^*)\cdot\vec{\eta}(k^{[j]},k^*)}{||\vec{\eta}(k^{[i]},k^*)||\times||\vec{\eta}(k^{[j]},k^*)||} = \frac{\frac{1}{2}(\hat{\kappa}(k^*,k^{[i]})+\hat{\kappa}(k^*,k^{[j]})-\hat{\kappa}(k^{[i]},k^{[j]}))}{\sqrt{\hat{\kappa}(k^*,k^{[i]})\times\hat{\kappa}(k^*,k^{[j]})}}. \tag{31}$$

To successfully identify k^*, $\mathcal{X}$ has to stay in $\mathcal{W}(k^{[i]},k^{[j]},k^*) = \mathcal{W}\left(k^{[i]},k^*\right)\cap \mathcal{W}\left(k^{[j]},k^*\right)$ as shown by the shadow in Fig 7. A smaller δ implies a broader success space and a weaker confusion property. On these grounds, the (i,j) element of the $S\times S$ covariance matrix Σ_H becomes:

$$\begin{aligned}(\Sigma_H)_{ij} &= Cov\left(H(k^{[i]};\mathcal{X}),H(k^{[j]};\mathcal{X})\right) = Cov\left(\vec{\eta}(k^{[i]},k^*)\cdot\vec{\mathcal{X}},\vec{\eta}(k^{[j]},k^*)\cdot\vec{\mathcal{X}}\right)\\ &= \vec{\eta}(k^{[i]},k^*)\cdot\vec{\eta}(k^{[j]},k^*)\times Cov\left(\textstyle\sum_{q_1=1}^{Q}x_{q_1},\sum_{q_2=1}^{Q}x_{q_2}\right)\\ &= \frac{1}{2}(\hat{\kappa}(k^*,k^{[i]})+\hat{\kappa}(k^*,k^{[j]})-\hat{\kappa}(k^{[i]},k^{[j]}))\times Q\times\hat{\sigma}_E^2\times\sigma_N^2.\end{aligned} \tag{32}$$

Inheriting the independence between encryptions, measurements (x_{q_1},x_{q_2}) have a nonzero covariance if and only if $q_1=q_2$. In the end, let $\Phi^S_{\Sigma_H}$ denote the cumulative distribution function of the S-dimension normal distribution $\mathcal{N}(\mu_H,\Sigma_H)$, and we obtain the following theorem:

Theorem 3. *The SR on candidate set $\mathcal{K}$ takes the unified expression:*

$$SR(\mathcal{K}) = \Phi^S_{\Sigma_H}(\mu_H) = \Phi^S_{\mathbf{K}}(\frac{\sqrt{Q\times SNR}}{2}\times\mathbf{k}). \tag{33}$$

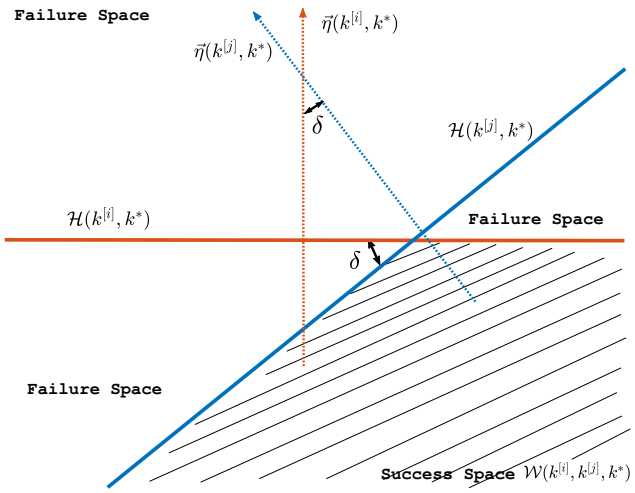

Fig. 7: A sketch map of hyperplane angle δ.

The $1 \times S$ *mean vector* $\mathbf{k} = \{\tilde{\kappa}(k^*, k^{[1]}) - \tilde{\kappa}(k^*, k^*), \ldots, \tilde{\kappa}(k^*, k^{[S]}) - \tilde{\kappa}(k^*, k^*)\}$. *The* $S \times S$ *covariance matric* $\mathbf{K}_{ij} = \frac{1}{2}(\hat{\kappa}(k^*, k^{[i]}) + \hat{\kappa}(k^*, k^{[j]}) - \hat{\kappa}(k^{[i]}, k^{[j]}))$.

Due to the normalization, the confusion coefficients capture the model errors and decouple them from the physical property of implementation (i.e., the SNR of real leakages). They describe the cryptographical features from the perspective of an adversary with given abilities. This theorem shows new observations:

(1) It covers our deduction for DoM in Subsection 2.3 that if the SNR is decreased to $1/\beta$, the number of measurements Q has to be multiplied by β to achieve the same SR. This is the well-known "*Rule of Thumb*" [23] and we now have proved that it is suitable even for inaccurate profiled models.
(2) The models of adversary and device are not commutative. Keeping other parameters, exchanging the two models will cause differences in SR because of different covariance matrix $\mathbf{K}$.

Corollary 3. *If the adversary exploits the perfect leakage model (i.e.,* $\hat{\Psi} = \Psi = \varphi$*), then success rate of univariate DPA attacks on set* $\mathcal{K}$ *becomes:*

$$SR(\mathcal{K}) = \Phi^S_{\mathbf{K}'}\left(\frac{\sqrt{Q \times SNR}}{2} \times \mathbf{k}'\right). \tag{34}$$

The $1 \times S$ *mean vector* $\mathbf{k}' = \{\kappa(k^*, k^{[1]}), \ldots, \kappa(k^*, k^{[S]})\}$. *The* $S \times S$ *covariance matric* $\mathbf{K}'_{ij} = \frac{1}{2}(\kappa(k^*, k^{[i]}) + \kappa(k^*, k^{[j]}) - \kappa(k^{[i]}, k^{[j]}))$.

The success rate on candidate pair $SR(k^*, k^{[i]})$ can be seen as the i-th dimension of the multidimensional Gaussian distributed $SR(\mathcal{K})$. As a result, we extend Corollary 2 to obtain the sufficient (not necessary) criterion which judges robustness of $SR(\mathcal{K})$ by examining each of its dimensions:

Corollary 4. *The $SR(\mathcal{K})$ of univariate DPA attack will be robust (i.e., not be distorted by model errors and increase with the number of measurements) if it satisfies:* $\forall k \in \bar{\mathcal{K}}, C(k) = \frac{\hat{\kappa}(k^*,k)-\hat{\kappa}(k^*,k^*)}{\sqrt{\hat{\kappa}(k^*,k)\times\kappa(k^*,k)}} > 0$. *The larger the overall criterion values are, the stronger performance univariate DPA attack achieves.*

It confirms that in the perfect model setting, CPA, PPA and Bayes attack ($\forall k \in \bar{\mathcal{K}}, C(k) = 1$) will always outperform the DoM family ($\forall k \in \bar{\mathcal{K}}, C(k) \leq 1$).

5 Experimental Results

The experiments bases on an open data set of hardware implementation (i.e., TeSCASE [1]). It contains measurements sampled from an AES on Sasebo-GII board and the source code can be found in [2]. We additionally consider another popular model profiling method besides the one mentioned in Subsection 3.5 that estimates the leakage function as $\hat{\varphi}(y) = \hat{\mathbb{E}}\{x_{q|\mathrm{Sbox}(k\oplus t_q)=y}\}$ (which is denoted as Mean-Based (MB) model). The new method is called Regression-Based (RB) model [32]. It builds leakage function on a binary basis $\mathbf{g}(y) = \{\mathbf{g}_1(y), \cdots, \mathbf{g}_{\mathrm{B}}(y)\}$ whose size is not necessarily the bit length of y. A small basis will converge faster but a more complex model can gain more accuracy. Profiling the model turns into estimating the coefficients c_i such that $\hat{\varphi}(y) = \sum_j c_j \mathbf{g}_j(y)$ is the least-square approximation of the leakages. It has been proven to be optimal when the noise is Gaussian [5]. In the experiment, we target at the first S-box of the last round encryption and simply set the binary basis of the RB model as the XOR of Sbox input and output. This introduces extra assumption errors [12] [13] for RB model even after intensive profiling. The corresponding POI is displayed in Fig. 8. We control model errors by restricting profiling measurements (i.e., $100,000 \times m$).

5.1 CPA, PPA and Bayes Attack against Hardware Implementation

Experimental results of 7 different settings and the corresponding criterion values are illustrated in Fig.9∼10. For MB model on the full profiling measurement set (i.e, m=1), theoretical SR-s calculated by Equ.(34) approximated the empirical ones best and well enough. So, it was treated as the perfect model setting. Theoretical SR-s of the others 6 settings were calculated by Equ.(33). They are all represented by lines 'THEO'. Criterion values $C(k)$ are examined for every model and subkey candidate $k \in \bar{\mathcal{K}}$. They are plotted in red crosses for largest model error setting and in grey circles for the others. Our observations are:

(a) The RB method is less effective (see Fig.9). It requires 1800 measurements, compared with 600 measurements of the MB method, to reach 95% success rate under $m = 1$. This is mainly because the simple basis based only on the S-box output bits can not accurately reflect behaviours of the chip so there are always assumption errors which can not be eliminated even with full profiling measurement set.

(b) The RB method converges faster (see Fig.9). SR-s of the RB model under $m = 0.01$ achieve a similar tendency as the MB model under $m = 0.05$. Increasing m of the RB model to 0.015 (Δ=0.005) brings significantly more improvement of SR than increasing m of the MB model to 0.1 (Δ=0.05).
(c) Success rate becomes distorted (i.e., decrease with Q) when the number of profiling measurements is reduced to an extent (see Fig.10(a)). In this case nearly half of the criterion values (red crosses) are found less than 0 whereas all grey circles corresponding to robust SR-s don't (see Fig.10(b)).
(d) Our theoretical SR-s successfully predict the behaviours of CPA, PPA and Bayes attack from the setting of inadequate profiling measurements to sufficient profiling measurements.

5.2 G-DoM and AON-DoM against Hardware Implementation

Experimental results of 5 different settings and the corresponding criterion values are illustrated in Fig.11∼13. The DoM's models are generated by mapping the model values of MB and RB models to some integers according to Equ.(13) (just as we did in Subsection 3.5). Our observations are:

(a) G-DoM is more powerful (see Fig.11(a) and Fig.12(a)). Under the MB model and $m = 1$, about 1200 measurements can ensure a 95% success rate for G-DoM while 8200 measurements are necessary for AON-DoM.
(b) G-DoM is more robust (see Fig.11(b) and Fig.12(b)). Despite the poor performance, SR-s of G-DoM in the largest model error setting still follow an upward trend. This is the opposite case for AON-DoM.
(c) Profiling method has greater impact on G-DoM (see Fig.11(a) and Fig.12(a)). Differences between SR-s are significantly bigger for G-DoM under the two profiling methods on full profiling measurement set. This can be explained by the fact that AON-DoM only cares about the two extreme model values where limited differences exist for the MB and RB methods. It can also answer why RB model converges much faster for AON-DoM (i.e., profiled model of $m = 0.02$ achieves almost the same performance as that of $m = 1$).
(d) The criterion are sufficient but not necessary (see Fig.13). Criterion values associated with robust SR-s in 4 settings (grey circles) stay positive as expected. However, a few negative criterion values for robust SR-s of G-DoM in largest model error setting (i.e, Fig.11(b)) are found. These few distorted dimensions seems did not play a decisive role in the multidimensional Gaussian distributed SR so it is still upward. In contrast, half of tested criterion values came out to be negative for AON-DoM in the same setting.
(e) Large criterion values result in strong performance. This observation verifies the conclusion of Corollary 4. The larger criterion values of G-DoM in overall confirms the experimental phenomenon that it outperformed AON-DoM.
(f) Our theoretical SR-s precisely predict behaviours of G-DoM in all settings. Note that for AON-DoM the plaintext bytes corresponding to the maximum and minimum model values may not appear all the time when Q is small. So,

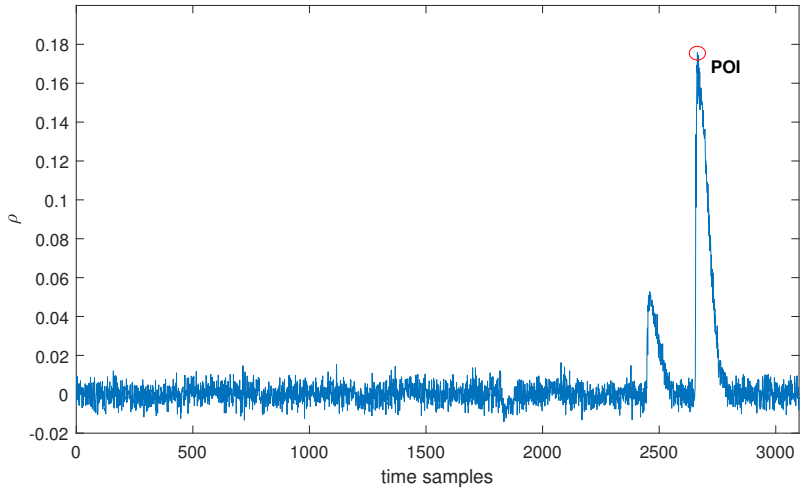

Fig. 8: The selected POI from the real leakages of the TeSCASE dataset.

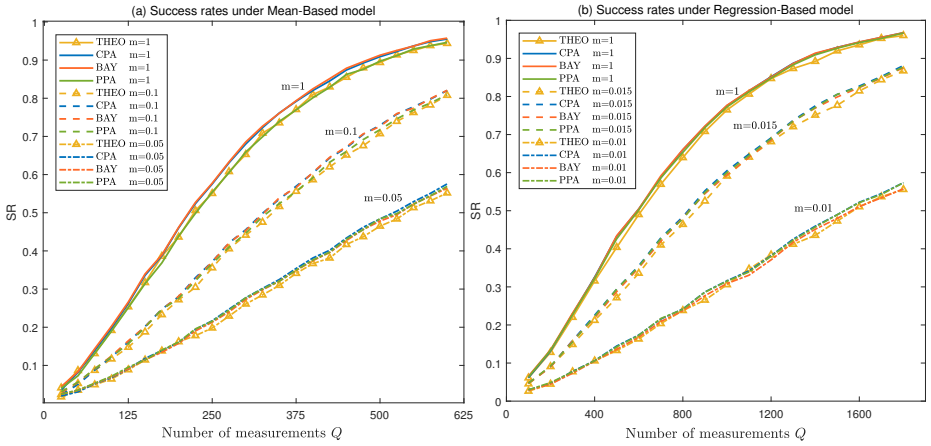

Fig. 9: Success rates of CPA, PPA and Bayes attack on the TeSCASE dataset.

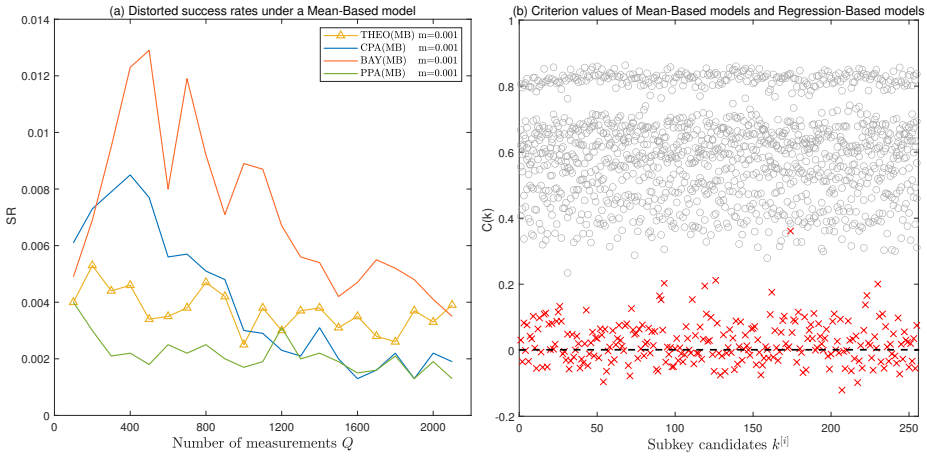

Fig. 10: Left: distorted success rates of CPA, PPA and Bayes attack on the TeSCASE dataset. Right: Criterion values of Mean-Based models and Regression-Based models of CPA, PPA and Bayes attack.

its empirical performances are a bit lower than our theoretical SR-s (which is derived in an average sense) at the beginning but soon get close to them as Q increases. They are still desirable evaluation tools for AON-DoM.

5.3 SB-DoM and M-DoM against Hardware Implementation

Experimental results and the corresponding criterion values are illustrated in Fig.14. Performance of SB-DoM (on the least significant bit) and M-DoM were less than satisfactory in the experiment (i.e., success rates of 2000 measurements are lower than 2% even with the most effective MB model on full profiling measurement set). This is probably because the leakage model of the hardware implemented TeSCASE data set does not strictly follow a type of model like the Hamming weight but more likely Hamming distance. Classification based only on a S-box output bit (the original definition of SB-DoM in [21]) will bring about a lack of relevance (i.e, additional assumption errors). Similar phenomenon has already been observed in [6] that several incorrect key candidates of hardware implementation may result in higher distinguishing values and those peaks are referred to as *ghost peaks*. Indeed this highlights the necessity of other DPA distinguishers which are later improvements on this line of research. Therefore, we did not consider other settings with even worse model. Our observations are:

(a) M-DoM is more robust (see Fig.14(a)). Success rates of SB-DoM are distorted by model errors. Recalling Equ.(7), M-DoM is an improvement of SB-DoM that simply sums its result on each bit of S-box output. This integration of more information brings gains in robustness.
(b) Criterion values of M-DoM are in blue crucifixes and of SB-DoM are red crosses (see Fig.14(b)). Similar to G-DoM, several distorted dimensions of SR (i.e., negative criterion values) did not defeat the robustness of M-DoM. Yet, a third of bad criterion values skewed the overall performance of SB-DoM on the whole candidate set. The criterion are not necessary.
(c) Our theoretical SR-s are able to maintain accuracy in the inferior setting of univariate DPA distinguisher. They have the potential to be an affordable evaluation tools in practice.

6 Conclusions

This paper facilitated a better understanding of univariate DPA attack. We built an evaluation framework centered around leakage space $\mathcal{V}$ where different univariate DPA distinguishers were unified as linear ML-attack. It allowed discussing their relationship in a straightforward manner. Further, we proposed the concept of "success space" and derived the theoretical expression of SR which can work under any (possibly inaccurate) leakage model. Eventually, the criterion judging robustness of SR were suggested for an in-depth research of model errors. We believe our theory brings a new road for evaluation of other side-channel

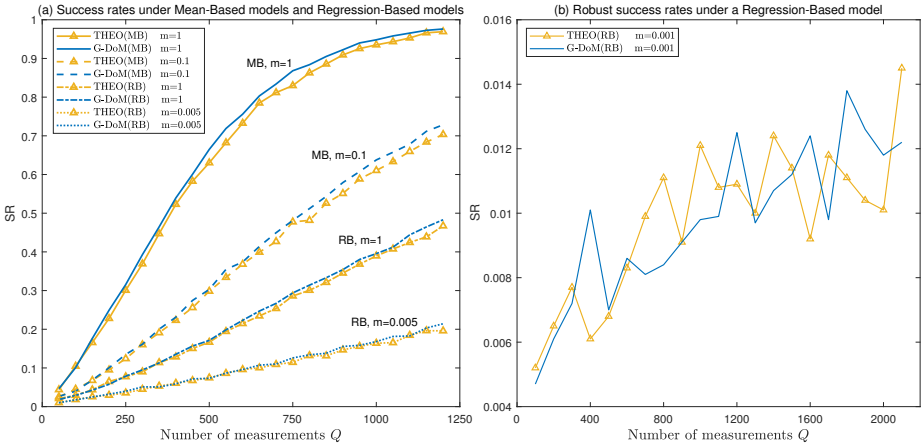

Fig. 11: Success rates of G-DoM on the TeSCASE dataset.

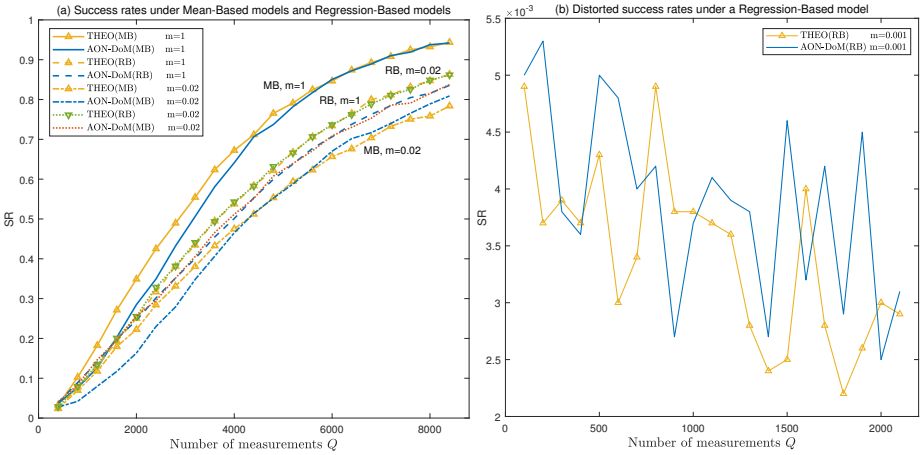

Fig. 12: Success rates of AON-DoM on the TeSCASE dataset.

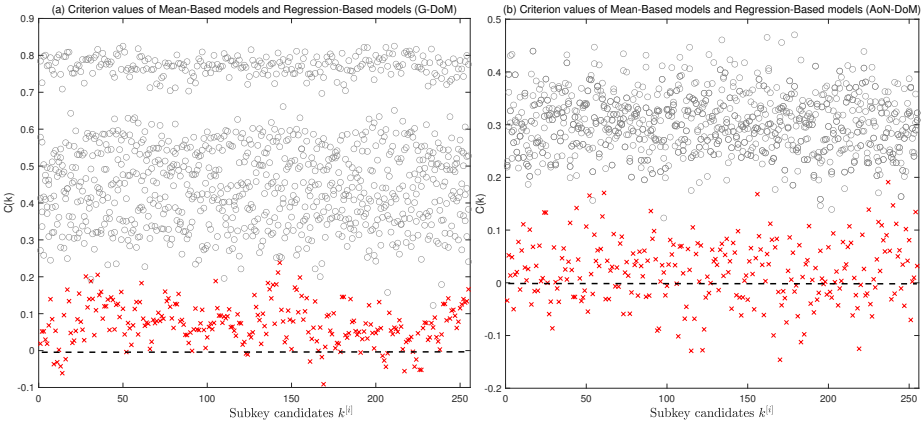

Fig. 13: Criterion values of Mean-Based models and Regression-Based models of G-DoM and AON-DoM.

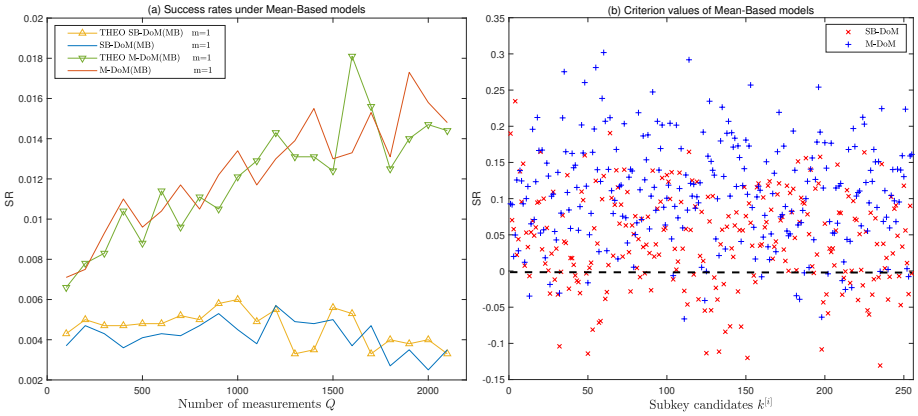

Fig. 14: Left: Success rates of SB-DoM and M-DoM on the TeSCASE dataset. Right: Criterion values of Mean-Based models of SB-DoM and M-DoM.

distinguishers, e.g., collision attack [19,28] and mutual information analysis [39]. In the future, we will also extend our research to other security metrics, such as guessing entropy, and look forward to the "*surprises*" brought by it.

References

1. Northeastern University TeSCASE dataset. https://chest.coe.neu.edu/.
2. Side-channel attack standard evaluation board (sasebo): Sasebo-gii. http://www.rcis.aist.go.jp/special/SASEBO/SASEBOGII-en.html./.
3. D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. The EM Side-Channel(s). In *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, volume 2523 of *Lecture Notes in Computer Science*, pages 29–45. Springer, 2002.
4. R. Bevan and E. Knudsen. Ways to enhance differential power analysis. In P. J. Lee and C. H. Lim, editors, *Information Security and Cryptology - ICISC 2002, 5th International Conference Seoul, Korea, November 28-29, 2002, Revised Papers*, volume 2587 of *Lecture Notes in Computer Science*, pages 327–342. Springer, 2002.
5. C. M. Bishop. *Pattern Recognition and Machine Learning, 5th Edition*. Information science and statistics. Springer, 2007.
6. E. Brier, C. Clavier, and F. Olivier. Correlation Power Analysis with a Leakage Model. In *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer, 2004.
7. N. Bruneau, C. Carlet, S. Guilley, A. Heuser, E. Prouff, and O. Rioul. Stochastic Collision Attack. *IEEE Trans. Inf. Forensics Secur.*, 12(9):2090–2104, 2017.
8. N. Bruneau, S. Guilley, A. Heuser, and O. Rioul. Masks Will Fall Off - Higher-Order Optimal Distinguishers. In *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and*

Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II, volume 8874 of *Lecture Notes in Computer Science*, pages 344–365. Springer, 2014.
9. E. 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.*, 2019(2):49–79, 2019.
10. J. Doget, E. Prouff, M. Rivain, and F. Standaert. Univariate Side Channel Attacks and Leakage Modeling. *J. Cryptogr. Eng.*, 1(2):123–144, 2011.
11. F. Durvaux and F. Standaert. From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces. In *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 240–262. Springer, 2016.
12. F. Durvaux, F. Standaert, and S. M. D. Pozo. Towards Easy Leakage Certification. In *Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*, volume 9813 of *Lecture Notes in Computer Science*, pages 40–60. Springer, 2016.
13. F. Durvaux, F. Standaert, and N. Veyrat-Charvillon. How to Certify the Leakage of a Chip? In *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 459–476. Springer, 2014.
14. L. Egghe and L. Leydesdorff. The Relation between Pearson's Correlation Coefficient r and Salton's Cosine Measure. *J. Assoc. Inf. Sci. Technol.*, 60(5):1027–1036, 2009.
15. Y. Fei, A. A. Ding, J. Lao, and L. Zhang. A Statistics-based Success Rate Model for DPA and CPA. *J. Cryptogr. Eng.*, 5(4):227–243, 2015.
16. Y. Fei, Q. Luo, and A. A. Ding. A Statistical Model for DPA with Novel Algorithmic Confusion Analysis. In *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *Lecture Notes in Computer Science*, pages 233–250. Springer, 2012.
17. K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic Analysis: Concrete Results. In *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, volume 2162 of *Lecture Notes in Computer Science*, pages 251–261. Springer, 2001.
18. B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel. Mutual Information Analysis. In *Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008. Proceedings*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer, 2008.
19. C. Glowacz and V. Grosso. Optimal Collision Side-Channel Attacks. In *Smart Card Research and Advanced Applications - 18th International Conference, CARDIS 2019, Prague, Czech Republic, November 11-13, 2019, Revised Selected Papers*, volume 11833 of *Lecture Notes in Computer Science*, pages 126–140. Springer, 2019.
20. S. Guilley, A. Heuser, and O. Rioul. A Key to Success - Success Exponents for Side-Channel Distinguishers. In *Progress in Cryptology - INDOCRYPT 2015 - 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings*, volume 9462 of *Lecture Notes in Computer Science*, pages 270–290. Springer, 2015.

21. P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.
22. T. Le, J. Clédière, C. Canovas, B. Robisson, C. Servière, and J. Lacoume. A proposition for correlation power analysis enhancement. In L. Goubin and M. Matsui, editors, *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings*, volume 4249 of *Lecture Notes in Computer Science*, pages 174–186. Springer, 2006.
23. S. Mangard. Hardware Countermeasures against DPA ? A Statistical Analysis of Their Effectiveness. In *Topics in Cryptology - CT-RSA 2004, The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings*, volume 2964 of *Lecture Notes in Computer Science*, pages 222–235. Springer, 2004.
24. S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks - Revealing the Secrets of Smart Cards*. Springer, 2007.
25. S. Mangard, E. Oswald, and F. Standaert. One for All - All for One: Unifying Standard Differential Power Analysis Attacks. *IET Inf. Secur.*, 5(2):100–110, 2011.
26. T. S. Messerges and E. A. Dabbish. Investigations of power analysis attacks on smartcards. In S. B. Guthery and P. Honeyman, editors, *Proceedings of the 1st Workshop on Smartcard Technology, Smartcard 1999, Chicago, Illinois, USA, May 10-11, 1999*. USENIX Association, 1999.
27. T. S. Messerges, E. A. Dabbish, and R. H. Sloan. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Computers*, 51(5):541–552, 2002.
28. A. Moradi, O. Mischke, and T. Eisenbarth. Correlation-Enhanced Power Analysis Collision Attack. In *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*, volume 6225 of *Lecture Notes in Computer Science*, pages 125–139. Springer, 2010.
29. E. Prouff, M. Rivain, and R. Bevan. Statistical Analysis of Second Order Differential Power Analysis. *IEEE Trans. Computers*, 58(6):799–811, 2009.
30. M. Renauld, F. Standaert, N. Veyrat-Charvillon, D. Kamel, and D. Flandre. A formal study of power variability issues and side-channel attacks for nanoscale devices. In K. G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 109–128. Springer, 2011.
31. M. Rivain. On the Exact Success Rate of Side Channel Analysis in the Gaussian Model. In *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, volume 5381 of *Lecture Notes in Computer Science*, pages 165–183. Springer, 2008.
32. W. Schindler, K. Lemke, and C. Paar. A Stochastic Model for Differential Side Channel Cryptanalysis. In *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings*, volume 3659 of *Lecture Notes in Computer Science*, pages 30–46. Springer, 2005.
33. C. E. Shannon. Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.*, 28(4):656–715, 1949.

34. F. Standaert, T. Malkin, and M. Yung. A unified framework for the analysis of side-channel key recovery attacks (extended version). *IACR Cryptol. ePrint Arch.*, page 139, 2006.
35. F. Standaert, T. Malkin, and M. Yung. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*, pages 443–461. Springer, 2009.
36. F. Standaert, E. Peeters, G. Rouvroy, and J. Quisquater. An overview of power analysis attacks against field programmable gate arrays. *Proc. IEEE*, 94(2):383–394, 2006.
37. A. Thillard, E. Prouff, and T. Roche. Success through Confidence: Evaluating the Effectiveness of a Side-Channel Attack. In *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*, pages 21–36. Springer, 2013.
38. N. Veyrat-Charvillon, B. Gérard, and F. Standaert. Soft Analytical Side-Channel Attacks. In *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 282–296. Springer, 2014.
39. N. Veyrat-Charvillon and F. Standaert. Mutual Information Analysis: How, When and Why? In *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings*, volume 5747 of *Lecture Notes in Computer Science*, pages 429–443. Springer, 2009.
40. C. Whitnall and E. Oswald. A Fair Evaluation Framework for Comparing Side-Channel Distinguishers. *J. Cryptogr. Eng.*, 1(2):145–160, 2011.
41. A. Wiemers. A Remark on a Success Rate Model for Side-Channel Attack Analysis. *J. Cryptogr. Eng.*, 10(3):269–274, 2020.