Systematic Construction and Comprehensive Evaluation of the Kolmogorov-Smirnov Test based Side-Channel Distinguishers[†]

Hui Zhao[1], Yongbin Zhou[1,*], François-Xavier Standaert[2], and Hailong Zhang[1]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences,
89A, Mingzhuang Rd, Beijing 100195, P.R. China
{zhaohui,zhouyongbin,zhanghailong}@iie.ac.cn
[2] UCL Crypto Group, Université catholique de Louvain
{fstandae@uclouvain.be}

Abstract. Generic side-channel distinguishers aim at revealing the correct key embedded in cryptographic modules even when few assumptions can be made about their physical leakages. In this context, Kolmogorov-Smirnov Analysis (KSA) and Partial Kolmogorov-Smirnov analysis (PKS) were proposed respectively. Although both KSA and PKS are based on the Kolmogorov-Smirnov (KS) test, they really differ a lot from each other in terms of construction strategies. Inspired by this, we construct nine new variants by combining their strategies in a systematic way. Furthermore, we explore the effectiveness and efficiency of all these twelve KS test based distinguishers under various simulated scenarios in a univariate setting within a unified comparison framework, and also investigate how these distinguishers behave in practical scenarios. For these purposes, we perform a series of attacks against both simulated traces and real traces. Evaluation metrics such as Success Rate (SR) and Guessing Entropy (GE) are used to measure the efficiency of key recovery attacks in our evaluation. Our experimental results not only show how to choose the most suitable KS test based distinguisher in a particular scenario, but also clarify the practical meaning of all these KS test based distinguishers in practice.

Keywords: Side-Channel Analysis, Distinguisher, Kolmogorov-Smirnov Test, Construction, Evaluation

1 Introduction

Side-channel attack aims at identifying the secret information embedded in a cryptographic device from its physical leakages. One of the most famous side-channel attacks is Differential Power Analysis (DPA), which was proposed by

[†] An abridged version of this paper will appear at ISPEC 2013.

[*] Corresponding Author

Kocher in his seminal work [1]. Generally, DPA employs some type of statistics (also referred to as *distinguisher* in side-channel cryptanalysis) to reveal the correct key hypothesis about the secret key or part of it within a set of candidates. In side-channel attacks, the most famous two distinguishers known are distance-of-means introduced by Kocher in [1], Pearson correlation coefficient in Correlation Power Analysis (CPA) proposed by Brier in [3]. Meanwhile, other variants of these two distinguishers, such as Multi-bit DPA [2] and Proposition Power Analysis (PPA) [4], are also proposed to enhance the performance of DPA and CPA respectively. Concerning these distinguishers, a recent work by Mangard et al. [5] has shown that DPA, CPA and even Gaussian templates [22] are in fact asymptotically equivalent to each other, given that they are provided with the same a priori information about the leakages. The results of [5] are further complimented by [6] where Doget et al. stduy if the statement in [5] also hold in non-asymptotic contexts (when the number of measurements is reasonably small). Therefore, these distinguishers are collectively called CPA-like distinguishers throughout this paper. Essentially, all these CPA-like distinguishers exploit linear dependency between key-dependent hypothetical power consumptions and physical leakages.

Even though CPA-like distinguishers are well capable of measuring linear dependency between hypothetical power consumptions and physical leakages, they become less efficient when the dependency is not strictly linear [11]. In light of this, Mutual Information Analysis (MIA) was proposed by Gierlichs in [7] to measure total dependency (both linear and nonlinear) between the hypothetical power consumptions and the physical leakages. Consequently, MIA is considered to be generic because it is capable of dealing with the total dependency. Although MIA is generic, it also bears some technical challenges. For example, the probability density function estimation (PDF) in MIA is widely accepted to be a difficult problem [8–10]. Experiments in [11–13] confirmed that the PDF estimation methods have a decisive impact on the performance of MIA. Among those different methods, the histogram estimation method was adopted in [7]. The performance of histogram based MIA can also be greatly affected by the power model and noise. In [11], Charvillon and Standaert showed that kernel estimation methods can improve the performance of MIA. However, kernel estimation methods based MIA requires a considerable number of traces to attain a good performance in key recovery attacks. Therefore, the performance of MIA depends on the accuracy of the estimation methods. Considering the probability density function of MIA is hard to estimate accurately, Kolmogorov-Smirnov Analysis (KSA) [11] and Partial Kolmogorov-Smirnov analysis (PKS) [15] were independently proposed. KSA and PKS use cumulative density function estimation, instead of probability density function estimation, to avoid explicit probability density function estimation. Both KSA and PKS sound like promising alternatives for MIA, but which one is a better alternative for MIA in key recovery attacks?

On the one hand, although both KSA and PKS are based on the Kolmogorov-Smirnov (KS) test, they differ a lot from each other in terms of construction strategies, such as partition method, similarity measure used by KS test, assumption about leakages and normalization. One natural yet important question is that whether we can construct more efficient distinguishers via combining different construction strategies by both KSA and PKS. For all these KS test based distinguishers, how can we choose the most suitable KS test based distinguisher in a certain scenario? For all these KS test based distinguishers, to what extent do they pose severe threats on the implementations of cryptographic modules in practice? In order to answer these relevant questions above, we will investigate the efficiency of all these KS test based distinguishers in a comprehensive comparison framework. Since it seems difficult to study the relationship of all KS test based distinguishers theoretically, we will explore the advantages and limitations of the KS test based distinguishers experimentally.

Note that we only compare the KS test based distinguishers in a univariate setting, due to the fact that PKS does not have multivariate extensions.

1.1 Our contributions

The contributions of this paper are threefold. First, we show how to systematically construct the KS test based distinguishers via combining different construction strategies by both KSA and PKS. Specifically, nine new variants of the KS test based distinguishers are constructed.

Second, we investigate the effectiveness and efficiency of all twelve KS test based distinguishers in a comprehensive comparison framework. In the framework, we consider the impacts of leakage function, noise level and power model to these KS test based distinguishers in simulated experiments. Evaluation metrics such as Success Rate (SR) and Guessing Entropy (GE) are used to evaluate the efficiency of these KS test based distinguishers. We believe that each of these KS test based distinguishers has both pros and cons, and will give a balanced view of all these KS test based distinguishers in simulated experiments. Experimental results show that how to choose the most suitable distinguisher in a certain scenario. For example, three out of these nine distinguishers, which are MP-KSA, C-KSA and MPC-KSA, outperform both KSA and PKS in terms of success rate for a given number of traces in a certain scenario, respectively.

Third, we also demonstrate the practical meaning of all these KS test based distinguishers in practice. For example, MPC-KSA is better than CPA when they are against the unprotected hardware AES implementation on Xilinx Virtex-5 FPGA provided by DPA Contest v2. Specifically, the number of traces required for MPC-KSA to achieve a partial success rate of 80% is 6,000, while that of CPA is 15,000, and the number of traces required for MPC-KSA to achieve the global success rate of 80% is 14,500, while that of CPA is 16,900.

The rest of this paper is organized as follows. Section 2 introduces KS test, and then briefly recalls both KSA distinguisher and PKS distinguisher. Section 3 analyzes the construction strategies by both KSA and PKS, and then nine new variants of KS test based distinguishers are proposed. Section 4 presents the comparison framework, and then shows our findings in different leakage scenarios. Conclusions are given in Section 5.

2 Preliminaries

In this section, we will first introduce the KS test, and then briefly recall KSA distinguisher and PKS distinguisher.

2.1 Kolmogorov-Smirnov Test

In statistics, the Kolmogorov-Smirnov (KS) test is a nonparametric test whose main target is to determine if two distributions differ significantly. Therefore, one can use the Kolmogorov-Smirnov test to measure the similarity of two distributions in terms of their distance. Assume that the random variable X has n samples. Its empirical cumulative distribution function is $F_n(x) = \frac{1}{n}\sum_{i=1}^{n} I_{A_i \leqslant x}$. $I_{A_i \leqslant x}$ is the indicator function, where its value is 1 when $A_i \leqslant x$, otherwise 0. For a given cumulative distribution function $F(x)$, formula (1) is used to test their similarity.

$$D_n = sup_x |F_n(x) - F(x)| \tag{1}$$

where sup_x is the supremum of the set of distances. Specifically, the largest distance between two distributions represents the similarity between two distributions. On the other hand, p-value can also be used to measure the similarity of two distributions. The smaller of the p-value, the less similar between the two distributions.

2.2 KSA Distinguisher

KSA distinguisher is based on two-sample KS test. Its central idea is to measure the maximum distance between the global trace distribution L and the conditional trace distribution $L|M$, and then average the distances over the prediction space, where M denotes hypothetical power consumption model. Denote l the leakages, and m the hypothetical power consumption values. Denote Pr the probability. KSA is shown in the formula (2).

$$E_{m\epsilon M}(D_{KS}(Pr[L = l|M = m]||Pr[L = l])) \tag{2}$$

KSA can be extended to a normalized version (norm-KSA) that is shown in the formula (3). The starting point of norm-KSA is the distance of each partition plays an equal role in deciding which key hypothesis is the correct one.

$$E_{m\epsilon M}(\frac{1}{|L|M = m|} D_{KS}(Pr[L = l|M = m]||Pr[L = l]))) \tag{3}$$

Example 2.1: We illustrate the working principle of KSA via a very simple example consisting of an AES implementation leaking the Hamming Weight (HW) of the first S-box with a signal-to-noise ratio (SNR, defined as $\frac{Var(Signal)}{Var(Noise)}$) of 64. Figure 1(a) shows partitions of leakages (in blue) under the correct key hypothesis, where the red line represents the global CDF of leakages and the blue lines stand for partitions of leakages under the correct key hypothesis. Figure 1(b) shows partitions of leakages (in blue) under the wrong key hypothesis, where the red line represents the global CDF of leakages and the blue lines stand for partitions of leakages which correlated with the wrong key hypothesis. It is expected that only the correct key hypothesis produces a large average difference.

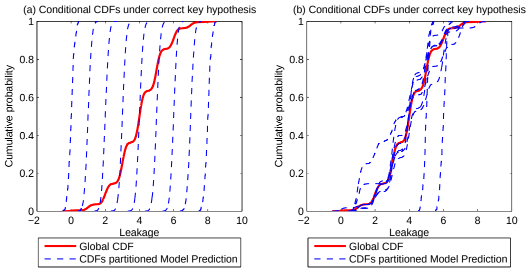

Fig. 1. KSA is based on the largest distance between the CDFs of two leakages.

2.3 PKS Distinguisher

In power analysis attacks, for each single point of a power trace, the power consumption of one cryptanalysis device can be modeled as the sum of an operation-dependent component P_{op}, a data-dependent component P_{data}, electronic noise component $P_{el-noise}$, and a constant component P_{const} [17]. For most cryptographic devices, it is valid to approximate the distribution of the data-dependent component P_{data} of the power consumption by a normal distribution if the processed data is uniformly distributed [17]. In light of this, [15] proposed a generic distinguisher, namely PKS, based on single-sample KS test. Leakages L and the hypothetical power consumptions M should be processed by Z-score transformation in PKS. p is an empirical parameter in PKS from zero to one. N(0,1) represents the standard normal distribution. PKS is shown in the formula (4).

$$P_{value}(D_{KS}(Pr[L = l|M \leq p]||N(0,1))) \tag{4}$$

PKS will return the smallest p-value when the key hypothesis is correct. PKS with a single test in the formula (4) only tests partial leakages, so PKS will lose some important information of the other leakages. To overcome this problem, [15] introduced another PKS enhancement: two-partial KS test, as is shown in the formula (7).

$$D_{KS_l} = P_{value}(D_{KS}(Pr[L = l|M \leq p]||N(0,1))) \tag{5}$$

$$D_{KS_r} = P_{value}(D_{KS}(Pr[L = l|M > p]||N(0,1))) \tag{6}$$

$$D_{PKS} = D_{KS_l} \times D_{KS_r} \tag{7}$$

Example 2.2: We describe the working principle of PKS using the same setting as that in *Example 2.1*. In Figure 2(a), the red line represents the global CDF of standard normal distribution and the blue lines stand for partial samples which correlated with the key hypothesis. In Figure 2(b), the red line represents the global CDF of standard normal distribution and the blue lines stand for the partial samples which correlated with the incorrect key hypothesis. PKS will return the smallest p-value when the key hypothesis is correct.

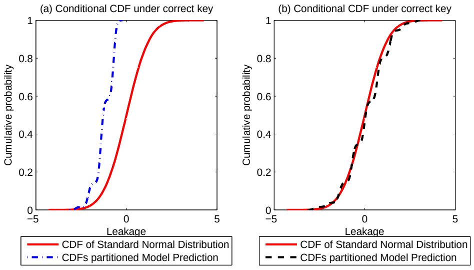

Fig. 2. PKS is based on the smallest p-value between the CDFs of standard normal distribution and paritial leakages

3 Systematic Construction of the KS Test based Side-Channel Distinguishers

From section 2, we learn that both KSA and PKS are based on the KS test, and they are able to recover the correct key by partitioning the leakages correctly. However, KSA and PKS are really different from each other in terms of their construction strategies. Therefore, we will show how to construct other new variants of the KS test based distinguishers by combining their different construction strategies in a systematic way. For this purpose, we will analyze the construction strategies using by KSA and PKS, and then we will present nine new variants of the KS test based distinguishers.

3.1 Construction strategies of KSA and PKS

In this subsection, we will compare the construction differences between KSA and PKS in four aspects: partition method, similarity measure used by the KS test, assumption about leakages, and normalization.

Partition method. In a partition attack [20], leakages are divided into several sets $p_k^1, p_k^2, ..., p_k^n$ according to each key hypothesis k. These sets are built according to a power model H. It directly yields a hypothetical power consumption m_k^q, where q is the plaintext or ciphertext. In this paper, partition method is classified as non-cumulative partition method and cumulative partition method. Examples of hypothetical leakages that can be used to partition 16-element leakages will be shown in Table 1. Specifically, the non-cumulative partition method used by KSA is shown in the left part of Table 1, while the cumulative partition method used by PKS is shown in the right part of Table 1.

Table 1. Examples of the non-cumulative partition method (left) and the cumulative partition method (right)

p_k^1	p_k^2	p_k^3	p_k^4	p_k^5
l_5	l_2	l_1	l_3	l_{14}
	l_7	l_4	l_6	
	l_9	l_8	l_{12}	
	l_{16}	l_{10}	l_{13}	
		l_{11}		

p_k^1	p_k^2	p_k^3	p_k^4	p_k^5
l_5	l_5	l_5	l_5	l_5
	l_2	l_2	l_2	l_2
	l_7	l_7	l_7	l_7
	l_9	l_9	l_9	l_9
	l_{16}	l_{16}	l_{16}	l_{16}
		l_1	l_1	l_1
		l_4	l_4	l_4
		l_8	l_8	l_8
		l_{10}	l_{10}	l_{10}
		l_{11}	l_{11}	l_{11}
		l_{15}	l_{15}	l_{15}
			l_3	l_3
			l_6	l_6
			l_{12}	l_{12}
			l_{13}	l_{13}
				l_{14}

Similarity measure used by KS test. Distance is used by KSA to measure the similarity of two distributions. In contrast, p-value is adopted in PKS to indicate whether or not partial leakages follow a normal distribution.

Assumption about leakages. PKS distinguisher considers that leakages follow a normal distribution, while KSA makes no assumption about leakages.

Normalization. [11] suggested that normalization could improve the performance of KSA. The performance of normal-KSA is also verified with attacks against the power traces provided by DPA Contest v1. However, our question is whether or not the normalization is always effective in some typical scenarios for KSA. We will also try to answer this question in this work.

3.2 Nine New Variants of the KS Test based Distinguishers

In subsection 3.1, we analyzed the construction strategies of both KSA and PKS. We find that KSA and PKS have different choices for a specific construction strategy. One natural yet pertinent question is that is it possible to construct other (more efficient) KS test based distinguisher by combining the construction methods of both KSA and PKS ? To answer this question, we combine the construction strategies using by both KSA and PKS to construct nine new variants of the KS test based distinguishers, in a systematic way.

For convenience, we will label each strategy that was used by KSA and PKS. Denote A0 the non-cumulative partition method, and A1 the cumulative partition method. Denote B0 the expectation of distance as the similarity measure of the KS test, and B1 the product of p-value as the similarity measure of the KS test. Denote C0 the distinguisher that makes no assumption about leakage distribution, and C1 the distinguisher that assumes the leakage follows a normal distribution. Denote D0 that we perform normalization on a distinguisher, and D1 that we do not.

By combining these strategies systematically, one can, in total, construct 2^4 KS test based distinguishers. Among these 16 distinguishers, three are existing and they are KSA (A0,B0,C0,D1), PKS (A1,B1,C1,D1) and norm-KSA (A0,B0,C0,D0).On the other hand, note that B1 and D0 conflict with each other, therefore four combinations (A1,C1,B1,D0; A1,C0,B1,D0; A0,C1,B1,D0; A0,C0,B1,D0) do not make any sense. Additionally, three combinations , which are (A0, B0, C1, D1), (A0, B0, C0 and D0) and (A0,B1,C1,D1), fail to work in the key recovery attacks. We free the limitation of Z-score on hypothetical power consumptions of D-PKS (A1, B0, C1, D1), norm-D-PKS (A1, B0, C1, D0) and PKS (A1,B1,C1,D1) to form C-PKS (A1, B0, C1, D1), norm-C-PKS (A1, B0, C1, D0) and MPC-PKS (A1, B1, C1, D1). Therefore, we only construct $9(= 2^4 - 4 - 3 - 3 + 3)$ new variants of the KS test based distinguishers. These nine new distinguishers are as follows.

MP-KSA distinguisher. A0, B1, C0 and D1 are selected to construct the product of Multiple P-values based KSA (MP-KSA) distinguisher. In order to avoid arithmetic underflow, one typically applies the logarithm to the MP-KSA distinguisher. MP-KSA is shown in the formula (8).

$$log_2(\prod_{m \epsilon M} P_{value}(D_{KS}(Pr[L=l|M=m]||Pr[L=l]))) \tag{8}$$

MP-KSA will return the smallest product of p-values under the correct key hypothesis.

C-KSA distinguisher. A1, B0, C0 and D1 are selected to construct Cumulative partition method based KSA (C-KSA) distinguisher. C-KSA is shown in the formula (9).

$$E_{m \epsilon M}(D_{KS}(Pr[L=l|M \leqslant m]||Pr[L=l])) \tag{9}$$

C-KSA will return the largest expected distance under the correct key hypothesis.

norm-C-KSA distinguisher. A1, B0, C0 and D0 are selected to construct normalized C-KSA (norm-C-KSA) distinguisher. norm-C-KSA is shown in the formula (10).

$$E_{m\epsilon M}(\frac{1}{|L|M=m|}D_{KS}(Pr[L=l|M\leqslant m]||Pr[L=l])) \tag{10}$$

norm-C-KSA will return the largest expected normalized distance under the correct key hypothesis.

MPC-KSA distinguisher. A1, B1, C0 and D1 are selected to construct the product of Multiple P-values and Cumulative partition method based KSA (MPC-KSA) distinguisher. In order to avoid arithmetic underflow, one typically applies the logarithm to the MPC-KSA distinguisher. MPC-KSA is shown in the formula (11).

$$log_2(\prod_{m\epsilon M}P_{value}(D_{KS}(Pr[L=l|M\leqslant m]||Pr[L=l]))) \tag{11}$$

MPC-KSA will return the smallest the product of p-values under the correct key hypothesis.

D-PKS distinguisher. A1, B0, C1 and D1 are selected to construct Distance based PKS (D-PKS) distinguisher. It is assumed that the distribution of the leakages follows normal distribution. L and M should be processed by Z-score transformation before processing by D-PKS. p is an empirical parameter for D-PKS. D-PKS is shown in the formula (12).

$$E(D_{KS}(Pr[L=l|M\leqslant p]||N(0,1))) \tag{12}$$

D-PKS will return the largest expected distance under the correct key hypothesis.

norm-D-PKS distinguisher. A1, B0, C1 and D0 are selected to construct normalized D-PKS (norm-D-PKS) distinguisher. It is assumed that the distribution of the leakages follows normal distribution. L and M should be processed by Z-score transformation before processing by norm-D-PKS. p is an empirical parameter for norm-D-PKS. norm-D-PKS is shown in the formula (13).

$$E(\frac{1}{|L|M\leqslant p|}D_{KS}(Pr[L=l|M\leqslant p]||N(0,1))) \tag{13}$$

norm-D-PKS will return the largest expected normalized distance under the correct key hypothesis.

C-PKS distinguisher. A1, B0, C1 and D1 are selected to construct Cumulative partition method based PKS (C-PKS) distinguisher. It is assumed that the distribution of the leakages follows normal distribution. L should be processed by Z-score transformation before processing by C-PKS. C-PKS is shown in the formula (14).

$$E_{m\epsilon M}(D_{KS}(Pr[L=l|M\leqslant m]||N(0,1))) \tag{14}$$

C-PKS will return the largest expected distance under the correct key hypothesis.

norm-C-PKS distinguisher. A1, B0, C1 and D0 are selected to construct normalized C-PKS (norm-C-PKS) distinguisher. It is assumed that the distribution of the leakages follows normal distribution. L should be processed by Z-score transformation before processing by norm-C-PKS. norm-C-PKS is shown in the formula (15).

$$E_{m\epsilon M}(\frac{1}{|L|M\leqslant m|}D_{KS}(Pr[L=l|M\leqslant m]||N(0,1))) \tag{15}$$

norm-C-PKS will return the largest expected normalized distance under the correct key hypothesis.

MPC-PKS distinguisher. A1, B1, C1 and D1 are selected to construct the product of Multiple P-values and Cumulative partition method based PKS (MPC-PKS) distinguisher. It is assumed that the distribution of the leakages follows normal distribution. L should be processed by Z-score transformation before processing by MPC-PKS. In order to avoid arithmetic underflow, one typically applies the logarithm to the MPC-PKS distinguisher. MPC-PKS is shown in the formula (16).

$$log_2(\prod_{m\epsilon M}P_{value}(\frac{1}{|L|M\leqslant m|}D_{KS}(Pr[L=l|M\leqslant m]||N(0,1)))) \tag{16}$$

MPC-PKS will return the smallest the product of p-values under the correct key hypothesis.

4 A Comprehensive Evaluation of All Twelve KS Test based Side-Channel Distinguishers

So far, we have constructed nine new variants of the KS test based distinguishers. The performance of these KS test based distinguishers in a univariate setting has a huge impact on how to choose the most suitable KS test based distinguisher in a certain scenario. Consequently, we will evaluate the performance of all these KS test based distinguishers by amounting key recovery attacks, and analyze their effectiveness and efficiency by using the evaluation metrics such as Success Rate (SR) and Guessing Entropy (GE) in typical scenarios. On the one hand, we will evaluate the performance of these KS test based distinguishers in in a unified comparison framework inspired by [14]. In this framework, we will evaluate the influence of different factors, such as leakage function, noise level and power model, on the performance of each KS test based distinguisher. We will compare the attacking efficiency of these distinguishers in terms of SR, and we also provide the results in terms of GE in Appendix A. On the other hand, we will perform a series of attacks against the real traces from both OpenSCA and DPA Contest v2, respectively. With these practical attacks, we will demonstrate the practical meaning of all these KS test based distinguishers. Note that we do not compare the running cost for different distinguishers.

4.1 A Comprehensive Comparison Framework

According to previous studies, target function [16], leakage function [14], power model, noise level and evaluation metrics are very important factors in the evaluation of different distinguishers. Therefore, the performance of each distinguisher should be evaluated in different scenarios taking all these factors into consideration [14]. We will describe these factors in the following.

Target Function. Different target functions may lead to different evaluation results. In this paper, we will select the output of commonly-used S-box of the first AES round as our target function.

Leakage Function. Leakage function is used to test the adaptability of the KS test based distinguishers. Therefore, in simulated experiments, we select three typical leakage scenarios, and they are Hamming weight (HW) leakage function, an Unevenly Weighted Sum of the Bits (UWSB) leakage function, and highly nonlinear leakage function. In practical experiments, however, the leakage functions are unknown.

Power Model. The characterization abilities, namely power model, of an adversary pose a great impact on the performance of a distinguisher. So we consider the adversary who has two kinds of characterization abilities. The first one is that the adversary is able to fully characterize the leakage. The second one is that adversary only can partially characterize the leakage. In detail, HW model in the HW leakage scenario represents the fact that the adversary can accurately characterize the leakage; while HW model and Identity (ID) model in the other scenarios stand for the fact that the adversary is unable to fully characterize the leakages.

The Influence of Noise. Normally, noises have negative effects on the performance of side-channel distinguishers exploiting the noisy leakages. In this paper, we consider the influence of noise level on the performance of the KS test based distinguishers, and assume that noise follows a normal distribution. Specifically, we consider the performance of KS test based distinguishers under seven Signal-to-noise ratios, which are 0.125, 1, 8, 16, 32, 64 and positive infinity.

Evaluation Metric. Evaluation Metric is of importance to the fair comparison of the KS test based distinguishers. In this paper, Success Rate (SR) and Guessing Entropy (GE) [19] are used to evaluate the efficiency of the KS test based distinguishers.

4.2 Simulated Experiments

In simulated scenarios, we use the output of the first S-box of the first round AES operation as the target intermediate value, and the chosen target intermediate values will be mapped to pure leakages by three typical leakage functions, i.e. HW leakage function, UWSB leakage function and highly nonlinear leakage function. Finally, we take the sum of the pure leakages and some independent Gaussian noise to be simulated leakages. Noise level in simulated leakages is measured by SNR. We particularly employ seven SNRs, i.e. 0.125, 1, 8, 16, 32, 64 and positive infinity, to test the influence of Gaussian noise level on KS test based distinguishers.

In each scenario, we perform key recovery attacks using all twelve KS test based distinguishers [1] and MIA [2] as well. For each one of these fourteen kinds of attacks, we repeat it 300 times by choosing different plaintexts, in order to evaluate its average performance.

Our experiments are also carefully organized in order to make them understood more easily. Specifically, we divide the results of all these thirteen distinguishers into three groups, and denote these groups by A, B and C respectively. Group A consists of four existing distinguishers and they are PKS, KSA, norm-KSA and MIA. For each scenario, we select the most efficient one from Group A, and the selected one is set to be a benchmark for this scenario. Next, the other new nine KS test based distinguishers are classified into two groups, according to their relative efficiency over the selected benchmark. Namely, for each scenario, those distinguishers that are more efficient than the benchmark are set into Group B, while the others that are less efficient than the benchmark are put into Group C.

Hamming Weight Leakage

In these scenarios, we assume that the leakage of a cryptographic device consists of HW of target intermediate value and Gaussian noise. Under this reasonable assumption, we will investigate the performance of different distinguishers with two adversarial characterization abilities.

- An Adversary with a Perfect Power Model. Figure 3 shows the success rate of twelve KS test based distinguishers and MIA using a HW model against

[1] We use the enhancement of PKS, which is shown in the formula (7), as our PKS distinguisher in this context. PKS and its variants use different parameters in this context.

[2] Number of bins used in MIA are equal to the number of the power model image. I.e. MIA(HW,bins=9), MIA(ID,bins=256).

HW leakage of the first AES S-box. We divide all these distinguishers into three groups, and they are Group A, Group B and Group C. Group A only consists of four existing generic distinguishers and they are PKS(HW), KSA(HW), norm-KSA(HW) and MIA(HW), and the best of these four distinguishers will be selected as the benchmark accordingly. Group B and Group C contain nine new variants of KS test based distinguishers. Distinguishers in Group B are those more efficient than the benchmark, while distinguishers in Group C are those less efficient than the benchmark. For example, when the SNR is 0.125, the selected benchmark from Group A (see Figure 3(a)) is PKS (HW,p=0.618). In this case, Group B (see Figure 3(d)) consists of three distinguishers and they are C-KSA(HW), C-PKS(HW) and MPC-PKS(HW), while Group C (see Figure 3(g)) consists of six distinguishers and they are MP-KSA(HW), MPC-KSA(HW), norm-C-KSA(HW), D-PKS(HW), norm-D-PKS(HW) and norm-C-PKS(HW). In detail, Figure 3(a), 3(b), 3(c) and 3(ci) show the performance of existing KS test based distinguishers in Group A under four noise levels. Figure 3(d), 3(e), 3(f) and 3(fi) show the performance of KS test based distinguishers in Group B under four noise levels. Figure 3(g), 3(h), 3(i) and 3(ii) show the performance of KS test based distinguishers in Group C under four noise levels.

In Group A, KSA(HW) outperforms norm-KSA(HW) in terms of SR. As it is stated in [15], p using by PKS(HW) has a straightforwardly impact on the performance of PKS(HW). Figure 3(a) and 3(b) show that PKS(HW,p=0.618) is the best distinguisher when the SNRs are 0.125 and 1 respectively. Figure 3(c) and 3(ci) show that KSA(HW) is the most efficient distinguisher when the SNR is 8 and positive infinity. The best distinguisher in Group A will be selected as the benchmark to verify the effectiveness of the nine new variants of the KS test based distinguisher in Group B and Group C. When the SNR is 0.125, PKS(HW,p=0.618) in Figure 3(a) is used as the benchmark for Figure 3(d) and 3(g). Figure 3(d) shows that, C-KSA(HW), MPC-PKS(HW) and C-PKS(HW) are better than the benchmark, and C-KSA(HW) is the best distinguisher. Distinguishers in Figure 3(g) are less efficient than the benchmark, so we do not explain them in more details. When the SNR is 1, PKS(HW,p=0.618) in Figure 3(b) is also selected as the benchmark for Figure 3(e) and 3(h). Due to fact that Figure 3(e) and 3(h) can be analyzed in the similar way as that of Figure 3(d) and 3(g), we do not explain them in more details. When the SNR is 8, KSA(HW) is selected as the benchmark for Figure 3(f) and 3(i). Figure 3(f) shows that, MP-KSA(HW) and MPC-PKS(HW) exhibit consistently better than KSA(HW), and MP-KSA(HW) is the best distinguisher. Distinguishers in Figure 3(i) are less efficient than the benchmark, so we do not explain them in more details. When the SNR is positive infinity, KSA(HW) is also selected as the benchmark. In this case, Figure 3(fi) and 3(ii) can be analyzed in the similar way as that of Figure 3(f) and 3(i).

In summary, C-KSA(HW) is the best choice of all twelve KS test based distinguishers when the SNRs are 0.125 and 1 respectively, while MP-KSA(HW) is the best choice in all KS test based distinguishers when the SNR is 8 and positive infinity. Additionally, MPC-PKS(HW) is better than the benchmark when the SNRs are 0.125, 1 and 8 respectively.

- An Adversary with a Generic Power Model. Figure 4 shows the success rate of twelve KS test based distinguishers and MIA using an ID model against HW leakage of the first AES S-box. In this scenario, we organize the experimental results in the same way as those used in the ***An Adversary with a Perfect Power Model*** scenario.

In Group A, KSA(ID), norm-KSA(ID) and MIA(ID) all fail to reveal the correct key, while both PKS(ID,p=0.25) and PKS(ID,p=0.618) succeeds to do that. PKS(ID,p=0.618) is the most efficient distinguisher when the SNRs are 0.125, 1, 8, and positive infinity. The best distinguisher in Group A will be selected as the benchmark to verify the effectiveness of the nine new variants of the KS test based distinguisher in Group B and Group C. Therefore, PKS(ID,p=0.618) will be chosen as the benchmark when the SNRs are 0.125, 1, 8, and positive infinity. For example, PKS(ID,p=0.618) is chosen as the benchmark in Figure 4(d) and 4(g) when the SNR is 0.125. Figure 4(d) shows that C-KSA(ID), norm-C-KSA(ID), MPC-KSA(ID), C-PKS(ID), norm-C-PKS(ID) and MPC-PKS(ID) are more efficient than the benchmark, and they have the similar performance. Distinguishers in Figure 4(g) are less efficient than the benchmark, so we do not explain them in more details. When the SNRs are 1, 8, and positive infinity, they can be analyzed in the similar way as that of SNR of 0.125.

In a word, although C-KSA(ID), norm-C-KSA(ID), MPC-KSA(ID), C-PKS(ID), norm-C-PKS(ID) and MPC-PKS(ID) are more efficient than the benchmark and they have similar performance under four noise levels, C-KSA(ID), norm-C-KSA(ID) and MPC-KSA(ID) are slightly more efficient than C-PKS(ID), norm-C-PKS(ID) and MPC-PKS(ID).

An Unevenly Weighted Sum of the Bits Leakage Scenario.
In these scenarios, we consider the performance of different distinguishers in the case that the adversary does not have a precise power model. Motivated by [21], we focus the case that the device leaks an Unevenly Weighted Sum of the Bits (UWSB). In our experiments, we assume that the least significant bit dominates in the leakage function with a relative weight of 10 and other bits with a relative weight of 1. We will investigate the performance of twelve KS test based distinguishers and MIA with two adversarial characterization abilities.

- An Adversary with an Imprecise Power Model. Figure 5 shows the success rate of twelve KS test based distinguishers and MIA using a HW model against UWSB leakage of the first AES S-box. In this scenario, we organize the experimental results in the same way as those used in the ***An Adversary with a Perfect Power Model*** scenario.

In Group A, KSA(HW) outperforms norm-KSA(HW) in terms of SR. In this scenario, p using by PKS(HW) also has a straightforwardly impact on the performance of PKS(HW). For example, PKS(HW,p=0.618) is more efficient than PKS(HW,p=0.25). In detail, when the SNRs are 0.125 and 1, KSA(HW) and PKS(HW) are more efficient than MIA(HW), while PKS(HW,p=0.618) is

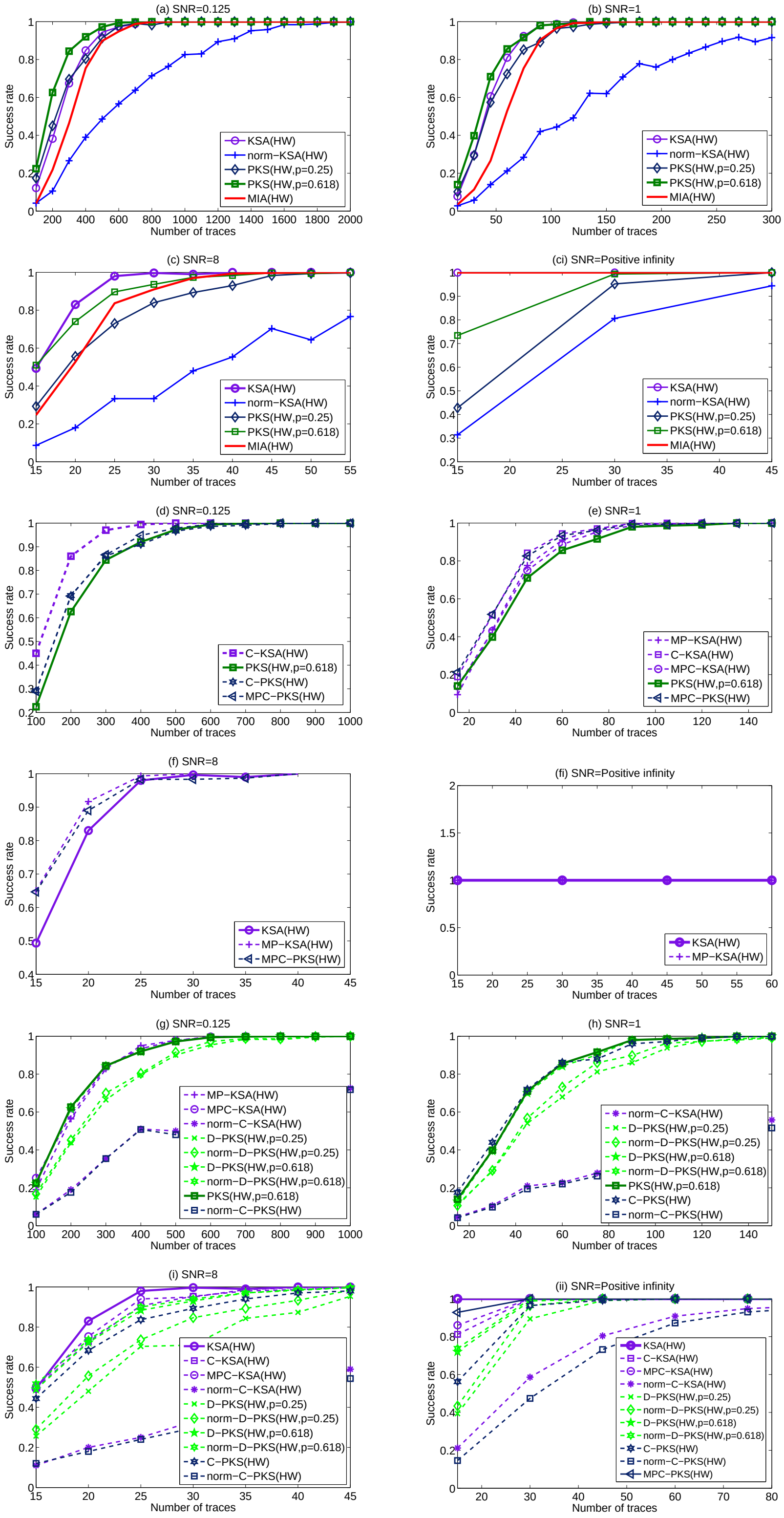

Fig. 3. Success rate of different distinguishers against the first AES S-box in Hamming Weight leakage

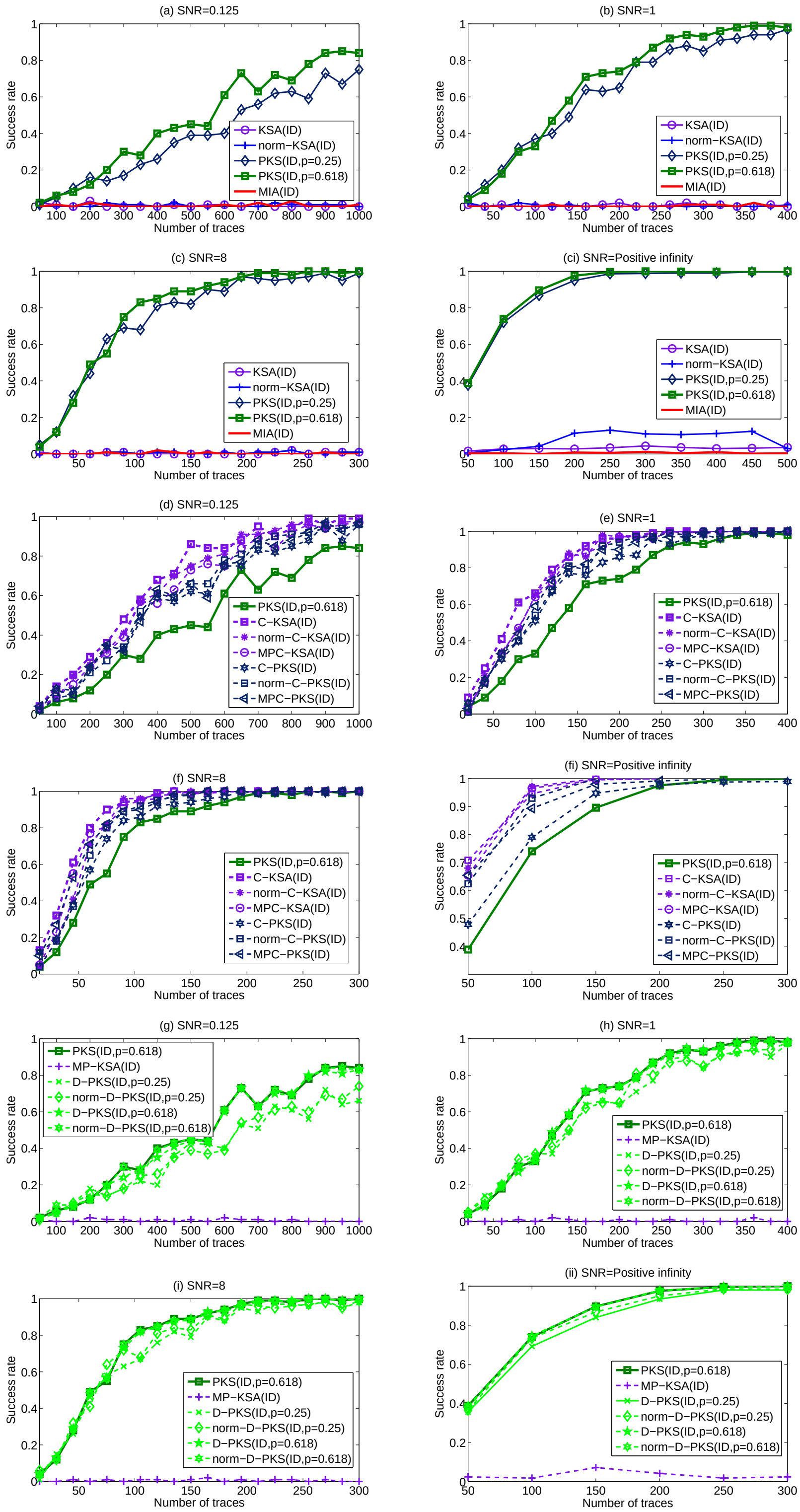

Fig. 4. Success rate of different distinguishers against the first AES S-box in Hamming Weight leakage

slightly more immune to noise compared with KSA(HW) (see Figure 5(a) and 5(b)). When the SNRs are 8 and positive infinity, neither of three existing distinguishers is better than MIA(HW) (see Figure 5(c) and 5(ci)). The best distinguisher in Group A will be selected as the benchmark to verify the effectiveness of the nine new variants of the KS test based distinguisher in Group B and Group C. For example, when the SNR is 0.125, PKS(HW,p=0.618) in Figure 5(a) will be chosen as the benchmark for Figure 5(d) and Figure 5(g). Figure 5(d) shows that C-KSA(HW) exhibits consistently better performance compared with the benchmark. Distinguishers in Figure 5(g) are less efficient than the benchmark, so we do not explain them in more details. When the SNR is 1, PKS(HW,p=0.618) in Figure 5(b) is also selected as the benchmark for Figure 5(e) and 5(h). Due to the fact that Figure 5(e) and 5(h) can be analyzed in the similar way as that of Figure 5(d) and 5(g), so we do not explain them in more details. When the SNR is 8, MIA(HW) in Figure 5(c) is selected as the benchmark for Figure 5(f) and 5(i). Figure 5(f) shows that, C-KSA(HW), MP-KSA(HW) and MPC-KSA(HW) are more efficient than the benchmark, and C-KSA(HW) is the most efficient distinguisher. Distinguishers in Figure 5(i) are less efficient than the benchmark, so we do not explain them in more details. In this case, Figure 5(ii) can be analyzed in the similar way as that of Figure 5(f) and 5(i).

In summary, C-KSA(HW) is the best choice of all twelve KS test based distinguishers when the SNRs are 0.125, 1 and 8 respectively, while MIA(HW) is the best choice when the SNR goes into positive infinity. Additionally, MPC-KSA(HW) is no worse than the benchmark.

- An Adversary with a Generic Power Model. Due to the computation cost, we select the SNRs of 16, 32, 64 and positive infinity in this scenario. Figure 6 shows the success rate of twelve KS test based distinguishers and MIA using an ID model against UWSB leakage of the first AES S-box. In this scenario, we organize the experimental results in the same way as those used in the ***An Adversary with a Perfect Power Model*** scenario.

In Group A, Figure 6 shows that, KSA(ID), norm-KSA(ID) and MIA(ID) fail to recover the correct key, while PKS(ID) can not reveal the correct key with a relative small number of traces. The best distinguisher in Group A will be selected as the benchmark to verify the effectiveness of the nine new variants of the KS test based distinguisher in Group B and Group C. Since none of the distinguishers in Group A can reveal the correct key with a relative small number of traces, so we divide the distinguishers into Group B and Group C respectively. The distinguishers in Group B can recover the correct key with a trace number of 4,000, while the distinguishers in Group C fail to do that. For example, when the SNR is 0.125, C-KSA(ID), norm-C-KSA(ID) and MPC-KSA(ID) in Group B can recovery the correct key (see Figure 6(d)), while other new variants of KS test based distinguishers in Figure 6(g) to do that with 4,000 of power traces. Additionally, C-KSA(ID) is most efficient in terms of SR under the four noise levels.

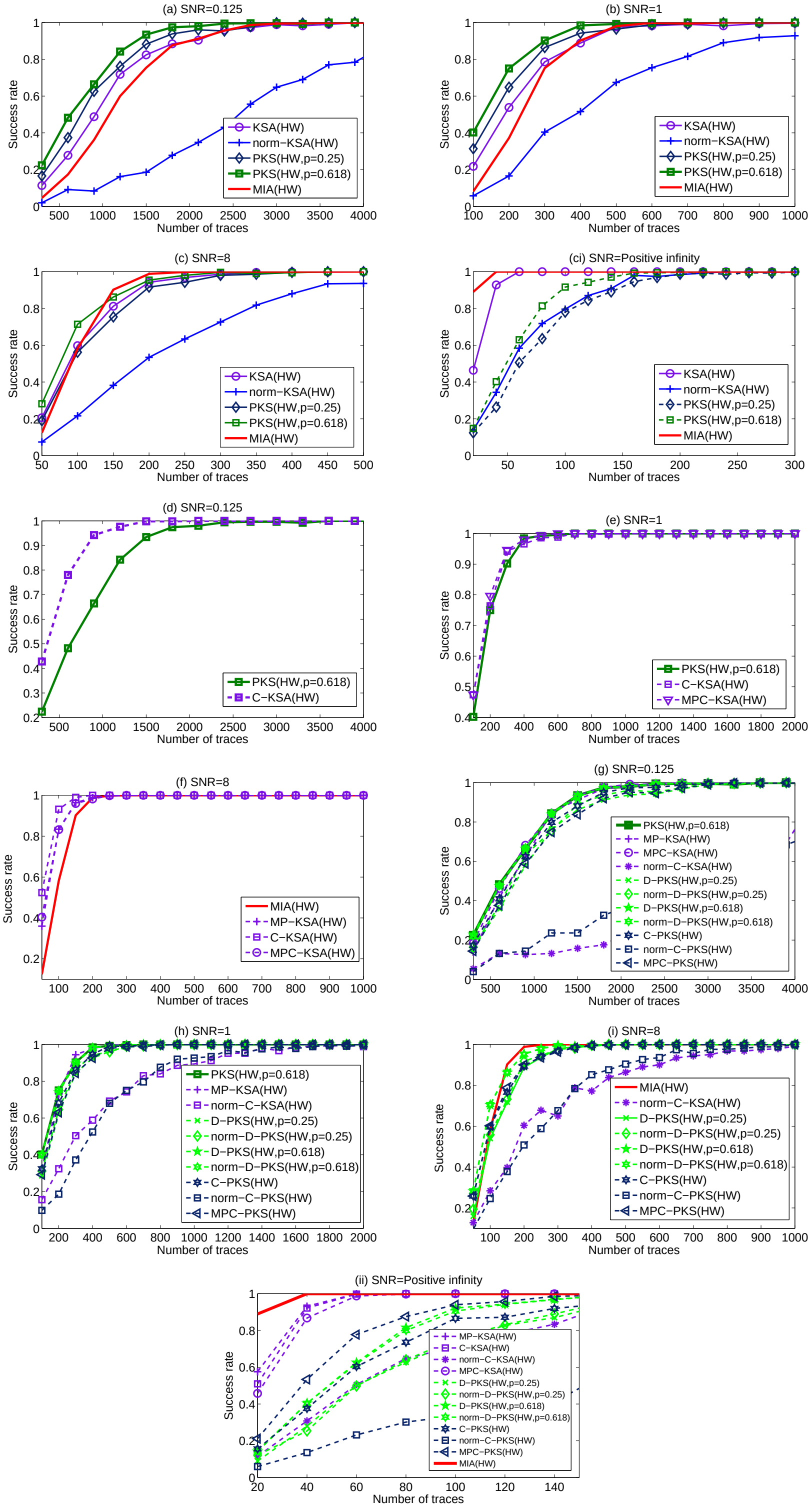

Fig. 5. Success rate of different distinguishers against the first AES S-box in UWSB leakage

To sum up, C-KSA(ID), norm-C-KSA(ID) and MPC-KSA(ID) are more efficient than the benchmark, and C-KSA(ID) is the best choice of all twelve KS test based distinguishers when the SNRs are 0.125, 1, 8 and positive infinity.

Highly Nonlinear Leakage Scenario. In highly nonlinear leakage scenario, we mean that the leakage function of cryptographic device is a highly nonlinear function. Without loss of generality, S-box is used in this leakage scenario[18]. Our experimental results show that all twelve KS test based distinguishers fail to recover the correct key in this scenario.

Note: When SNR goes into positive infinity, the performance of PKS with a fixed parameter may decrease with the increase of the trace number. This indicates that the parameter in PKS is critical to the performance of PKS, as is shown in [15].

4.3 Practical Experiments

In order to show how these twelve KS test based distinguishers behave in practical scenarios, we perform attacks against the unprotected software AES implementation on 8-bit microcontroller and the unprotected hardware AES implementation on Xilinx Vertex-5 FPGA respectively. These power traces are from OpenSCA [1] (Case 1) and from DPA Contest v2 [2] (Case 2) respectively.

In the view of an adversary, we will choose the power model according to our priori knowledge. Specifically, we will use the Hamming weight model in Case 1, and Hamming distance (HD) model in Case 2. We will choose SR as our evaluation metric to evaluate the efficiency, by amounting key recovery attacks 300 times. In this part, the experiments are also organized exactly in the same way as that in our simulated experiments [3], except that we also perform CPA attacks. This means that we place CPA distinguisher in Group D. That is to say, in practical experiments, we will show the performance of traditional CPA distinguisher, which is widely believed to be well capable of characterizing linear leakages.

Case 1: Unprotected Software AES Implementation Provided by OpenSCA

In this scenario, the output of the first S-box of the first round of AES operation is chosen as the target. We divide the distinguishers into four groups, and they are Group A, Group B, Group C and Group D. Group A only consists of four existing distinguishers and they are PKS(HW), KSA(HW), norm-KSA(HW) and MIA(HW), and the best of these four distinguishers will be selected as the benchmark accordingly. Group B and Group C contain nine new variants of KS test

[1] leakages in the DPA Demo folder. http://www.cs.bris.ac.uk/home/eoswald/opensca.html

[2] leakages in DPA_contest2_public_base_diff_vcc_a128_2009_12_23 folder with secret key 0x08 0x2e 0xfa 0x98 0xec 0x4e 0x6c 0x89 0x45 0x28 0x21 0xe6 0x38 0xd0 0x13 0x77. http://www.dpacontest.org/v2/download.php

[3] PKS distinguisher used here is shown in the formula (7).

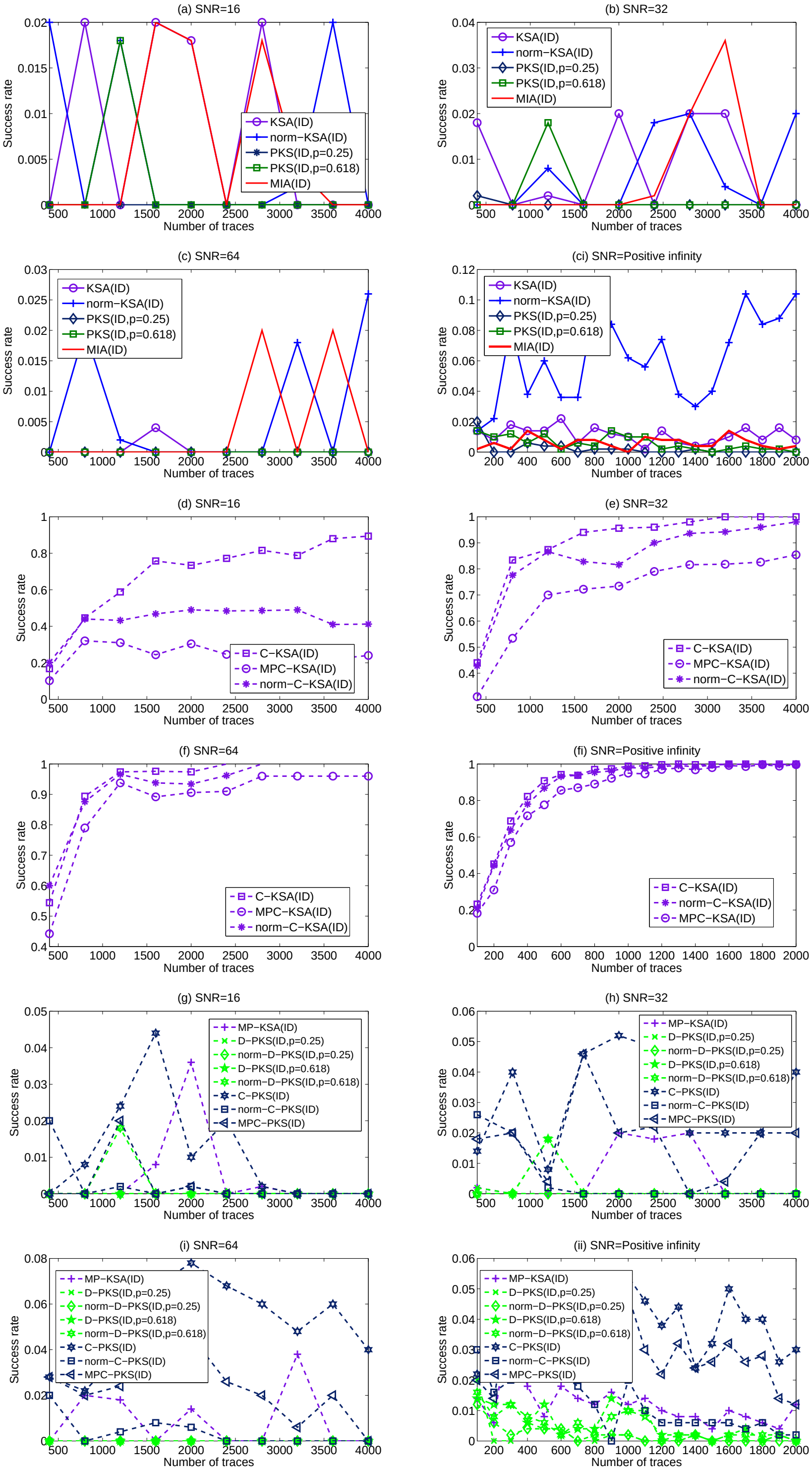

Fig. 6. Success rate of different distinguishers against the first AES S-box in USWB leakage

based distinguishers. Distinguishers in Group B are those more efficient than the benchmark, while distinguishers in Group C are those less efficient than the benchmark. In Group D, we will compare the best distinguisher in Group B with CPA. For example, in this scenario, Group B consists of one distinguishers, and it is MP-KSA(HW). Group C consists of eight distinguishers, and they are C-KSA(HW), norm-C-KSA(HW), MPC-KSA(HW), D-PKS, norm-D-PKS, C-PKS(HW), norm-C-PKS(HW) and MPC-PKS(HW). In Group A, Figure 7 (a) shows that, KSA (HW) exhibits the best performance among three existing KS test based distinguishers, so KSA(HW) is used as the benchmark for Figure 7(b) and 7(c). In Group B, Figure 7(b) shows that, MP-KSA(HW) is more efficient than the benchmark. In Group C, Figure 7(c) shows that, other new variants of KS test based distinguishers are less efficient than the benchmark. In Group D, Figure 7(d) shows that, MP-KSA(HW) is less efficient than CPA(HW).

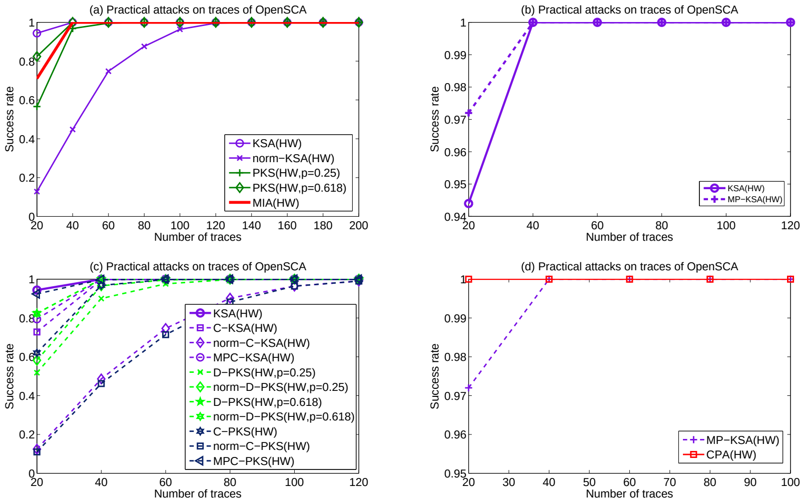

Fig. 7. Success rate for KS test based distinguishers with HW model, MIA(HW) and CPA(HW) in attacks against the first AES S-box

In summary, MP-KSA(HW) is the best choice in all these KS test based distinguishers in this case. In the view of an adversary, CPA is an ideal distinguisher. This indicates that, when the leakage of a cryptographic device could be accurately characterized, CPA is the best choice compared with all KS test based distinguishers.

Case 2: Unprotected Hardware AES Implementation Provided by DPA Contest v2

In this scenario, the input of the first S-box of the last round of AES operation is chosen as the target. That is to say, we try to attack the last round of AES encryption[1]. In Group A, Figure 8(a) shows that, both PKS(HD) and MIA(HD) can reveal the correct key, while KSA(HD) and norm-KSA(HD) fail to do that. The empirical parameter in PKS(HD) can largely improve the performance of PKS(HD). Therefore, PKS(HD,p=0.01) is selected as the benchmark for finding the most promising variants in this case. In Group B, Figure 8(b) shows that, MPC-KSA(HD) and MPC-PKS(HD) outperform PKS(HD,p=0.01) in terms of achieving a partial success rate of 80%. In Group C, other KS test based distinguishers are less efficient than the benchmark, so we do not discuss them into detail. In Group D, Figure 8(d) shows that, MPC-KSA(HD) is even better than CPA(HD).

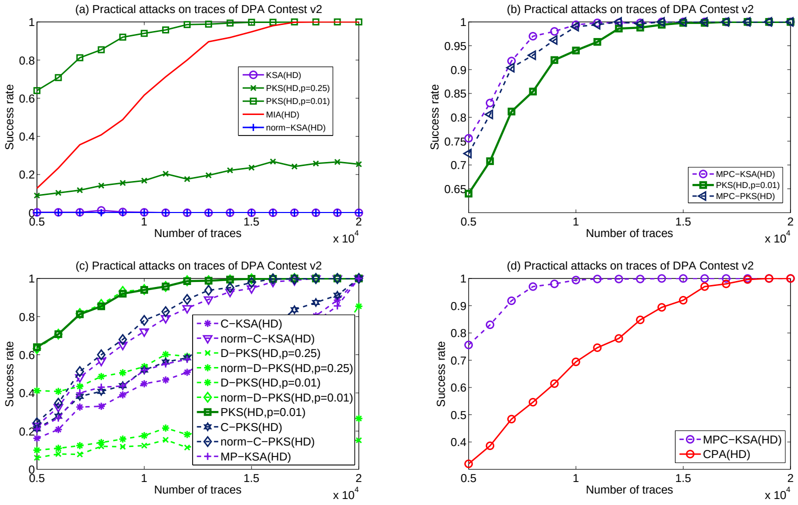

Fig. 8. Success rate for the KS test based distinguishers with HD model, MIA(HD) and CPA(HD) in attacks against the first AES S-box of the last round

Table 2. Number of Traces Required to Achieve Partial Success Rate of 80% on individual byte

	byte 1	byte 2	byte 3	byte 4	byte 5	byte 6	byte 7	byte 8
MPC-KSA	5,300	6,100	5,700	9,800	9,600	5,500	4,800	6,800
CPA	12,500	10,000	6,900	7,000	12,700	6,000	5,900	7,400
	byte 9	byte 10	byte 11	byte 12	byte 13	byte 14	byte 15	byte 16
MPC-KSA	4,500	5,200	9,200	3,500	4,100	14,500	6,000	5,500
CPA	6,800	3,600	10,000	3,000	6,600	16,900	15,000	5,100

[1] The target intermediate value is selected as the official website of DPA Contest v2 has suggested.

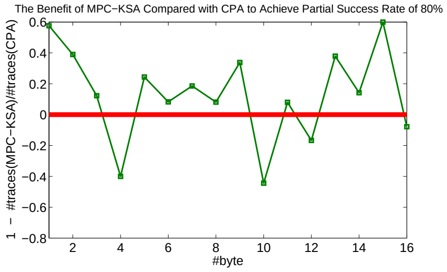

Fig. 9. To achieve partial success rate of 80%, the benefit of MPC-KSA compared with CPA

In order to enhance the understanding on whether or not MPC-KSA is a reasonable alternative for CPA, we perform attacks on all 16 bytes of AES encryption. Table 2[1] shows the number of traces required to achieve a partial success rate of 80% of attacks on individual bytes. Compared with CPA, MPC-KSA is more efficient on 12 bytes (byte 1, byte 2, byte 3, byte 5, byte 6, byte 7, byte 8, byte 9, byte 11, byte 13, byte 14, byte 15), and less efficient on other 4 bytes (byte 4, byte 10, byte 12, byte 16). The number of required traces for MPC-KSA to achieve a partial success rate of 80% is 6,000, while that of CPA is 15,000 for byte 15. However, the number of required traces for MPC-KSA to achieve a partial success rate of 80% is 9,800, while that of CPA is 7,000 for byte 4. Therefore, MPC-KSA does not perform consistently better than CPA, but it performs better than CPA on 75% of bytes, as it is shown in Figure 9. As a whole, MPC-KSA is more efficient than CPA in terms of the required number of traces to achieve the global success rate of 80%. In summary, MPC-KSA is the best choice in this case. This experimental result indicates that, when the leakages of a cryptographic device could not been accurately characterized, MPC-KSA exhibits better performance than CPA in terms of SR, as the former is capable of measuring the total dependency between hypothetical power consumptions and physical leakages.

5 Conclusions

Distinguishers play an vital role in exploiting physical leakages in side-channel attacks. Due to the capability of dealing with both linear and nonlinear dependencies, generic side-channel distinguishers are being increasingly popular. Among those are KS test based distinguishers, such as KSA and PKS. In this paper, we constructed nine variants of the KS test based distinguishers via combining different construction strategies of KSA and PKS, and then explored the

[1] Since traces provided by OpenSCA only contain the leakage of the first byte of S-box of AES in the first round, we do not compare the performance of KS test based distinguishers in terms of global success rate.

effectiveness and efficiency of twelve KS test based distinguishers and MIA in typical simulated scenarios and practical scenarios.

In simulated scenarios, we considered the influence of different factors, such as leakage function, noise level and power model. Experimental results provide a balanced view of how to choose the most suitable KS test based distinguisher in a certain scenario. Specifically, experimental results show that, MP-KSA exhibits better performance than other KS test based distinguishers when the SNR is moderately high. MPC-KSA and C-KSA are more robust to noise than the other KS test based distinguishers in terms of low SNR. An interesting point is that C-KSA and MPC-KSA share generic potential with PKS, and are more efficient than PKS.

In practical scenarios, we performed attacks against two typical unprotected AES implementations. Experimental results show the realistic meaning of KS test based distinguishers in practice. For example, we find that MPC-KSA is more efficient than CPA against the unprotected hardware AES implementation on Xilinx Vertex-5 FPGA in DPA Contest v2.

In a whole, we experimentally investigated the performance of the KS test based distinguishers, and provided some helpful guides on how to choose a suitable distinguisher. However, we did not provide any theoretical analysis yet about why this happens, which could be part of our future work.

Acknowledgments This work was supported in part by National Natural Science Foundation of China (No. 61272478, 61073178, 60970135 and 61170282), Beijing Natural Science Foundation (No. 4112064), Strategic Priority Research Program of the Chinese Academy of Sciences (No.XDA06010701), and IIE Cryptography Research Project (No. Y2Z0011102).

References

1. P. Kocher, J. Jaffe and B. Jun. Differential Power Analysis. CRYPTO 1999. LNCS 1666, pp.388-397, 1999.
2. T.S.Messerges, E.A.Dabbish and R.H.Sloan. Examining Smart-Card Security under the Threat of Power Analysis Attacks. IEEE Transactions on Computers. Vol.51, No.5, pp.541-552,2002.
3. E.Brier, C.Clavier and F.Olivier. Correlation Power Analysis with a Leakage Model. CHES 2004. LNCS 3156, pp.16-29, 2004.
4. Thanh-Ha Le, J.Cldire, C.Canovas, B.Robisson, C.Servire and Jean-Louis Lacoume. A Proposition for Correlation Power Analysis Enhancement. CHES 2006. LNCS 4249, pp.174-186, 2006.
5. S.Mangard, E.Oswald, and F.-X.Standaert. All for one-one for all: Unifying univariate DPA attacks. IET Information Security. Vol.5, No.2, pp.100-110, 2011.
6. J.Doget, E.Prouff, M.Rivain and F.-X.Standaert. Univariate side channel attacks and leakage modeling. Journal of Cryptographic Engineering. Vol.1, No.2, pp.123-144, 2011.
7. B.Gierlichs, L.Batina, P.Tuyls and B.Preneel. Mutual Information Analysis: A Generic Side-Channel Distinguisher. CHES 2008. LNCS 5154, pp.426-442, 2008.

8. Young-II Moon, B.Rajagopalan and U.Lall. Estimation of Mutual Information using Kernal Density Estimators. Physical Review E. Vol.52, pp.2318-2321, 1995.
9. Janett Walters-Williams and L.Yan Estimation of Mutual Information: A Survey. RSKT 2009. LNCS 5589, pp.389-396, 2009.
10. Tomas Marek, Petr Tichavsky. On The Estimation Of Mutual Information. ROBUST 2008. Available at http://www.utia.cas.cz/DAR-publications
11. N.Veyrat-Charvillon and F.-X.Standaert. Mutual Information Analysis: How, When and Why? CHES 2009. LNCS 5747, pp.429-443, 2009.
12. L.Batina, B.Gierlichs, E.Prouff, M.Rivain, F.-X.Standaert and N.Veyrat-Charvillon Mutual Information Analysis: A Comprehensive Study. Journal of Cryptology. Vol.24, Issue 2, pp.269-291, 2011.
13. E.Prouff and M.Rivain. Theoretical and practical aspects of mutual information based side channel analysis. ACNS 2009. LNCS 5536, pp.499-518, 2009.
14. C.Whitnall, E.Oswald and L.Mather. An Exploration of the Kolmogorov-Smirnov Test as Competitor to Mutual Information Analysis. CARDIS 2011. LNCS 7079, pp. 234-251, 2011.
15. L.Jiye, Z.Yongbin, Y.Shuguo and F.Dengguo. Generic Side-Channel Distinguisher Based on Kolmogorov-Smirnov Test: Explicit Contruction and Practical Evaluation. Chinese Journal of Electronics. Vol.21, No.3, pp.547-553, 2012.
16. C.Whitnall, E.Oswald, and F.-X.Standaert. The myth of generic DPA...and the magic of learning. Cryptology ePrint Archive. Avaliable at http://eprint.iacr.org/2012/256.pdf
17. S.Mangard, E.Oswald and T.Popp. Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer-Verlag, 2007.
18. C.Whitnall and E.Oswald. A Fair Evaluation Framework for Comparing Side-Channel Distinguishers. Journal of Cryptographic Engineering. Vol.1, Issue.2, pp.145-160, 2011.
19. F.-X. Standaert, T.Malkin and M.Yung. A unified framework for the analysis of side-channel key recovery attacks. EUROCRYPT 2009. LNCS 5479, pp.443-461, 2009.
20. F.-X.Standaert, B.Gierlichs and I.Verbauwhede. Partition vs Comparison Side-Channel Distinguishers: An Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices. ICISC 2008. LNCS 5461, pp.253-267, 2009.
21. Mehdi-Laurent Akkar, Regis Bevan, Paul Dischamp, Didier Moyart. Power Analysis, What Is Now Possible. ASIACRYPT 2000. LNCS 1976, pp.489-502, 2000.
22. S.Chari, Josyula R.Rao and P.Rohatgi. Template attacks. CHES 2002. LNCS 2523, pp.13-28, 2002.

6 Appendix A

In this part, we provide the results of simulated experiments in terms of Guessing Entropy(GE). These results are shown in Figure 10, 11, 12 and 13. Such figures contain the results of key recovery attacks using the twelve KS test based distinguishers and MIA as well. For ease of analysis and comparison, these results are also organized in the same way as those used in Section 4.2.

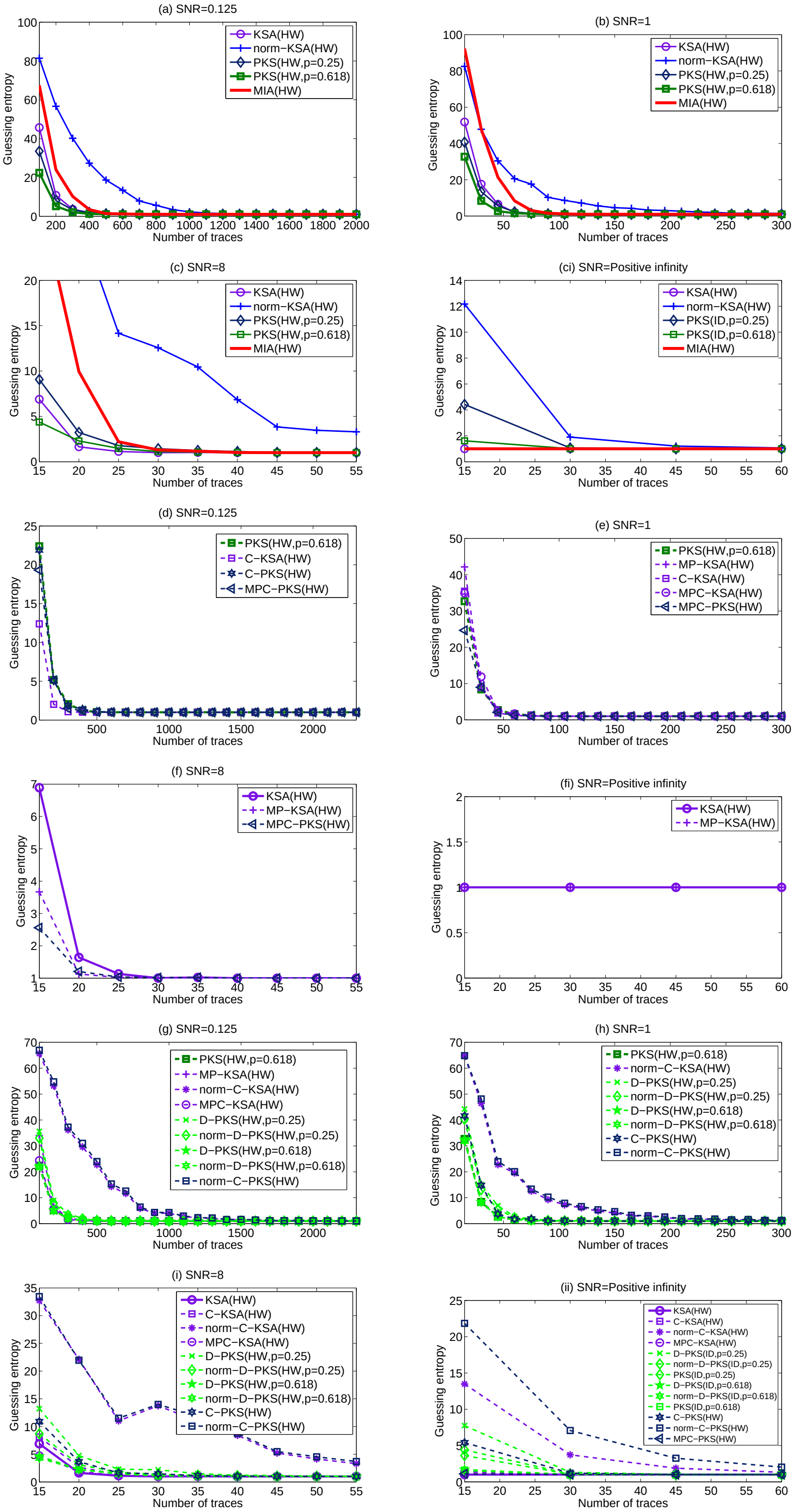

Fig. 10. Guessing entropy of different distinguishers against the first AES S-box in Hamming Weight leakage

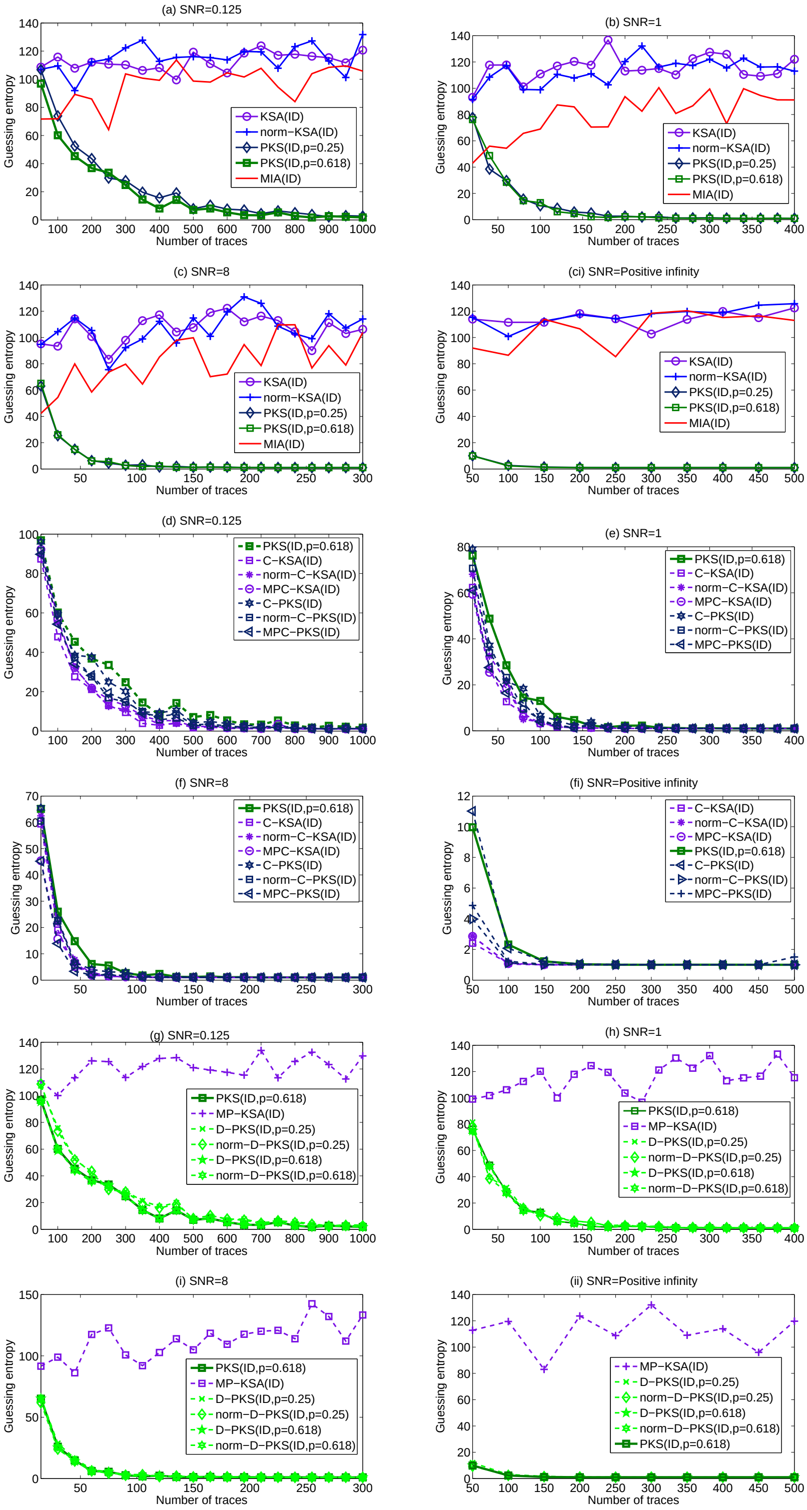

Fig. 11. Guessing entropy of different distinguishers against the first AES S-box in Hamming Weight leakage

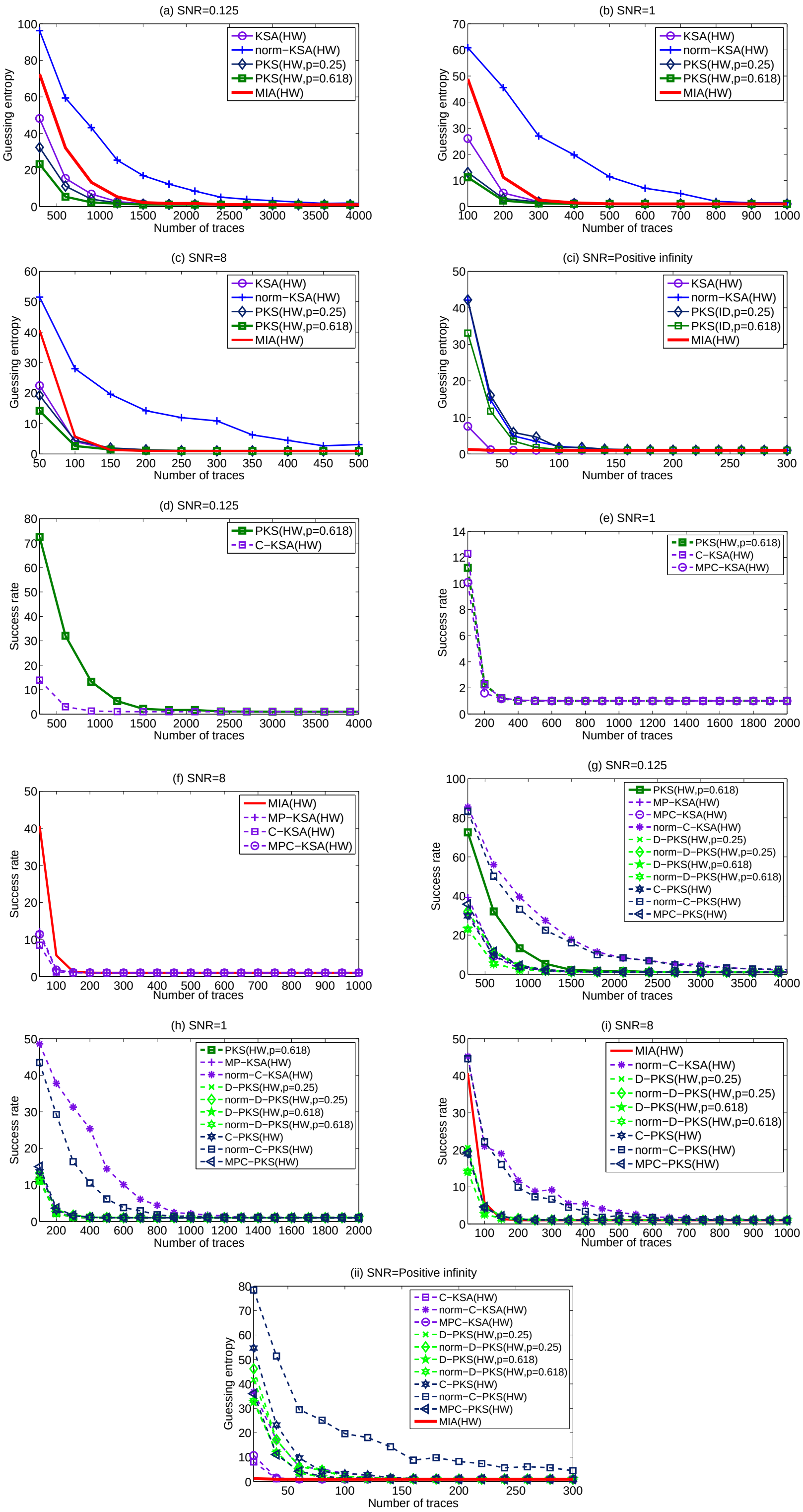

Fig. 12. Guessing entropy of different distinguishers against the first AES S-box in UWSB leakage

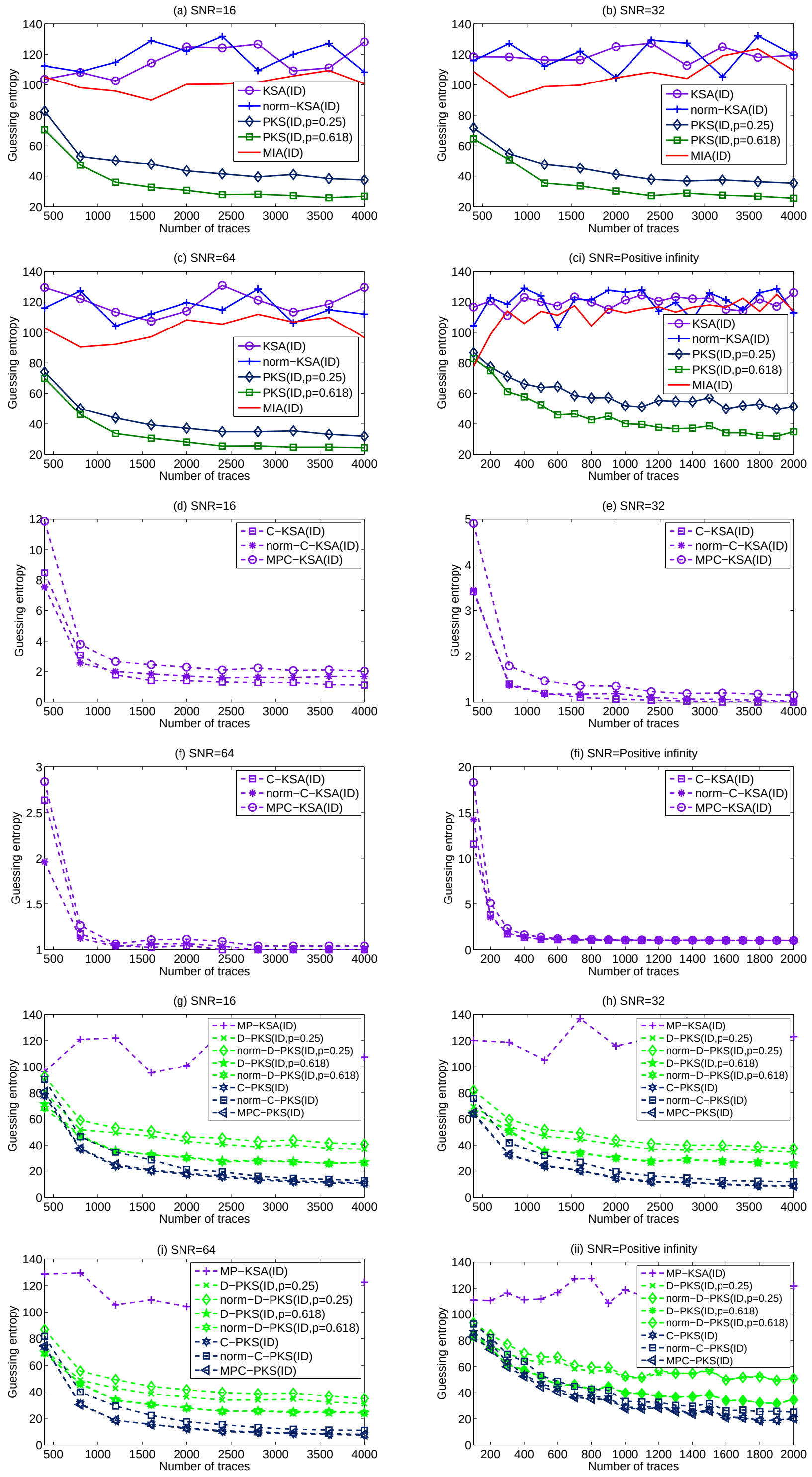

Fig. 13. Guessing entropy of different distinguishers against the first AES S-box in USWB leakage