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 empirically and theoretically a common metric for evaluating the performance of side-channel attacks. Intuitive expressions of success rate are desirable since they reveal and explain the functional dependence on relevant parameters, such as number of measurements and Signal-to-Noise Ratio (SNR), in a straightforward manner. Meanwhile, existing works more or less expose unsolved fundamental problems, such as strong leakage assumption, difficulty in interpretation of principle, inaccurate evaluation, and inconsideration of high-order SR. In this paper, we first provide an intuitive framework that statistical tests embedded in different univariate DPA attacks are unified as analyzing and comparing visualized vectors in a Euclidean space by using different easy-to-understand metrics. Then, we establish a unified framework to abstract and convert the security evaluations to the problem of finding a boundary in the Euclidean space. With expressions of the boundary, judging whether a DPA attack succeeds in sense of o^{th}-order becomes fairly efficient and intuitive, and the corresponding SR can be calculated theoretically by integral. Finally, we propose an algorithm that is capable of estimating arbitrary order of SR effectively. Our experimental results verify the theory and highlight the superiority. We believe our research raises many new perspectives for comparing and evaluating side-channel attacks, countermeasures and implementations.

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

1 Introduction

Physical leakages, such as power consumption [16] and electromagnetic radiation [2,11], unintentionally emitted from implementations breaks the traditional security model of cryptographic algorithms that assumed an adversary has only black box access to cryptosystem. These leakages statistically depend on certain intermediate value which is closely related to the secret key and therefore imply a new road to frustrate the protection. In this paper, we investigate the context of side-channel attacks, in which adversaries are enhanced with ability to conduct several statistical tests on the physical leakages. In the past decade, many univariate DPA distinguishers like Bayes attack [29], Correlation Power Analysis (CPA) [28] and Distance-of-Means (DoM) test [16], have been proposed. Such distinguishers have different performance in practice and their efficiency relies on the ability of statistical test embedded, which is susceptible to properties of cryptographic algorithm, physical characteristics of cryptosystem, number of measurements and assumed knowledge on how the device leaks. How to evaluate their efficiency has become a crucial issue in side-channel evaluations, and has attracted extensive attention and in-depth research. Related works will be discussed in Section 1.1 before describing our contributions.

1.1 Related Works

Evaluation of the performance of a given distinguisher provides valuable and instructive suggestions about whether and to what extent a cryptosystem or countermeasure is side-channel resistant. Success rate (SR) [27], which indicates the probability of success, is the most common metric to evaluate the performance of a side-channel distinguisher under given conditions. The o^{th}-order success rate can be defined as the probability that secret subkey is one of the first o optimal candidates. Estimation on SR can be experimental and theoretical. The former always brings heavy computation loads because of repeated experiments. The latter estimates SR by revealing its functional relationship with the number of measurements, SNR, etc. that determines the relationship between correct and false key candidates, but requires complex derivation.

So far, only a very limited number of distinguishers, such as DoM [10], CPA [17,25,28] and Bayes attacks [25], can be theoretically evaluated in terms of success rate. However, these theoretical estimations depend on strong assumptions that the leakage follows Gaussian distribution, and its model is perfectly known. Moreover, the high dimensional expressions involved limit an intuitive conclusion about what is the functional dependence between those relevant parameters and how they work. Success rate of CPA can be approximated using a multivariate normal c.d.f [23], but was found the corresponding matrices are not of full rank and such a probability density function does not exist [25]. This results in an obviously restricted and biased estimation of success rate. Generalizing the approach in [25], [17] presented a methodology to estimate the success rate of higher-order side-channel attacks against masked implementations and thereby should suffer the same drawbacks.

Closed-form expressions of success rate based on the so called Success Exponent (SE) were given by [14] and improved in [31]. They extended the evaluations from additive distinguishers (e.g., CPA and DoM) to some non-additive distinguishers like Mutual Information Analysis (MIA) [12], and have achieved desired results for a large class of distinguishers. However, the estimation is based on the central limit theorem and only applicable to scenarios that the adversaries have a large number of measurements. Moreover, the paper barely explains the soundness and superiority of the underlying mathematical foundation: "*why exploit an exponential form to express success rate?*" Finally, such closed-form expressions involve high-dimensional complex statistical functions that are hard to estimate.

Recent work in [7] introduced a lower bound of error rate (i.e., an upper bound of success rate) given in [3] and linked success rate with mutual information to obtain a more precise bound of SR. This bound is based on the relationship between mutual information and random probing, and works under a very small number of measurements. However, it is valid only for leakages with low SNR and the bound is loose. The authors in [15] derived the relation between Perceived Information (PI) given in [24] and SR from a probability-theoretical perspective. However, the given bound is very loose as well.

It is noteworthy that, in addition to the above problems in the existing works, there is no discussion on higher-order success rate. Moreover, another fundamental problem that the intuitive meaning of the statistical tests in different univariate DPA attacks, is still open. Their solutions will help accelerate development of evaluation against side-channel attacks.

1.2 Our Contributions

In this paper, we tackle the fundamental problem: "*what is the intuitive meaning of the statistical test embedded in different univariate DPA attacks and how to intuitively evaluate them?*" Our main contributions are as follows:

- To facilitate intuitive understanding of different univariate DPA attacks, we propose a unified framework with concise definitions. The framework allows a straightforward discussion that to which extent different univariate DPA attacks share the same foundation of mathematics. Our definitions capture a large class of DPA attacks whilst being specific enough to allow us to make concrete statements and sound comparison. We show that by applying an intuitive framework, statistical tests embedded in different univariate DPA attacks are unified as analyzing and comparing visualized vectors in a Euclidean space but using different easy-to-understand metrics. This is an important contribution towards putting such attacks on a common theoretical basis.
- On the basis of our framework, we abstract the notion of success rate and establish a unified scheme for evaluating arbitrary order success rate. Specifically, we present the concepts of "*success space*" and "*success boundary*", and show that judging whether a DPA attack succeeds in sense of o^{th}-order becomes fairly efficient and intuitive whenever the corresponding expressions

of boundary is given. We further demonstrate a rigorous derivation of theoretical success rate and raise several significant conclusions in an intuitive manner.
- Motivated by the challenge of evaluating higher-order success rate and benefiting from the intuition of our framework, we put forward an algorithm that can estimate success rate of arbitrarily order in a very efficient way. We believe our algorithm serves as a feasible and effective tool for evaluation of implementations against side-channel attacks in practice.

Experimental results fully illustrate the superiority of our framework and scheme.

1.3 Organization

The rest of this paper is organized as follows: preliminaries such as side-channel leakages, CPA, Bayes attack and DoM attack, success rate and confusion coefficient, are introduced in Section 2 before introducing our works. Concise definition of our unified framework and the corresponding intuitive expression of different univariate DPA attacks are detailed in Section 3. We then further theoretically analyze the intuitive meaning of success rate and generalize its expressions in Section 4. Experiments on both simulated leakages and measurements sampled from an ATMega328p micro-controller are presented in Sections 5 and 6 to illustrate the superiority of our evaluation frameworks and schemes. Finally, we conclude this paper in Section 7.

2 Preliminaries

2.1 Side-Channel Leakages

Let k^* denote the secret subkey selected at random from a set $\mathcal{K} : k^* \xleftarrow{R} \mathcal{K}$, k denote the corresponding guessing value, the uppercase Q denote the total number of encryptions conducted while cryptosystem being monitored and sampled by adversaries, and the corresponding lowercase q denote the q-th encryption $(q = 1, 2, \ldots, Q)$. Let t_q denote the q-th encrypted plaintext byte selected at random from a set $\mathcal{T} : t_q \xleftarrow{R} \mathcal{T}$, and x_q denote the corresponding leakage. Most side-channel attacks assume a known-plaintext attack scenario with both t_q and x_q available to adversaries. Here an identical leakage model can be expressed as:

$$x_q = \alpha \cdot \varphi\left(t_q \oplus k^*\right) + \mathsf{N}, \tag{1}$$

φ actually is a composition of two independent functions, i.e., $\varphi = y \cdot z$. Specifically, z represents the S-box operation which is determined by the underlying cryptographic primitive implemented and y stands for the leakage function relative and specific to physical characteristics of hardware circuits of the cryptosystem. For example, Hamming weight is one of the most commonly considered instances of y. N is the additive and independent noise component following Gaussian distribution, i.e., $\mathsf{N} \sim \mathcal{N}\left(0, \sigma^2\right)$. Without loss of generality and with

reference to [14], we normalize φ such that the expectation $\mathbb{E}\{\varphi\} = 0$ and the variance $\mathbb{D}\{\varphi\} = \mathbb{E}\{\varphi^2\} = 0$. The Signal-to-Noise Ratio (SNR) is thus equal to α^2/σ^2.

For clarity, we use $\hat{x}_q$ to denote instance of Gaussian random variable x_q, which is virtually what adversaries possess and used as input to side-channel distinguishers (e.g., CPA). Finite sample set $X = \{\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_q\}$ then automatically denotes all leakage samples adversaries gather.

2.2 Correlation Power Analysis

Correlation power analysis, abbreviated as CPA, is a well-known side-channel distinguisher identifying secret subkey k^* by assessing the linear fitting rate between the assumed model and measured power consumption [19,22]. Statistical test embedded in CPA is the well-known Pearson's correlation coefficient and CPA is expressed as follows:

$$\mathcal{D}_{\mathsf{CPA}} = \underset{k\in\mathcal{K}}{\arg\max} \frac{Q\sum_{q=1}^{Q}\hat{x}_q\varphi(t_q\oplus k) - \sum_{q=1}^{Q}\hat{x}_q\sum_{q=1}^{Q}\varphi(t_q\oplus k)}{\sqrt{Q\sum_{q=1}^{Q}\hat{x}_q^2 - \left(\sum_{q=1}^{Q}\hat{x}_q\right)^2}\sqrt{Q\sum_{q=1}^{Q}\varphi^2(t_q\oplus k) - \left(\sum_{q=1}^{Q}\varphi(t_q\oplus k)\right)^2}}. \tag{2}$$

2.3 Bayes Attack

Based on the maximum likelihood principle, Bayes attack selects subkey candidate k by calculating the corresponding probability density function where k serves as a parameter. This side-channel distinguisher has attracted wide attentions, especially in Template Attacks, and is regarded as "optimal" in general [5, 6, 13] when priori knowledge about leakage model is available. Bayes Attack is written as:

$$\begin{aligned}\mathcal{D}_{\mathsf{Bayes}} &= \underset{k\in\mathcal{K}}{\arg\max} \prod_{q=1}^{Q}\mathbb{P}\{\hat{x}_q|k\} \\ &= \underset{k\in\mathcal{K}}{\arg\max} \prod_{q=1}^{Q} f_{\sigma^2}(\hat{x}_q - \alpha\cdot\varphi(t_q\oplus k))\end{aligned} \tag{3}$$

considering our leakage model given in Equation (1). Here f_{σ^2} denotes Gaussian distribution with the mean value 0 and the standard deviation σ.

2.4 Distance-of-Means Attack

Originally introduced in [16], Distance-of-Means attack, abbreviated as DoM, employs a binary classification process before conducting a statistical test. Specifically, leakage corresponding to the same binary model value under a candidate

k will fall into the same class, indicating that they may share vary similar characteristics. Distance-of-Means statistical test is then applied to verify the correctness of classification under candidate k, and the incorrect candidates will eventually lead to misclassification where elements assigned to the same class approach random. In this case, only very limited difference can be detected between the two classes. Adversaries are able to identify k^* when a candidate k satisfies $k = k^*$. DoM can be written as follows:

$$\mathcal{D}_{\mathsf{DoM}} = \arg\max_{k \in \mathbb{F}_2^n} \frac{\sum_{q=1}^{Q} \hat{x}_q \times \varphi(t_q \oplus k)}{\sum_{q=1}^{Q} \varphi(t_q \oplus k)} - \frac{\sum_{q=1}^{Q} \hat{x}_q \times (1 - \varphi(t_q \oplus k))}{Q - \sum_{q=1}^{Q} \varphi(t_q \oplus k)}, \tag{4}$$

where $\varphi(x) \in \{0, 1\}$.

2.5 Success Rate

As a generic security metric, success rate [27] of a side-channel adversary is defined as follows: the adversary $\mathcal{A}$ is an algorithm to the target implementation. Its goal is to select the secret subkey k^* from all the subkey candidates $k \in \mathcal{K}$ by exploiting its collected information. To achieve this goal, we assume that the output of the adversary $\mathcal{A}$ is a score vector $\mathbf{s} = [s_1, s_2, \ldots, s_{|\mathcal{K}|}]$. Each score relates to the probability that the corresponding candidate subkey k is the secret subkey k^*. A larger score means that the corresponding candidate subkey k is more likely to be the secret subkey k^*. Finally, we can define an order of possibilities for the secret subkey k^* as follows:

$$g(k^*) = \sum_{k \in \mathcal{K}} \mathbb{1}(s_k \geq s_{k^*}). \tag{5}$$

The o^{th}-order success rate of the side-channel subkey recovery adversary $\mathcal{A}$ is straightforwardly defined as:

$$SR^o(\mathcal{A}) = \mathbb{P}[g(k^*) \leq o]. \tag{6}$$

2.6 Confusion Coefficient

Let τ denote the output of the leakage function φ, which is a key-dependent and thereby security-critical intermediate value, i.e., $\tau = \varphi(t \oplus k)$. Referring to [9, 10], two subkey candidates k_i and k_j under the same plaintext t may produce different outputs, which can be denoted as $\tau|k_i$ and $\tau|k_j$ respectively. The behavior of $\tau|k_i$ and $\tau|k_j$ affects how difficult it is for side-channel attacks to distinguish $k_i(k_j)$ from $k_j(k_i)$ by leakage measured. The original confusion coefficient κ, proposed in [10], measures the differences between behavior of $\tau|k_i$ and $\tau|k_j$ under a binary model as:

$$\kappa(k_i, k_j) = \mathbb{P}[(\tau|k_i \neq \tau|k_j)]. \tag{7}$$

If τ has more than two values, confusion coefficient measures the differences by calculating the expectation of squared distance [9]. Specifically, this general two-way confusion coefficient can be defined as:

$$\kappa(k_i, k_j) = \mathbb{E}[(\tau|k_i - \tau|k_j)^2]. \tag{8}$$

One can easily proof that $\mathbb{E}[(\tau|k_i - \tau|k_j)^2]$ is equal to probability $\mathbb{P}[(\tau|k_i \neq \tau|k_j)]$ under a binary model.

3 Unified Framework for Univariate DPA Attacks

The relationship between efficiency of different univariate DPA attacks is an important and basic issue of great concern. As discussed in [20], when fed with the same assumptions about the target device (i.e., with the same leakage model), the most popular approaches such as DoM test, correlation analysis (CPA) and Bayes attack, are essentially equivalent in this setting. Differences observed in practice are not due to differences in the statistical tests but statistical artifacts from which no intuition can be extracted. Their work provides a rigorous mathematical deduction and the experimental results remain convincing. As an extension and supplement, instead of transforming mathematical expressions straightforwardly, we propose a unified framework with which the mathematical foundation behind different univariate DPA attacks can be revealed and explained in a natural and intuitive manner, putting understanding of the relationship between them to a higher degree.

3.1 Leakage Feature Space

Euclidean space and coordinate system are suitable ways of intuitively revealing and explaining the common mathematical principle that different side-channel distinguishers are based on. For this purpose, we introduce leakage feature space, denoted as $\mathcal{V} = \mathbf{R}^Q$, as an effective and unified framework for distinguisher description and abstraction. This leakage feature space $\mathcal{V}$ is a kind of Euclidean space with flexible number of dimensions, says Q, that is equivalent to the size of the sample set X. Thereafter, the whole sample set X is bijectively mapped to a point (vector), denoted as $\mathcal{X}$ ($\vec{\mathcal{X}}$, respectively), in the leakage feature space $\mathcal{V}$ with element $\hat{x}_q$ accounting for the q-th dimensional coordinate value. In other words, $\mathcal{X}(\vec{\mathcal{X}}) = (\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_Q)$. Obviously, affected by additive Gaussian noise N, the location of $\mathcal{X}$ in $\mathcal{V}$ is not fixed and varies under different times of sampling. Thus, we may turn to its mathematical expectation for analysis: $\mathbb{E}\{\mathcal{X}\} = (\mathbb{E}\{\hat{x}_1\}, \mathbb{E}\{\hat{x}_2\}, \ldots, \mathbb{E}\{\hat{x}_Q\}) = (\alpha \cdot \varphi(t_1 \oplus k^*), \alpha \cdot \varphi(t_2 \oplus k^*), \ldots, \alpha \cdot \varphi(t_Q \oplus k^*))$.

It is noteworthy that:

- Compared to $\mathcal{X}(\vec{\mathcal{X}})$, $\mathbb{E}\{\mathcal{X}\}$ is mapped to a fixed point (vector) that contains and implies key-dependent side-channel leakage feature under certain secret key k^* and certain plaintext set $(t_1, t_2, \ldots, t_Q)$. Moreover, the location of $\mathbb{E}\{\mathcal{X}\}$ significantly decides which guessing value k is more difficult to be

distinguished from k^* and to what extent. Nevertheless, $\mathbb{E}\{\mathcal{X}\}$ is unknown to adversaries because of uncertainty of the secret key k^*.

- Adversaries observe $\mathcal{X}(\vec{\mathcal{X}})$. Given that additive Gaussian noise N applying to each dimension of $\mathcal{X}(\vec{\mathcal{X}})$ is mutually independent, the probability of occurrence of event $\mathcal{X}(\vec{\mathcal{X}})$ can be expressed as:

$$\begin{aligned}\mathbb{P}\left\{\mathcal{X}(\vec{\mathcal{X}})\right\} &= \left(\frac{1}{\sqrt{2\pi}\sigma}\right)^{Q} \exp\left(-\frac{1}{2\sigma^2}\sum_{q=1}^{Q}\left(\hat{x}_q - \alpha\cdot\varphi\left(t_q \oplus k^*\right)\right)^2\right) \\ &= \left(\frac{1}{\sqrt{2\pi}\sigma}\right)^{Q} \exp\left(-\frac{1}{2\sigma^2}|\vec{\mathcal{X}} - \vec{\mathbb{E}}\{\mathcal{X}\}|^2\right).\end{aligned} \tag{9}$$

Interestingly, we find that $Pr\left\{\mathcal{X}(\vec{\mathcal{X}})\right\}$ only depends on Euclidean distance between point $\mathcal{X}$ and point $\mathbb{E}\{\mathcal{X}\}$. Hence, we obtain an expression of probability density function in leakage feature space $\mathcal{V}$ as:

$$\phi(r) = \left(\frac{1}{\sqrt{2\pi}\sigma}\right)^{Q} \exp\left(-\frac{r^2}{2\sigma^2}\right), \tag{10}$$

where r represents Euclidean distance from point $\mathbb{E}\{\mathcal{X}\}$. In virtue of the famous "3σ" principal of Gaussian distribution, we can easily identify a sound neighborhood range where $\mathcal{X}(\vec{\mathcal{X}})$ randomly walks. Let $U(\mathbb{E}\{\mathcal{X}\}, 3\sigma)$ denote this neighborhood range and it turns into a suprasphere of radius 3σ whenever $Q > 3$. We can always expect that the observed $\mathcal{X}(\vec{\mathcal{X}})$ falls in it.

- Adversaries may know an estimation of φ due to Kerckhoffs's principle and their efforts to carefully characterize cryptosystem. In side-channel attacks, adversaries guess k^* and subsequently calculate $\{\varphi(t_1 \oplus k), \varphi(t_2 \oplus k), \ldots, \varphi(t_Q \oplus k)\}$, with k representing the guessing value. Similarly, this process can be naturally and conveniently abstracted and then mapped to leakage feature space $\mathcal{V}$ by introducing the point $\xi(k) = (\varphi(t_1 \oplus k), \varphi(t_2 \oplus k), \ldots, \varphi(t_Q \oplus k))$. Obviously, $\mathbb{E}\{\mathcal{X}\} = \alpha \cdot \xi(k^*)$.

Thanks to leakage feature space $\mathcal{V}$, we are able to abstract and view standard univariate DPA side-channel attacks as a process of analyzing potential '*similarity*' and '*association*' between distributions of the observed $\mathcal{X}(\vec{\mathcal{X}})$ and $\xi(k)$ in $\mathcal{V}$. Specifically, different statistical tests in DoM test, correlation analysis(CPA) and Bayes attack are exactly equivalent to detect and measure the '*similarity*' and '*association*' from the aspect of vector projection, vector cosine and vector Euclidean distance respectively. We will demonstrate that our views of these distinguishers largely inspire novel but straightforward conclusions and understanding.

3.2 Bayes attack

As introduced in Section 2.3, based on the maximum likelihood principle, Bayes attack is usually assumed to be much more powerful. One non-negligible drawback is that there exists a gap in practice: adversaries have to deal with problem

of parameters estimation. Probability density function involved can be calculated if and only if parameters α and σ are properly estimated. In our work, for better illustration of the underlying mathematical principle, we assumed that adversaries know the precise α and σ.

In leakage feature space $\mathcal{V}$, Bayes distinguisher follows:

$$\begin{aligned} \mathcal{D}_{\mathsf{Bayes}} &= \arg\max_{k\in\mathcal{K}} \prod_{q=1}^{Q} \mathbb{P}\{\hat{x}_q|k\} \\ &= \arg\max_{k\in\mathcal{K}} \prod_{q=1}^{Q} f_{\sigma^2}(\hat{x}_q - \alpha\cdot\varphi(t_q\oplus k)) \\ &= \arg\min_{k\in\mathcal{K}} |\vec{\mathcal{X}} - \alpha\vec{\xi}(k)\,|^2, \end{aligned} \tag{11}$$

where f_{σ^2} denotes Gaussian distribution with the mean value 0 and the standard deviation σ. Equation (11) well shows that Bayes distinguisher selects candidate k entirely according to Euclidean distance between the observed sample point $\mathcal{X}$ and point $\alpha\cdot\xi\,(k)$. Candidate k corresponding to the minimum Euclidean distance is regarded as the secret k^*.

The mathematical principle behind in Bayes distinguisher can be explained from leakage feature space $\mathcal{V}$ perspective: point $\mathcal{X}$ mostly takes a random walk in neighborhood $U\left(\alpha\cdot\xi\left(k^*\right),3\sigma\right)$. The probability that it happens to reach and be observed in another neighborhood $U\left(\alpha\cdot\xi\left(k^\circ\right),3\sigma\right)$ with $k^\circ\neq k^*$, and thereafter is closer to point $\alpha\cdot\xi\left(k^\circ\right)$, is relatively low. By applying Euclidean distance, Bayes distinguisher measures and tells which neighborhood is most likely the observed $\mathcal{X}$ actually and originally belongs to.

Meanwhile, we can conclude that the effectiveness of Bayes distinguisher is up to the overlapped part of $U\left(\alpha\cdot\xi\left(k^\circ\right),3\sigma\right)$ and $U\left(\alpha\cdot\xi\left(k^*\right),3\sigma\right)$, which may confuse and mislead the Bayes distinguisher. Intuitively, confusion coefficient on plaintext set $(t_1,t_2,\ldots,t_Q)$ and (k^*,k°) is a suitable tool for quantifying such an overlap, by measuring the Euclidean distance between centers of neighborhoods as follows:

$$\begin{aligned} \alpha^2\cdot Q\cdot\kappa\left(k^*,k^\circ\right) &= \textstyle\sum_{q=1}^{Q}\left\{\left(\alpha\cdot\varphi(t_q\oplus k^*)-\alpha\cdot\varphi(t_q\oplus k^\circ)\right)^2\right\} \\ &= \left|\alpha\vec{\xi}(k^*)-\alpha\vec{\xi}(k^\circ)\right|^2. \end{aligned} \tag{12}$$

3.3 CPA

CPA is another fairly generic distinguisher that has been well studied. The statistical test embedded is the well-known Pearson's correlation coefficient as given in Equation (2). Due to its complexity, dedicated works [14,20,25] have proposed several important characteristics of side-channel attack scenario, achieving desired results in simplifying and facilitating the analysis and evaluations of this distinguisher. Note that we are not indicating that launching direct analysis

against sample distribution of Pearson's correlation coefficient, such as using Fisher z-transformation [4], is unnecessary. Here we briefly illustrate them as following:

- The first and second moments of sample set X are constant and independent of guessing value k [25]. In other words, as soon as adversaries finish their sampling on target cryptosystem, these two moments are determined and remain constant regardless of side-channel distinguishers used.
- Property of Equal Images under different Subkeys (EIS) [26]. Let $\mathcal{A}$ be an arbitrary set and $\varphi : \mathcal{T} \times \mathcal{K} \to \mathcal{A}$ be a mapping for which the images $\varphi(\mathcal{T} \times k) \subset \mathcal{A}$ are equal for all subkey $k \in \mathcal{K}$. Property of EIS indicates that though the first and second moments of $\{\varphi(t_1 \oplus k), \varphi(t_2 \oplus k), \ldots, \varphi(t_Q \oplus k)\}$ may vary under different guessing key k, there leaves no extra information about k^* that can be extracted from these differences.

Based on above characteristics, [14] simplified Pearson's correlation coefficient in side-channel attack scenario up to an additive distinguisher $\mathcal{D}_{\mathsf{CPA}} = \arg\max_{k\in\mathcal{K}} \sum_{q=1}^{Q} \hat{x}_q \times \varphi(t_q \oplus k)$ and subsequently developed a feasible security bound for success rate metrics, which has attracted wide attention. Inspired by their works, we simplify CPA distinguisher in leakage feature space $\mathcal{V}$ as following:

$$\begin{aligned} \mathcal{D}_{\mathsf{CPA}} &= \arg\max_{k\in\mathcal{K}} \frac{\sum_{q=1}^{Q} \hat{x}_q \times \varphi(t_q \oplus k)}{\sqrt{\sum_{q=1}^{Q} \hat{x}_q^2}\sqrt{\sum_{q=1}^{Q} \varphi^2(t_q \oplus k)}} \\ &= \arg\max_{k\in\mathcal{K}} \; cos < \vec{\mathcal{X}}, \vec{\xi}(k) > . \end{aligned} \tag{13}$$

The mathematical principle behind is very similar with that of Bayes attack from leakage feature space $\mathcal{V}$ perspective. The main difference is that instead of measuring Euclidean distance, CPA chooses to measure the so-called "*cosine similarity*" between vectors. It is noteworthy that the Euclidean distance $|\xi(k^*) - \xi(k)|$ has a very close connection with $cos < \xi(k^*), \xi(k) >$. More specifically, one can easily proof that $|\xi(k^*) - \xi(k)|$ is a monotonously decreasing function of $cos < \xi(k^*), \xi(k) >$. As a result, on one hand, we believe that more or less Bayes attack links with CPA at a certain extent. On the other hand, we verify that the effectiveness of CPA distinguisher is also up to the confusion coefficient $\kappa(k^*, k)$, which has already been mentioned and investigated in [9, 10].

3.4 DoM Test

Compared to Bayes attack and CPA, DoM test assumes a binary leakage model, which brings additional noise under the same circumstances. This is because there are more bits that are not under consideration and their random shifts produce extra irrelevant "*algorithmic noise*" [8]. Using our notation and following the normalization this means that $\varphi \in \{-1, 1\}$. In leakage feature space $\mathcal{V}$

adversaries select key candidate as:

$$\begin{aligned}\mathcal{D}_{\mathsf{DoM}} &= \arg\max_{k\in\mathcal{K}} \frac{\frac{1}{2}\sum_{q=1}^{Q}\hat{x}_q \times (\varphi(t_q \oplus k)+1)}{\frac{1}{4}\sum_{q=1}^{Q}(\varphi(t_q \oplus k)+1)^2} + \frac{\frac{1}{2}\sum_{q=1}^{Q}\hat{x}_q \times (\varphi(t_q \oplus k)-1)}{\frac{1}{4}\sum_{q=1}^{Q}(\varphi(t_q \oplus k)-1)^2} \\ &= \arg\max_{k\in\mathcal{K}} \; Proj < \vec{\mathcal{X}}, \vec{\varrho}(k) >,\end{aligned} \tag{14}$$

where $\vec{\varrho}(k) = \frac{\vec{\xi}(k)+\vec{1}}{|\vec{\xi}(k)+\vec{1}|^2} + \frac{\vec{\xi}(k)-\vec{1}}{|\vec{\xi}(k)-\vec{1}|^2}$, $\vec{1}$ is the vector with all dimensions equal 1, and $Proj < \vec{\mathcal{X}}, \vec{\varrho}(k) >$ represents the projection of $\vec{\varrho}(k)$ on $\vec{\mathcal{X}}$. Significantly, the vector projection DoM turns to is determined both by $cos < \vec{\mathcal{X}}, \vec{\varrho}(k) >$ and $|\vec{\varrho}(k)|$. Though $\varphi \in \{-1, 1\}$, property of EIS remains, indicating that we do not need to concern the differences in $|\vec{\varrho}(k)|$. $\kappa(k^*, k)$ still plays an important role in evaluation of DoM attack.

4 Unified Evaluation Framework for Univariate DPA Attacks

In Section 3, we proposed a unified framework, namely leakage feature space $\mathcal{V}$. Basing on it, we conclude that different distinguishers of univariate DPA attack can essentially be unified as a process of analyzing potential '*similarity*' and '*association*' between distributions of the observed $\mathcal{X}(\vec{\mathcal{X}})$ and $\xi(k)$, while relying on diverse similarity measure metrics. As presented in Section 2.1, adversaries know exactly the plaintext set $\{t_1, t_2, \cdots, t_Q\}$ that corresponds to the leakage they measured. Hence, the location of point $\xi(k)$ in leakage feature space $\mathcal{V}$ remains constant whenever guessing value k is determined. The only random factor that affects the success (failure) of a univariate DPA attack is the distribution of $\mathcal{X}(\vec{\mathcal{X}})$. From this point of view, one can deduce that the whole leakage feature space $\mathcal{V}$ is at least divided into two parts, of which one represents "*success space*". If $\mathcal{X}(\vec{\mathcal{X}})$ falls and is observed in the "*success space*", side-channel attacks succeed. The detailed distribution and shape of "*success space*" in $\mathcal{V}$ depends on the plaintext set assumed to be known in the most common attack scenarios, secret key and distinguisher actually used, which will be analyzed and detailed subsequently.

For better understanding our proposed unified evaluation framework, we start our elaboration by differentiating secret key k^* from candidate pair (k^*, k°) with k° being an arbitrary guessing subkey out of $|\mathcal{K}| - 1$ wrong candidates. Then we extend our scheme to scenario of all $|\mathcal{K}|$ candidates, thus making it more practical for side-channel evaluations.

4.1 First-Order Boundary of Success Space

To identify the "*success space*" in leakage feature space $\mathcal{V}$, locating and determining the corresponding, maybe nonlinear, boundary that surrounds it is of

particular necessity. The first-order boundary of the success space is the foundation for analysis of the first-order success rate. We can infer that when $\mathcal{X}(\vec{\mathcal{X}})$ falls on the first-order boundary, more than one candidate, of which the probability to be the secret subkey is completely the same, are ranked simultaneously at the first place of the score vector. The corresponding status of the side-channel attack is somewhere between success and failure.

We begin our analysis with the success space under certain candidate pair (k^*, k°) and certain plaintext set $(t_1, t_2, \ldots, t_Q)$. Let ω denote an arbitrary element that belongs to the first-order boundary.

- In Bayes attack, candidate that leads to the minimum Euclidean distance $|\vec{\mathcal{X}} - \alpha\vec{\xi}(k)|$ is considered as the secret subkey. Element of the first-order boundary in Bayes attack satisfies:

$$|\vec{\omega} - \alpha\vec{\xi}(k^\circ)| = |\vec{\omega} - \alpha\vec{\xi}(k^*)|, \tag{15}$$

  indicating the case where Bayes distinguisher cannot tell which one of (k°, k^*) has greater possibility to be the secret subkey. Finally, let 'T' represents matrix transposition, and we derive the equation of the first-order boundary in leakage feature space $\mathcal{V}$ as:

$$\left(\vec{\xi}(k^\circ) - \vec{\xi}(k^*)\right)^T \vec{\omega} - \frac{\alpha}{2}\left(|\vec{\xi}(k^\circ)|^2 - |\vec{\xi}(k^*)|^2\right) = 0, \tag{16}$$

  which turns out to be a hyperplane, denoted as $\mathbb{H}_{\mathsf{Bayes}}(k^\circ)$, that linearly divides leakage feature space $\mathcal{V}$ into two parts. Between these two parts, let $\mathfrak{I}^1_{\mathsf{Bayes}}(k^\circ)$ denote the first-order success space, and $\bar{\mathfrak{I}}^1_{\mathsf{Bayes}}(k^\circ)$ denote the remaining part (failure space), i.e., $\mathcal{V} = \mathfrak{I}^1_{\mathsf{Bayes}}(k^\circ) \bigcup \bar{\mathfrak{I}}^1_{\mathsf{Bayes}}(k^\circ)$. Apparently, $\xi(k^*) \in \mathfrak{I}^1_{\mathsf{Bayes}}(k^\circ)$.
- In CPA, candidate that leads to the maximum cosine $cos < \vec{\mathcal{X}}, \vec{\xi}(k) >$ is considered as the secret subkey. Element of the first-order boundary in CPA satisfies:

$$cos < \vec{\omega}, \vec{\xi}(k^\circ) >= cos < \vec{\omega}, \vec{\xi}(k^*) > . \tag{17}$$

  The corresponding equation in CPA is then as:

$$\left(\frac{\vec{\xi}(k^\circ)}{|\vec{\xi}(k^\circ)|} - \frac{\vec{\xi}(k^*)}{|\vec{\xi}(k^*)|}\right)^T \vec{\omega} = 0, \tag{18}$$

  which is also a hyperplane and is denoted as $\mathbb{H}_{\mathsf{CPA}}(k^\circ)$. Similarly, we can define $\mathfrak{I}^1_{\mathsf{CPA}}(k^\circ)$ and $\bar{\mathfrak{I}}^1_{\mathsf{CPA}}(k^\circ)$.
- In DoM, candidate that leads to the maximum vector projection $Proj < \vec{\mathcal{X}}, \vec{\varrho}(k) >$ is considered as the secret subkey. Element of the first-order boundary in DoM satisfies:

$$Proj < \vec{\omega}, \vec{\varrho}(k^\circ) >= Proj < \vec{\omega}, \vec{\varrho}(k^*) > . \tag{19}$$

The corresponding equation in DoM is then as:

$$\left(\vec{\varrho}(k^{\circ}) - \vec{\varrho}(k^{*})\right)^{T} \vec{\omega} = 0, \tag{20}$$

which is another hyperplane and is denoted as $\mathbb{H}_{\mathsf{DoM}}(k^{\circ})$. Again, we can define $\mathfrak{I}^{1}_{\mathsf{DoM}}(k^{\circ})$ and $\tilde{\mathfrak{I}}^{1}_{\mathsf{DoM}}(k^{\circ})$.

Based on above deductions, we offer a sketch map in Figure 4.1 for the sake of intuition. We now extend the first-order boundary of success space under certain candidate pair (k°, k^{*}) to **scenario of all $|\mathcal{K}|$ candidates**. Owing to the arbitrariness of k° from $|\mathcal{K}| - 1$ wrong candidates, one can naturally reason that the complete nonlinear first-order boundary of success space is consisted of $|\mathcal{K}| - 1$ linear but provably unparallel hyperplanes in $\mathcal{V}$. More specifically, take the Bayes attack as an example, the first-order boundary under certain plaintext set $(t_1, t_2, \ldots, t_Q)$ and all $|\mathcal{K}|$ candidates can be expressed using the following $|\mathcal{K}| - 1$ equations:

$$Bound^{1}_{\mathsf{Bayes}} = \begin{cases} \left(\vec{\xi}\left(k^{1}\right) - \vec{\xi}(k^{*})\right)^{T} \vec{\omega} - \dfrac{\alpha}{2}\left(|\vec{\xi}\left(k^{1}\right)|^{2} - |\vec{\xi}(k^{*})|^{2}\right) = 0, \\ \left(\vec{\xi}\left(k^{2}\right) - \vec{\xi}(k^{*})\right)^{T} \vec{\omega} - \dfrac{\alpha}{2}\left(|\vec{\xi}\left(k^{2}\right)|^{2} - |\vec{\xi}(k^{*})|^{2}\right) = 0, \\ \ldots \\ \left(\vec{\xi}\left(k^{|\mathcal{K}|-1}\right) - \vec{\xi}(k^{*})\right)^{T} \vec{\omega} - \dfrac{\alpha}{2}\left(|\vec{\xi}\left(k^{|\mathcal{K}|-1}\right)|^{2} - |\vec{\xi}(k^{*})|^{2}\right) = 0, \end{cases} \tag{21}$$

where $\{k^{1}, \cdots, k^{|\mathcal{K}|-1}\}$ denotes the $|\mathcal{K}|-1$ wrong candidates of the secret subkey. As a result, the complete first-order success space satisfies:

$$\mathfrak{I}^{1}_{\mathsf{Bayes}} = \bigcap_{k \in \mathcal{K} \setminus \{k^{*}\}} \mathfrak{I}^{1}_{\mathsf{Bayes}}(k). \tag{22}$$

Although equations of the first-order boundary in different univariate DPA attacks seem entirely irrelevant at the first sight, there is a significant and interesting observation: Due to the EIS property and for any given number of leakage samples Q, the distribution of $|\vec{\xi}(k)|$ is independent of Gaussian noise N and is equal for all subkey candidates k. In other words, biases observed between $|\vec{\xi}(k)|$ are caused by unbalanced plaintext set rather than k. Meanwhile, the variance of the sample distribution of $|\vec{\xi}(k)|$ is a monotonously decreasing function of Q. Therefore, as σ increases, to achieve the same success rate, it is necessary to increase Q to make every $|\vec{\xi}(k)|$ approach the same level. In conclusion, when $Q \to +\infty$ or balanced plaintext set is in use, statistical artifacts bought by plaintext set is eliminated and thus all $|\vec{\xi}(k)|$ turn to their mathematical expectation, indicating that for $\forall k^{1}, k^{2} \in \mathcal{K}, k^{1} \neq k^{2}$ we have $|\vec{\xi}\left(k^{1}\right)| = |\vec{\xi}\left(k^{2}\right)|$. In this case, one can easily simplify the first-order boundary of different univariate DPA attacks under certain candidate pair (k^{*}, k°) to a unified mathematical expression:

$$\left(\vec{\xi}(k^{\circ}) - \vec{\xi}(k^{*})\right)^{T} \vec{\omega} = 0. \tag{23}$$

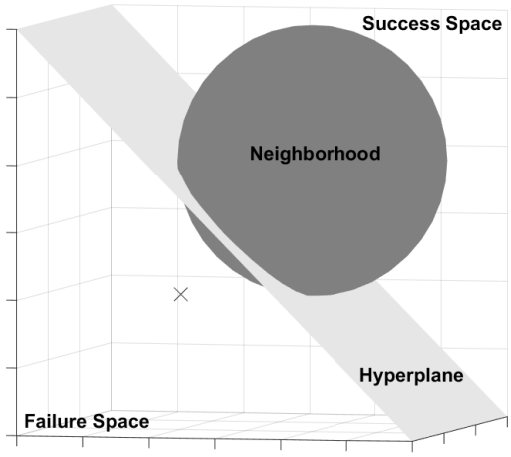

Fig. 1. A sketch map of boundary and success space.

More importantly, Bayes attack and CPA share the same leakage function φ, which implies the same expectation of the first-order boundary, and therefore the same expectation of their first-order success rate, i.e., $\mathbb{E}\left(\mathfrak{I}^1_{\mathsf{Bayes}}\right) = \mathbb{E}\left(\mathfrak{I}^1_{\mathsf{CPA}}\right)$. This further verifies the conclusion and observation mentioned in [20] that the efficiency of side-channel attacks using correlation coefficient and a Bayes distinguisher is statistically close, i.e., the small differences observed in practice are not due to the statistical test but statistical artifacts brought by unbalanced plaintext set).

Eventually, the expectation of first-order boundary of different univariate DPA attacks in scenario of all $|\mathcal{K}|$ candidates can be expressed using the following $|\mathcal{K}| - 1$ equations:

$$\mathbb{E}\left\{Bound^1\right\} = \begin{cases} \left(\vec{\xi}\left(k^1\right) - \vec{\xi}(k^*)\right)^T \vec{\omega} = 0, \\ \left(\vec{\xi}\left(k^2\right) - \vec{\xi}(k^*)\right)^T \vec{\omega} = 0, \\ \ldots \\ \left(\vec{\xi}\left(k^{|\mathcal{K}|-1}\right) - \vec{\xi}(k^*)\right)^T \vec{\omega} = 0. \end{cases} \tag{24}$$

Let $\vec{\eta}(k)$ denote the normal vector of hyperplane $\mathbb{H}(k)$ that belongs to the expectation, then $\vec{\eta}(k) = \vec{\xi}(k) - \vec{\xi}(k^*)$. To find out the distribution and shape

of the expectation, we calculate cosine between every two of $\vec{\eta}(k)$ as follows:

$$\begin{aligned} cos < \vec{\eta}(k^{\circ}), \vec{\eta}\left(k^{\#}\right) > &= \frac{\vec{\eta}(k^{\circ}) \cdot \vec{\eta}\left(k^{\#}\right)}{|\vec{\eta}(k^{\circ})||\vec{\eta}(k^{\#})|} \\ &= \frac{\kappa(k^{*}, k^{\circ}) + \kappa\left(k^{*}, k^{\#}\right) - \kappa\left(k^{\#}, k^{\circ}\right)}{2\sqrt{\kappa(k^{*}, k^{\circ})\,\kappa(k^{*}, k^{\#})}}, \end{aligned} \tag{25}$$

where k° and $k^{\#}$ denote two different values from $|\mathcal{K}|-1$ wrong candidates. It is remarkable that the distribution and shape of the expectation of the first-order boundary is independent of Q and SNR.

4.2 Derivation of First-Order Success Rate

From leakage feature space $\mathcal{V}$ perspective, the first-order success rate of a side-channel attack $\mathcal{A}$ is defined as the probability of $\mathcal{X}(\vec{\mathcal{X}})$ staying in the success space $\mathfrak{I}$ without crossing the first-order boundary. Therefore, the first-order success rate in Equation (6) can be re-expressed as:

$$SR^{1}(\mathcal{A}) = \frac{\mathbb{P}\{\mathcal{X} \in \mathfrak{I}^{1}\}}{\mathbb{P}\{\mathcal{X} \in \mathcal{V}\}} = 1 - \frac{\mathbb{P}\{\mathcal{X} \in \bar{\mathfrak{I}}^{1}\}}{\mathbb{P}\{\mathcal{X} \in \mathcal{V}\}}, \tag{26}$$

where $\mathbb{P}\{\mathcal{X} \in \mathcal{V}\} = 1$.

In the following, we derive the expression of the first-order success rate. As a starting point, we begin our derivation under certain candidate pair (k^{*}, k°) and certain plaintext set $(t_1, t_2, \ldots, t_Q)$. In this case, the first-order boundary is a hyperplane $\mathbb{H}$ whose equation was given in Section 4.1. To calculate $\mathbb{P}\{\mathcal{X} \in \bar{\mathfrak{I}}\}$, let us first consider straight line γ passing point $\alpha \cdot \xi(k^{*})$ (i.e., point $\mathbb{E}\{\mathcal{X}\}$) and whose direction vector is parallel to the normal vector $\vec{\eta}$ of hyperplane $\mathbb{H}$. Noting that $\alpha \cdot \xi(k^{*})$ is the same for Bayes attack and CPA because of the same underlying leakage function φ. Apparently, γ is divided into two parts by $\mathbb{H}$ as well and similarly we denote the part in space $\bar{\mathfrak{I}}$ as $\bar{\gamma}$. Take advantage of Equation (10), we get:

$$\frac{\mathbb{P}\{\mathcal{X} \in \bar{\gamma}\}}{\mathbb{P}\{\mathcal{X} \in \gamma\}} = \frac{\int_{\mathfrak{L}}^{+\infty} \phi(r)\, dr}{\int_{-\infty}^{+\infty} \phi(r)\, dr} = \frac{\left(\frac{1}{\sqrt{2\pi}\sigma}\right)^{Q-1} \left(1 - \Phi_{\sigma^2}(\mathfrak{L})\right)}{\left(\frac{1}{\sqrt{2\pi}\sigma}\right)^{Q-1}} = 1 - \Phi_{\sigma^2}(\mathfrak{L}), \tag{27}$$

where $\mathfrak{L}$ denotes the Euclidean distance between point $\alpha \cdot \xi(k^{*})$ and the first-order boundary (i.e., the hyperplane $\mathbb{H}(k^{\circ})$ in this case) and $\Phi_{\sigma^2}(.)$ denotes the Gaussian cumulative distribution function (cdf) with the mean value 0 and the standard deviation σ. For certain candidate pair (k^{*}, k°) and certain, maybe unbalanced, plaintext set $(t_1, t_2, \ldots, t_Q)$, calculation of $\mathfrak{L}$ is specific to the distinguisher used. Specifically, $\mathfrak{L}$ for Bayes attack is:

$$\mathfrak{L}_{\mathsf{Bayes}} = \frac{|| \left(\vec{\xi}(k^{\circ}) - \vec{\xi}(k^{*})\right)^{T} \alpha \vec{\xi}(k^{*}) - \frac{\alpha}{2}\left(|\vec{\xi}(k^{\circ})|^{2} - |\vec{\xi}(k^{*})|^{2}\right) ||}{|\vec{\xi}(k^{\circ}) - \vec{\xi}(k^{*})|}, \tag{28}$$

$\mathfrak{L}$ for CPA is:

$$\mathfrak{L}_{\mathsf{CPA}} = \frac{|| \left(\frac{\vec{\xi}(k^\circ)}{|\vec{\xi}(k^\circ)|} - \frac{\vec{\xi}(k^*)}{|\vec{\xi}(k^*)|} \right)^T \alpha \vec{\xi}(k^*) ||}{|\frac{\vec{\xi}(k^\circ)}{|\vec{\xi}(k^\circ)|} - \frac{\vec{\xi}(k^*)}{|\vec{\xi}(k^*)|}|}, \tag{29}$$

and $\mathfrak{L}$ for DoM distinguisher is:

$$\mathfrak{L}_{\mathsf{DoM}} = \frac{|| \left(\vec{\varrho}(k^\circ) - \vec{\varrho}(k^*) \right)^T \alpha \vec{\xi}(k^*) ||}{|\vec{\varrho}(k^\circ) - \vec{\varrho}(k^*)|}. \tag{30}$$

Note that $||\cdot||$ denotes the operation of getting absolute value and $|\cdot|$ denotes the operation of getting vector module.

Next, let us consider another straight line β which is parallel to γ. Let θ denote the Euclidean distance between β and γ. Similarly, we are interested in:

$$\frac{\mathbb{P}\{\mathcal{X} \in \bar{\beta}\}}{\mathbb{P}\{\mathcal{X} \in \beta\}} = \frac{\int_{\mathfrak{L}}^{+\infty} \phi\left(\sqrt{r^2+\theta^2}\right) dr}{\int_{-\infty}^{+\infty} \phi\left(\sqrt{r^2+\theta^2}\right) dr}, \tag{31}$$

It is noteworthy that:

$$\phi\left(\sqrt{r^2+\theta^2}\right) = \left(\frac{1}{\sqrt{2\pi}\sigma}\right)^Q \exp\left(-\frac{r^2+\theta^2}{2\sigma^2}\right) = \hbar(\theta) \cdot \phi(r) \tag{32}$$

where $\hbar(\theta) = \exp\left(-\frac{\theta^2}{2\sigma^2}\right)$. Based on this, we subsequently acquire the result as follows:

$$\frac{\mathbb{P}\{\mathcal{X} \in \bar{\beta}\}}{\mathbb{P}\{\mathcal{X} \in \beta\}} = \frac{\hbar(\theta) \int_{\mathfrak{L}}^{+\infty} \phi(r)\, dr}{\hbar(\theta) \int_{-\infty}^{+\infty} \phi(r)\, dr} = 1 - \Phi_{\sigma^2}(\mathfrak{L}), \tag{33}$$

which is actually the same as Equation (27). Surprisingly, we find that the results is independent of θ. We draw a conclusion that the normal vector $\vec{\eta}(k^\circ)$ of the hyperplane $\mathbb{H}(k^\circ)$ spans the one-dimensional straight line γ, but together with the hyperplane $\mathbb{H}(k^\circ)$ itself, which is essentially a subspace with $Q-1$ dimensions, spans the whole Q-dimensional leakage feature space $\mathcal{V}$. Ultimately, we derive the expression of SR^1 under certain candidate pair (k^*, k°) and certain plaintext set $(t_1, t_2, \ldots, t_Q)$ as:

$$SR^1 = 1 - \frac{\mathbb{P}\{\mathcal{X} \in \bar{\mathfrak{I}}\}}{\mathbb{P}\{\mathcal{X} \in \mathcal{V}\}} = 1 - \frac{\mathbb{P}\{\mathcal{X} \in \bar{\gamma}\}}{\mathbb{P}\{\mathcal{X} \in \gamma\}} = \Phi_{\sigma^2}(\mathfrak{L}). \tag{34}$$

$\mathfrak{L}$ is determined by $\alpha \cdot \xi(k^*)$ and $\mathbb{H}$ which are both specific to the candidate pair (k^*, k°) and the plaintext set $(t_1, t_2, \ldots, t_Q)$.

In case that one may have particular interests in the expectation of SR^1 under the candidate pair (k^*, k°) but random plaintext set with fixed size Q, we derive the following results:

$$\mathbb{E}\{\mathfrak{L}\} = \mathbb{E}\left\{ \frac{|| \left(\vec{\xi}(k^\circ) - \vec{\xi}(k^*) \right)^T \alpha \vec{\xi}(k^*) ||}{|\vec{\xi}(k^\circ) - \vec{\xi}(k^*)|} \right\} = \frac{\alpha \sqrt{Q \times \kappa(k^*, k^\circ)}}{2} \tag{35}$$

according to Equations (10) and (8), and obtains:

$$\begin{aligned}\mathbb{E}\left\{SR^1\right\} =& \Phi_{\sigma^2}\left(\frac{\alpha\sqrt{Q\times\kappa\left(k^*,k^\circ\right)}}{2}\right)\\ =& 0.5+\frac{1}{2}\operatorname{erf}\left(\sqrt{\frac{1}{8}\times SNR\times Q\times\kappa\left(k^*,k^\circ\right)}\right).\end{aligned} \tag{36}$$

There are three interesting but very significant observations:

(1) If the SNR is decreased by a factor of m, the number of measurements Q has to be multiplied by m to achieve the same first-order success rate. This verifies the well-known "*Rule of Thumb*" for side-channel attacks as described in [18].

(2) $\mathbb{E}\left\{SR^1\right\} \geq 0.5$, indicating that conducting a side-channel attack by Bayes, CPA or DoM is always better than applying a random guess, regardless of SNR and Q. Further, the second item $\frac{1}{2}\operatorname{erf}\left(\sqrt{\frac{1}{8}\times SNR\times Q\times\kappa\left(k^*,k^\circ\right)}\right)$ can be seen as the gain of effectiveness brought by distinguishers, for the probability of a candidate randomly chosen from the candidate pair (k^*, k°) being the secret subkey is 0.50.

(3) Eventually, we find that the upper bound approximation used in [14, 18] and the corresponding idea [30] it refers to has a potential drawback. Note that this upper bound is originally designed to squeeze the success rate of scenario of all $|\mathcal{K}|$ candidates based on a candidate pair (k^*, k). Using our notations, the upper bound is expressed as:

$$SR^1 \leq \min_{k\neq k^*} \mathbb{P}\left\{g(k^*) < g(k)\right\}. \tag{37}$$

This implies that the upper bound is always greater than 0.50 and thus disagree with the fact that success rate observed and measured in practice can be much more lower. In conclusion, squeezing the success rate in scenario of all $|\mathcal{K}|$ candidates by calculating probability of correctly differentiating secret subkey k^* from certain candidate pair is somewhat inaccuracy.

Based on above deduction, the first-order success rate SR^1 in scenario of all $|\mathcal{K}|$ candidates under certain plaintext set $(t_1, t_2, \ldots, t_Q)$ can be calculated by performing a definite integral as follows:

$$SR^1 = \oiiint_{\mathfrak{I}^1} \phi\left(r\right) dr. \tag{38}$$

The first-order boundary restricts the upper and lower bounds of integral operation and the domain of integration is the first-order success space $\mathfrak{I}^1$ (e.g., Equation (22) for Bayes attack). As for $\mathbb{E}\left\{SR^1\right\}$, simply replacing $\mathfrak{I}^1$ with its expectation will do the job. It is worth mentioning that according to Equations (25) and (35), Q and SNR affect $\mathbb{E}\left\{SR^1\right\}$ by only affecting the Euclidean distance $\mathfrak{L}$. Therefore, we can further conclude that distribution of $\mathbb{E}\left\{Bound^1\right\}$ in leakage feature space $\mathcal{V}$ has a close connection to the behavior of φ (measured by the confusion coefficient) and is totally independent of Q and SNR.

4.3 From First-Order to Higher-Order Success Rate

Compared to the first-order success rate, higher-order implies an extra meaning by measuring the remaining workload of the adversary after the attack. To be specific, the o^{th}-order success rate indicates the probability that the adversary still has a maximum of o candidates to test after the attack. Therefore, we can infer that adversary who has ability to conduct additional statistical tests conveniently should prefer distinguishers with better success rate of higher-order, although SR^1 may be a bit low. Countermeasures against side-channel attacks should take these cases into consideration as well. In summary, the evaluation of higher-order success rate is of great importance and has been a long standing open problem. So far, however, there are hardly any methods or tools provide efficient and accurate estimation of higher-order success rate. Moreover, concise and intuitive explanation about the relationship between first-order and higher-order success rate is necessary for raising clear conclusions on how to estimate them. To fill this gap, we intuitively extend our first-order success space to higher-order scenario, and propose an algorithm that is capable of estimating success rate of arbitrary order in an efficient manner. Most importantly, we answer the question of why and how SR^o can be estimated according to (characteristics of) SR^1 and then put it into practice.

Here the o^{th}-order success rate of a side-channel attack $\mathcal{A}$ is defined as the probability of $\mathcal{X}(\vec{\mathcal{X}})$ staying in the success space $\mathfrak{I}$ without crossing the o^{th}-order boundary and thus can be re-expressed as:

$$SR^o\left(\mathcal{A}\right) = \frac{\mathbb{P}\{\mathcal{X} \in \mathfrak{I}^o\}}{\mathbb{P}\{\mathcal{X} \in \mathcal{V}\}} = 1 - \frac{\mathbb{P}\{\mathcal{X} \in \bar{\mathfrak{I}}^o\}}{\mathbb{P}\{\mathcal{X} \in \mathcal{V}\}}, \tag{39}$$

where $\mathfrak{I}^{(o)}$ represents the o^{th}-order success space $\mathfrak{I}^{(o)} = \bigcup(\mathfrak{I}(Bound^1 - \binom{|\mathcal{K}|-1}{o-1}\mathbb{H}))$. The subtraction operation $(Bound^1 - \binom{|\mathcal{K}|-1}{o-1}\mathbb{H})$ indicates that we randomly remove $o-1$ hyperplanes from the first-order boundary and thereby $\mathfrak{I}(Bound^1 - \binom{|\mathcal{K}|-1}{o-1}\mathbb{H})$ denotes the corresponding success space under this new boundary. The cancel of $o-1$ hyperplanes means that $\mathcal{X}$ is allowed to cross at most $o-1$ hyperplanes, resulting in at most $o-1$ wrong candidates being allowed to be placed in front of k^* in the score vector.

Although deriving accurate expression of $Bound^1$ is feasible, calculation of the integral in Equation (38) appears to be a troublesome and arduous problem. Besides, the challenge of computing higher-order success rate needs to be addressed in an efficient and intuitive way. To these ends, based on Monte Carlo method, we propose an algorithm that is capable of computing arbitrary order success rate under certain plaintext set in a very efficient way (see Algorithm 1).

Thanks to our unified framework given in leakage feature space $\mathcal{V}$, Algorithm 1 is general for Bayes attack, CPA and DoM. Let $H(k,x)$ denote function of hyperplane $\mathbb{H}\left(k\right)$, e.g., $H(k;x) = \left(\vec{\xi}(k) - \vec{\xi}(k^*)\right)^T \vec{x} - \frac{\alpha}{2}\left(|\vec{\xi}(k)\,|^2 - |\vec{\xi}(k^*)\,|^2\right)$ for $\mathbb{H}_{\mathsf{Bayes}}\left(k\right)$. Algorithm 1 takes the first-order boundary $H(k,x)$ as inputs (e.g., Equation (21) for Bayes Attack) and calculates the specified o^{th}-order success

Algorithm 1: The estimation on the o^{th}-order success rate.

Input: $|\mathcal{K}| - 1$ functions $H(k; x)$, order o, point $\xi(k^*)$.
Output: $\hat{SR}^o$.

1 Initialize a counter $suc = 0$;
2 **for** *i from 1 to 10000* **do**
3 Set success flag of an attack as: $sflag = 1$;
4 Initialize the position of x in the score vector as $pos = 1$;
5 Generate random sample x;
6 **for** k *in* $\{k^1, \cdots, k^{|\mathcal{K}|-1}\}$ **do**
7 **if** $H(k; x) \times H(k; \xi(k^*)) \leq 0$ **then**
8 $pos = pos + 1$;
9 **if** $pos \geq o$ **then**
10 $sflag = 0$; break;
11 **end**
12 **end**
13 **end**
14 $suc = suc + sflag$;
15 **end**
16 $\hat{SR}^o = suc/10000$;

rate. According to the well-known Bernoulli's theorem of large numbers in statistics, we estimate the result in Equation (38) by random sampling. Specifically, we set success flag for an attack as $sflag = 1$, initialize the position of x in the score vector as $pos = 1$, and generate a tremendous number of samples ($10,000$ samples in Algorithm 1) according to Equation (10) randomly to simulate the behavior of $\mathcal{X}(\vec{\mathcal{X}})$ (Steps $3 \sim 5$). By calculating frequency of samples falling in the o^{th}-order success space (Steps $6 \sim 12$), we thus approach SR^o (Steps $15 \sim 17$).

Due to expression of the first-order boundary, judging whether a certain sample falls in the o^{th}-order success space becomes a very simple task. To be specific, for sample x and a wrong candidate k°, we calculate $H(k^\circ; x) \times H(k^\circ; \xi(k^*))$ and see if it is greater than 0 (Step 7). If not, k° is ranked in front of k^* in the score vector. This is because $\xi(k^*) \in \mathfrak{I}^1(k^\circ)$ and x is on the other side of $\mathbb{H}(k^\circ)$, which is thereby the failure space $\bar{\mathfrak{I}}^1(k^\circ)$. Thus, by traversing $|\mathcal{K}| - 1$ wrong candidates (Step 6), we can eventually find out how many hyperplanes x have crossed. Using the definition of o^{th}-order success rate in Section 4.2, this means how many hyperplanes are removed from the first-order boundary.

5 Simulated Results

5.1 Validation of the Observations

In this section, we validate the observation in Section 4.2. In order to show that success rate of differentiating secret k^* from a candidate pair (k^*, k°) is always

greater 0.50 when applying a side-channel distinguisher, we conduct a simulated experiment where we can set SNR and Q to an extreme level (pretty close to 0). In the experiment, we assume the commonly used Hamming weight leakage function and AES-128 S-box. The candidate pair (k^*, k°) is set to $(212, 30)$ by applying simple random sampling method to set $\mathbb{F}_8^2$ which is the $\mathcal{K}$ in AES-128 scenario. In Figure 2, Q is fixed to 5 and α is fixed to 1. By increasing σ, SNR varies from a reasonable level to an extremely low level. In Figure 3, SNR is fixed to 0.01 and Q varies from 2 to 102. The step length is set to 5 and we repeat our experiment 2,000 times to get the empirical first-order success rate under different univariate DPA attacks. Theoretical results are calculated by Equation (36).

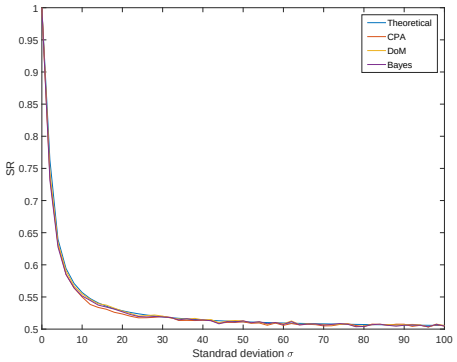

Fig. 2. SR^1 under candidate pair $(212, 30)$ and different SNR.

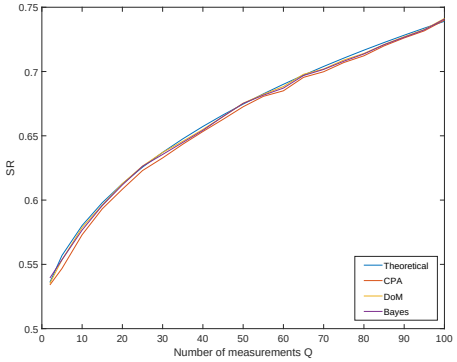

Fig. 3. SR^1 under candidate pair $(212, 30)$ and different Q.

Both Figures 2 and 3 clearly illustrate that the observation holds steadily regardless of SNR and Q. The small interval between the empirical and estimated success rate suggests that Equation 36 is convincing and agrees with the experimental results.

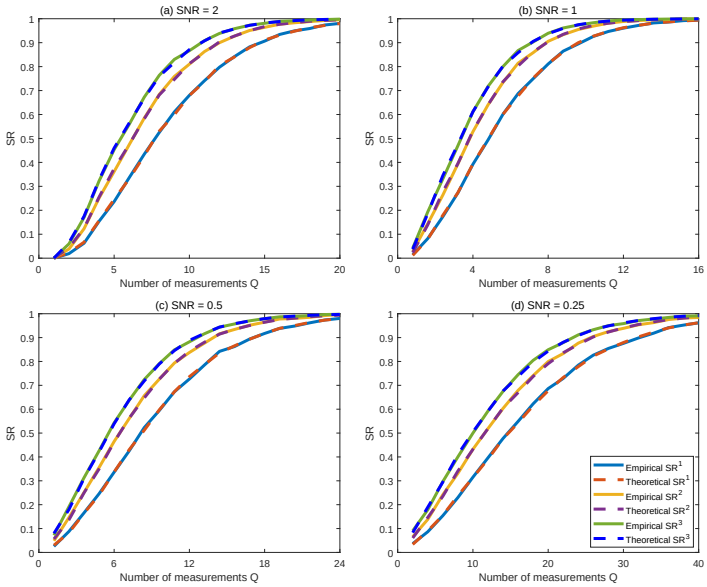

Fig. 4. Theoretical and experimental success rate of Bayes attack - simulated attacks.

5.2 Validation of the First-Order Boundary

Our proposed evaluation scheme revolve around the concept of first-order boundary that divides the leakage feature space $\mathcal{V}$ into a success space and a failure space. Algorithm 1 estimates success rate of an arbitrary order totally relying on the first-order boundary and its effectiveness needs to be tested as well. Thus, validating correctness of the first-order boundary is of great importance.

We assume the same Hamming weight leakage function and AES-128 S-box as the ones exploited in Section 5.1. There are three parameters to concern in this experiment, i.e., the number of measurements Q, the Signal-to-Noise Ratio SNR, and o the order of success rate. Therefore, for every distinguisher we provide 9 results. To achieve a better validation and comparison, we set a high SNR and repeat our experiment 10,000 times in order to make the empirical o^{th}-order success rate as accurate as possible. The step length of Q is set to 2. For generality, we generate plaintext set randomly for each repeated experiment in order to make it close enough to reality. Empirical curves are plotted totally according to corresponding outputs of the distinguishers. Meanwhile, we

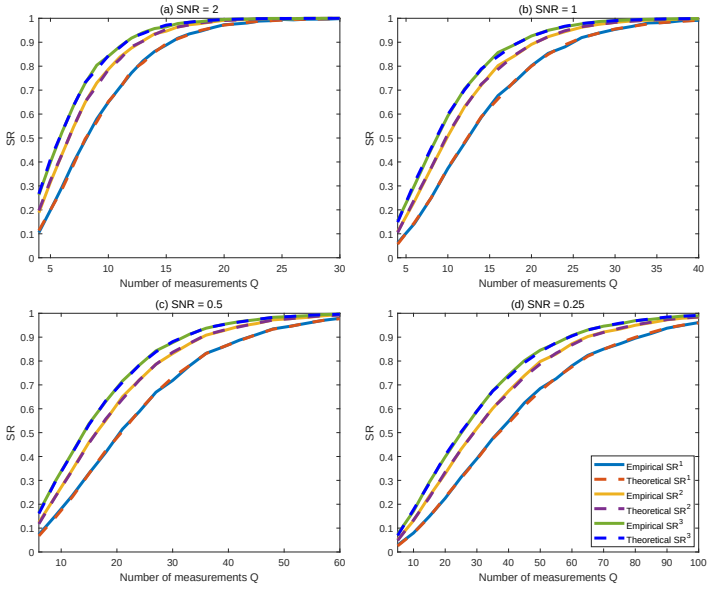

Fig. 5. Theoretical and experimental success rate of CPA - simulated attacks.

use Algorithm 1 to acquire the corresponding SR^o in theory. Theorical curves are plotted by averaging over computed SR^o-s (i.e. ouputs of Algorithm 1) after all repeated experiments. The hardly existing intervals in each of Figures 4, 5, 6 clearly illustrate the superiority of our proposed first-order boundary that is serves as an ideal tool for evaluation of arbitrary order success rate. Additionally, curves of different distinguishers presented in Figures 4, 5, 6 show very similar tendency, thereby agree with Equation (24) and conclusions made in [20]. Namely, different univariate DPA attacks share the same expectation of success rate and the differences observed are caused by statistical artifacts.

The gap observed between different orders of success rates is relatively narrow in low noise scenario ($SNR = 2$), since the correct candidate k^* will always be placed in the first position in the score vector. As a result, we can infer that there are few differences between higher-order and first-order success rate in this case. Interestingly, increased noise first widens the gap then narrows it by sinking the average position of k^* in the score vector. To be specific, $SNR = 1$ appears to be a medium level in our experiment that happens to sink the average position of k^* from the first place to about 2 or 3, making SR^2 and SR^3 much more higher than SR^1. Finally, as the noise approaches a higher level ($SNR = 0.5$ and $SNR = 0.25$), the average position of k^* falls out of the first three positions, resulting in the gap turning to narrow again.

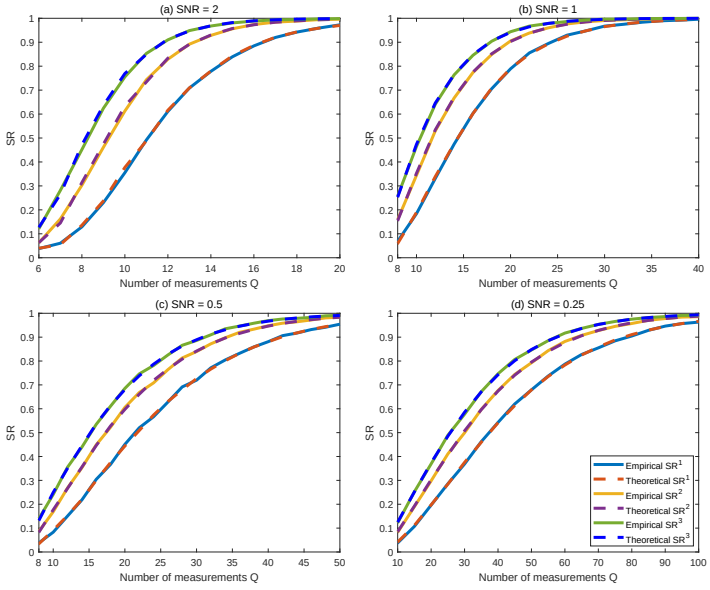

Fig. 6. Theoretical and experimental success rate of DoM - simulated attacks.

6 Experiments on an ATMega328p Micro-controller

6.1 Experimental Setups

To further validate *Bond*[1], this section shows that our results also hold in practice. For this purpose, we perform our experiments on an unprotected AES-128 algorithm [1] implemented on an ATMega328p micro-controller with a clock operating frequency of 16 MHz. By randomly encrypting 100,000 plaintexts and applying a WaveRunner 8104 oscilloscope, we acquire 100,000 power traces as our data set which are enough for an estimation of α and σ in Equation (1). The sampling rate is set to 1 GS/s. For better and more quick validation, we perform CPA to select the sample named Point-Of-Interest (POI) [8] with the highest Pearson correlation coefficient for the first S-box in the first round to perform the subsequent experiments.

6.2 Validation of the First-Order Boundary

To highlight the effectiveness of our proposed theory and find out whether and to what extent our results still make sense for empirical SR under limited measurements (which can not be told in simulated experiment), we repeat our real experiment 10000 times. Compared to simulated one, gaps more or less observed in Figures 7, 8, 9 are mainly due to statistical biases introduced by estimation of system parameters (i.e., α and σ in Equation (1)) and the fact that practical leakages may be complex and do not strictly follow our assumed leakage

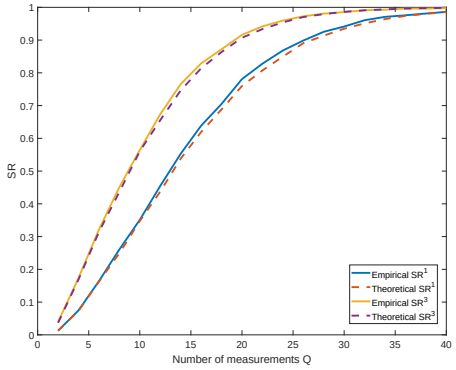

Fig. 7. Theoretical and experimental success rate of Bayes distinguishers - real measurements.

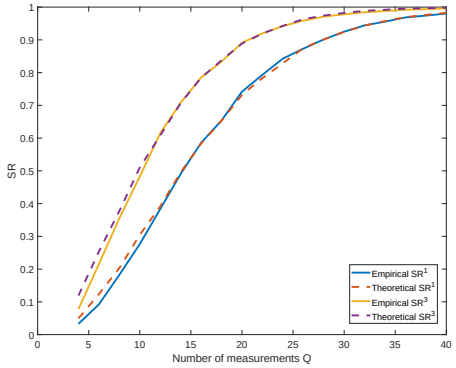

Fig. 8. Theoretical and experimental success rate of CPA distinguishers - real measurements.

model in Equation (1). Although fewer repetitions make the empirical SR thrash more violently, the corresponding theoretical SR still provide sound and effective prediction of it.

7 Conclusions

To facilitate better and intuitive understanding of different univariate DPA attacks, this paper built a unified evaluation framework from the leakage feature space $\mathcal{V}$. The framework was centered around a Euclidean space where leakage measurement X and the process of guessing subkey k^* were abstracted and mapped to visualized vectors (points). Different univariate DPA attacks were unified as comparing and analyzing vectors but applying different similarity measure metrics. It allowed discussing the underlying relationship between them in a straightforward manner. Further, we proposed a unified evaluation framework

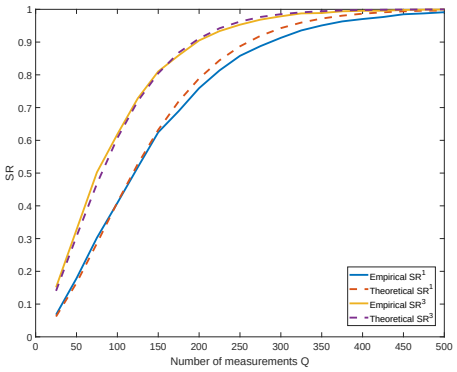

Fig. 9. Theoretical and experimental success rate of DoM - real measurements.

for success rate based on the leakage feature space $\mathcal{V}$ we provided. By building equations according to boundary conditions, we obtained the expression of success spaces in leakage feature space $\mathcal{V}$, making the derivation of success rate intuitive and easy to understand as well. We concluded that the success rate can be estimated by doing a density integral in Euclidean space $\mathcal{V}$. Eventually, we proposed an algorithm for efficient calculation of the integral.

Our evaluation framework on univariate DPA attacks is very intuitive with strict theoretical proof, and we believe it brings us a new road for evaluation of full-key recovery and other side-channel distinguishers, i.e., collision attack [5, 13, 21]. Secondly, we have not simplified Equation (38) to a closed-from expression due to complexity of the integral. This facilitates our attempt to further investigate other properties, if exists, of the first-order boundary and combined with Equations (25) and (35) to derive the closed-form expression of arbitrary order success rate. Finally, we will also carry out corresponding research on other security metrics, such as guessing entropy, and look forward to the "*surprises*" brought by our evaluation framework.

References

1. AVR-Crypto-Lib. https://github.com/DavyLandman/AESLib.
2. 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.
3. S. Arimoto. On the Converse to the Coding Theorem for Discrete Memoryless Channels. *IEEE Trans. Inf. Theory*, 19(3):357–359, 1973.
4. C. F. Bond, K. Richardson, et al. Seeing the Fisher Z-transformation. *psychometrika*, 69(2):291–303, 2004.
5. 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.

6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. A. Ito, R. Ueno, and N. Homma. Perceived Information Revisited New Metrics to Evaluate Success Rate of Side-Channel Attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2022(4):228–254, 2022.
16. 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.
17. V. Lomné, E. Prouff, M. Rivain, T. Roche, and A. Thillard. How to Estimate the Success Rate of Higher-Order Side-Channel Attacks. In *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, volume 8731 of *Lecture Notes in Computer Science*, pages 35–54. Springer, 2014.

18. 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.
19. S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks - Revealing the Secrets of Smart Cards*. Springer, 2007.
20. 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.
21. 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.
22. A. Moradi, N. Mousavi, C. Paar, and M. Salmasizadeh. A Comparative Study of Mutual Information Analysis under a Gaussian Assumption. In *Information Security Applications, 10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers*, volume 5932 of *Lecture Notes in Computer Science*, pages 193–205. Springer, 2009.
23. C. R. Rao. *Linear Statistical Inference and its Applications, Second Editon*. Wiley Series in Probability and Statistics. Wiley, 1973.
24. 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 *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.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.

30. C. Whitnall and E. Oswald. A Fair Evaluation Framework for Comparing Side-Channel Distinguishers. *J. Cryptogr. Eng.*, 1(2):145–160, 2011.
31. A. Wiemers. A Remark on a Success Rate Model for Side-Channel Attack Analysis. *J. Cryptogr. Eng.*, 10(3):269–274, 2020.