On the Negative Effects of Trend Noise and Its Applications in Side-Channel Cryptanalysis

Yuchen Cao[1], Yongbin Zhou[1,⋆] and Zhenmei Yu[2]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences,
89A, Mingzhuang Rd, Beijing, 100093, P.R. China
{YuchenCao,YongbinZhou}@iie.ac.cn
[2] School of Information Technology,
Shandong Women's University,
45, Yuhan Rd, Jinan, 250002, P.R. China
{yuzhenmei@gmail.com}

Abstract. Side-channel information leaked during the execution of cryptographic modules usually contains various noises. Normally, these noises have negative effects on the performance of side-channel attacks exploiting noisy leakages. Therefore, to reduce noise in leakages usually serves to be an effective approach to enhance the performance of side-channel attacks. However, most existing noise reduction methods treat all noises as a whole, instead of identifying and dealing with each of them individually. Motivated by this, this paper investigates the feasibility and implications of identifying trend noise from any other noises in side-channel acquisitions and then dealing with it accordingly. Specifically, we discuss the effectiveness of applying least square method (LSM for short) to remove inherent trend noise in side-channel leakages, and also clarify the limited capability of existing noise reduction methods in dealing with trend noise. For this purpose, we perform a series of correlation power analysis attacks, as a case of study, against a set of real power traces, published in the second stage of international DPA contest which provides a public set of original power traces without any preprocessing, from an unprotected FPGA implementation of AES encryption. The experimental results firmly confirmed the soundness and validity of our analysis and observations.

Keywords: side-channel cryptanalysis; information leakage; noise shape; trend noise; power analysis attack

1 Introduction

A physical implementation of a cryptographic algorithm usually leaks some physically observable information which is associated with the intermediate results of the algorithm. This kind of unintentional and unexpected information when its running is referred to as side-channel information, the sources of which include execution time[1], power consumption[2], electromagnetic radiation[3] and so on. Side-channel information is usually correlated with data manipulated and operation performed in the cryptographic implementation. Therefore, if this side-channel information is statistically analyzed, the secret key value can still be recovered although the cryptosystem is provable secure in black-box model. These attacks are usually referred to as side-channel attacks.

Among others, power analysis attack which uses the power consumption as its side-channel leakage is one of the most widely researched powerful side-channel attacks.The acquisition of the instantaneous power consumption of a physical implementation is the requisite for mounting power analysis attacks. The output of this acquisition process is referred to as power traces. Because of the electronic characteristics of the physical implementation, power traces always contain not only useful side-channel information which benefits power analysis attacks, but also a variety of noises which are found to have negative effects on the performance of side-channel attacks[5]. Therefore, to reduce noises inherent in power traces is commonly believed to be, in general, an effective approach enhancing the performance of power analysis attacks.

In order to reduce noises contained in power traces after sampling(i.e. to increase the signal-to-noise ratio(SNR for short)), a number of noise reduction methods are proposed, including applying wavelet

⋆ Corresponding Author

transform[6][7] and principal component analysis(PCA for short) transform[8] to sampled power traces. In [6], one applies wavelet transform to original power traces from a hardware implementation of unprotected DES on smart card, producing an approximation sub-signal. Afterwards, one performs differential power analysis(DPA for short)[2] on the approximation sub-signal. Additionally, authors in [6] use the highest peak in differential trace to assess the effectiveness of noise reduction. It is pointed out in [6] that although this method is capable of improving SNR, the correct key guess does not always correspond to the highest peak of DPA. [7] also applies wavelet transform into original power traces to obtain the approximation sub-signal and the detail sub-signal. The difference between [7] and [6] is that the former one sets a specific threshold value for the detail sub-signal, and sets the detail coefficients that dissatisfy the threshold to 0. Afterwards, one reconstructs the power traces and then performs power analysis attacks on the reconstructed power traces. In [8], one applies PCA to original power traces, and then performs a DPA attack on a PCA-transformed power traces.

These three noise reduction methods share one thing in common that they treat all noises as a whole, instead of identifying and dealing with each of them individually. Concerning noise reduction in power traces, a very natural and pertinent question arises at this point. Namely, is there any noise of specific shape contained in sampled power traces; and if any, how does it influence the performance of power analysis attacks?

1.1 Our Contributions

In this paper, we try to address the above-mentioned problem from the following three aspects. First of all, given certain side-channel leakages (i.e. sampled power traces in this paper), what kind of noises with specific shape does it consist of? Secondly, if there is some sort of noise with specific shape contained in the power traces, how and to what extent does this noise influence the performance of power analysis attacks? Whether or not will this influence be negligible? Thirdly, if the effects of certain noise of specific shape on power analysis attacks are not negligible, are those existing noise reduction methods well capable of eliminating this specific noise from power traces? If no, is there any effective method to eliminate the noise?

Specifically, we take correlation power analysis attack(CPA for short)[4] which is proved statistically close to most popular power analysis attacks [10] as a case of study, and focus only on the noise with a wavelength longer than the record length of power trace. In the research field of signal processing, this kind of noise is referred to as trend noise. The reason why we choose trend noise as our main object is three-fold. First of all, trend noise has a specific frequency characteristic much different from that of the most pertinent side-channel information. This will certainly makes it much easier for one to identify trend noise from power traces. Secondly, techniques for eliminating trend noise are easy to be adapted to frequency domain. For example, one can easily extend these ideas to the noises of high frequencies. Last but not the least, techniques for trend removal are relatively mature in the field of signal processing. Consequently, we could save time on designing effective trend removal method, and thus concentrate more on the influence of the trend noise on power analysis attacks.

In order to assess the effects of trend noise on the performance of power analysis attacks (resp. the effectiveness of applying trend removal), we perform CPA attack both on a set of real power traces published in the second stage of DPA Contest and on the same set of power traces after a certain trend removal process, as a case of study. For a fair and objective of evaluation, we adopt the unified framework proposed in [9], where some quantative metrics are used. These metrics cover success rate (SR for short) at a certain number of power traces, the number of power traces required to achieve a certain SR, and etc. Intuitively, given a certain number of power traces, the higher the SR of CPA attack is, the less serious the negative effects of trend noise is (resp. the more effective the corresponding trend removal is). The similar philosophy also holds for the case of the number of power traces required to achieve a certain SR.

Our real CPA attacks performed reveal the following two important observations.

Observation I. The number of power traces required to achieve a SR of 0.8 when doing CPA attack on original power traces after trend removal is 45% less than that on same power traces without any trend removal. Similarly, given any 12,000 power traces, the SR of doing CPA attack on original power traces (without any trend removal) is 0.856, while that on the same power traces after trend removal is 0.992. This implies that trend noise has significant negative effects on the performance of power analysis attacks. These negative effects are non negligible.

Observation II. The number of power traces required to achieve a SR of 0.8 when doing CPA attack on original power traces after de-noising with trend removal, and existing noise reduction methods (Wavelet transform based methods in [6][7] and PCA-based method in [8]) is about half of that on the same power traces after de-noising only with the corresponding existing noise reduction methods. A similar phenomenon holds also for the case of the SR of CPA attack at a certain number of power traces. This shows that existing noise reduction methods have a limited capability in dealing with trend noise.

Observation I together with ***Observation II*** shows that the application of noise reduction methods targeted certain noise with specific shape proves to be a promising and effective method in increasing the power of eliminating noises (and thus in enhancing the performance of power analysis attacks).

The rest of this paper is structured as follows. Section 2 briefly describes some relevant background knowledge, including composition of power trace and trend removal method using least square method (LSM for short). The negative effects of trend noise on power analysis attacks are investigated in Section 3. Section 4 mainly discusses the advantages of LSM over other existing noise reduction methods in eliminating trend noise. Section 5 concludes the whole paper.

2 Preliminaries

This section will present some relevant background knowledge of this article, including composition of power traces, SNR, the relationship between SNR and CPA, and a widely used trend removal method using LSM in signal processing.

2.1 Composition of Power Trace

Power analysis attacks exploit the fact that the power consumption of cryptographic modules is related to the operations performed and the data processed. For each single point of a power trace, we denote the operation-dependent component of a point by P_{op}, the data-dependent component by P_{data}. In practice the power measurements are not always the same even if the operation performed and data manipulated are fixed, and these differences are caused by the characteristics of the physical implementation. We refer to this noise component of power consumption as $P_{el.noise}$. Besides, each point also has a constant component denoted by P_{const} that is for example caused by leakage currents. Therefore, we can define each point of a power trace by (1).

$$P = P_{op} + P_{data} + P_{el.noise} + P_{const} \tag{1}$$

Note that different power analysis attacks often exploit different properties of P_{op} and P_{data}. We refer to the properties that exploited by a given attack as P_{exp}. For example, for SPA, P_{exp} equals to the combination of P_{op} and P_{data}, but for DPA, P_{exp} is only a part of P_{data}. We refer to the rest part of the sum of P_{op} and P_{data} which is not exploitable by a given attack as $P_{sw.noise}$. So we can rewrite (1) to (2) in a given attack scenario.

$$P = P_{exp} + P_{sw.noise} + P_{el.noise} + P_{const} \tag{2}$$

In this paper, ***we take the electronic noise ONLY into consideration.*** Under this assumption, we know from [5] that P_{exp} and $P_{el.noise}$ are the most important components. And because P_{const} provides no useful information for key recovery, it has nothing to do with power analysis attack.

2.2 SNR (Signal to Noise Ratio)

Under our assumption and in a given attack scenario, SNR of a set of power traces at a fixed point is given by (3), in which $\sigma(x)$ denotes the variance of x.

$$SNR = \frac{\sigma(P_{exp})}{\sigma(P_{el.noise})} \tag{3}$$

SNR quantifies the amount of information that leaks from a point of a set of power traces. The equation $\rho(H_i, P) = \rho(H_i, P_{exp})/\sqrt{1 + 1/SNR}$ [5] shows the relationship among the correlation coefficient

$\rho(H_i, P)$ between the hypothetical power consumption values and the real power consumption values, the correlation coefficient $\rho(H_i, P_{exp})$ between the hypothetical power consumption values and the real side-channel leakages and SNR. It can be seen that the decrease of SNR can effectively enhance the value of $\rho(H_i, P)$ with given power traces. Besides this, in [5] the number of power traces needed to break a cryptographic implementation by CPA which is referred to as n can be estimated by (4).

$$n = 3 + 8\frac{Z_{1-\alpha}^2}{ln^2\frac{1+\rho(H_{ck},P)}{1-\rho(H_{ck},P)}} \tag{4}$$

where $Z_{1-\alpha}$ is a quintile of a normal distribution for a 2-sided confidence interval with error $1-$. And under our assumption, we can rewrite (4) into (5).

$$n = 3 + 8\frac{Z_{1-\alpha}^2}{ln^2\frac{SNR+\rho(H_{ck},P_{exp})}{SNR-\rho(H_{ck},P_{exp})}} \tag{5}$$

We can see that with the decrease of SNR, n will become bigger, and the attack will become more difficult [5].So, in order to improve the performance of power analysis attacks on given power traces, attackers have to remove noises in power traces and enhance SNR.

2.3 Trend Noise and Trend Removal

Trend noise is the noise whose wavelength is longer than the record length of a given signal [13]. Trend removal methods in the field of signal processing mainly include estimating the mean trend [12], polynomial curve fitting [11], neural network modeling [14] and digital high-pass filtering. Among these methods, estimating the mean trend can only remove a constant value from the whole trace, estimating trend noises by neural network modeling requires a lot of training traces to model trend noises, and the digital high-pass filtering typically requires knowing the fundamental frequency of the part which interests the users. When taking noise reduction effect, computational cost and simplicity into consideration, polynomial fitting is a good choice and has a wide range of applications. The most common polynomial fitting method is LSM.

In order to assess the performance of trend removal using LSM, we should know exactly both trend and other noises for a given signal. For this purpose, we performed simulated experiments on a signal with certain trend. The original signal, trend, and the results of experiment are shown in Fig.1. This experiment consists of the following five steps.

First, we generated an original signal which has 120 points by a random number generator that met the Gaussian distribution $N(0, 0.5)$. The original signal was denoted as $Signal$ and shown in Fig.1(a).

Second, we produced a certain trend which is named $Trend$, where $Trend = 2\sin(\pi \cdot \frac{i}{80}), i = 0, 1, 2, ..., 119$, and this trend is shown in Fig.1(c).

Third, the signal mixed trend named $Signal'$ was computed by $Signal' = Trend + Signal$. And Fig.1(b) shows the curve of $Signal'$.

Fourth, LSM was applied to fit $Trend$, and we got $Trend'$ which is shown as trend' getting by LSM in Fig.1(c).

Last, we computed $Signal''$ by $Signal'' = Signal' - Trend'$, where $Signal''$ illustrated in Fig.1(d).

From the steps above, we can see that fitting $Trend$ with LSM is the most important step for trend removal using LSM. There are several steps to fit the trend noise by LSM. First of all, if we adopt polynomial of degree K to fit the trend noise, we need construct a function of trend noises as (6).

$$Trend'(i) = \sum_{k=0}^{K}(a_k \cdot i^k), i = 0, 1, 2, ..., 119 \tag{6}$$

In (6), a_k is the polynomial coefficient, i refers to a certain sampling point of $Signal'$. In practice, if the value of K is too big, the fitting costs and fitting error will be increased. In the field of digital signal processing, in order to better fit the trend of curve, the value of K always ranges from 3 to 5. Therefore, we choose $K = 3$ for this experiment. Next, define the error of the intermediate function between $Signal'$ and $Trend$ as (7), use LSM to find the coefficient, and then we come to the fitting polynomial of the trend noise.

$$E(i) = Signal'(i) - Trend'(i), i = 0, 1, 2, ..., 119 \tag{7}$$

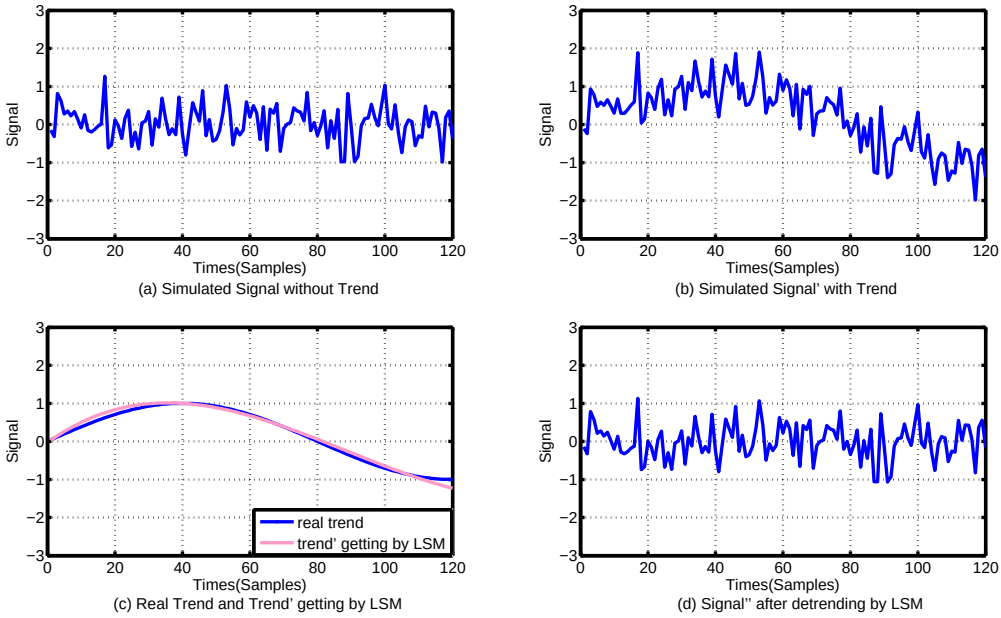


Fig. 1. Trend Removal by LSM

From Fig.1(c) we can see that the curve of $Trend'$ is approximately the same as that of $Trend$, and the Pearson correlation between $Trend$ and $Trend$ is 0.9948 which is approximately equal to 1. In order to determine whether the LSM can effectively eliminate trend noises of signal, we calculated the Pearson correlation coefficient between $Signal$ and $Signal'$ and between $Signal$ and $Signal''$. And we reach the results that the correlation coefficient between $Signal$ and $Signal'$ is 0.5883, and the correlation coefficient between $Signal$ and $Signal''$ reached 0.9870, which is much greater than 0.5883, increased by 67.77%. Therefore, this implies that LSM can effectively identifying the trend noise; thereby it can reduce the influence of the trend noise over the power analysis attack.

3 The Effects of Trend Noise on Side-Channel Attacks

In this section, we will show the existence of trend noise in real power traces, and then investigate how and to what extent the level of trend noise influences the performance of power analysis attacks.

3.1 The Existence of Trend Noise in Real Power Traces

From the discussion in Section 2, we know that LSM can be used to effectively fit the trend noise in simulated power traces. In this section, taking a random power trace in DPA contest V2 for an example, we will illustrate the existence of trend noise in real power traces. We adopt cubic polynomial to fit trend noise, and then generate the corresponding de-trended power trace by applying LSM-based trend removal to the original power trace. The results are shown in Fig.2.

It is clearly shown in Fig.2(a) that there exists an slowly changing trend in the original power trace, and that the existence of the trend results in an apparent drift in the power trace. In Fig.2(b), we can see that after eliminating the trend noise by using LSM, the trend in the new corresponding de-trended power trace becomes much smoother, and it reduces the drift in the new power trace caused by the trend noise accordingly. This shows that the trend noise approximated by using LSM can well fit the drift of power trace. Next, we will analyze the influence of drift caused by the trend noise over power analysis attacks. Specifically, we will consider this problem in the following two cases.

Case 1. Drifts of power traces due to the trend noises are equivalent to each other. In this case, even though the trend noise could be represented as a high-order polynomial, polynomials for trends of different power traces are almost the same. Therefore, trend noise at the interesting points should be a

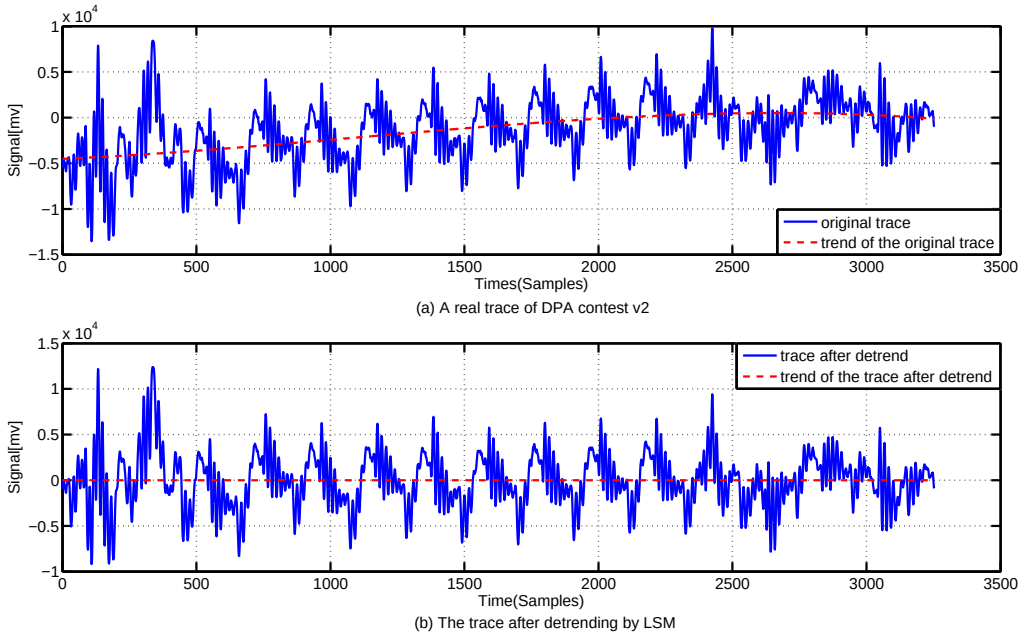
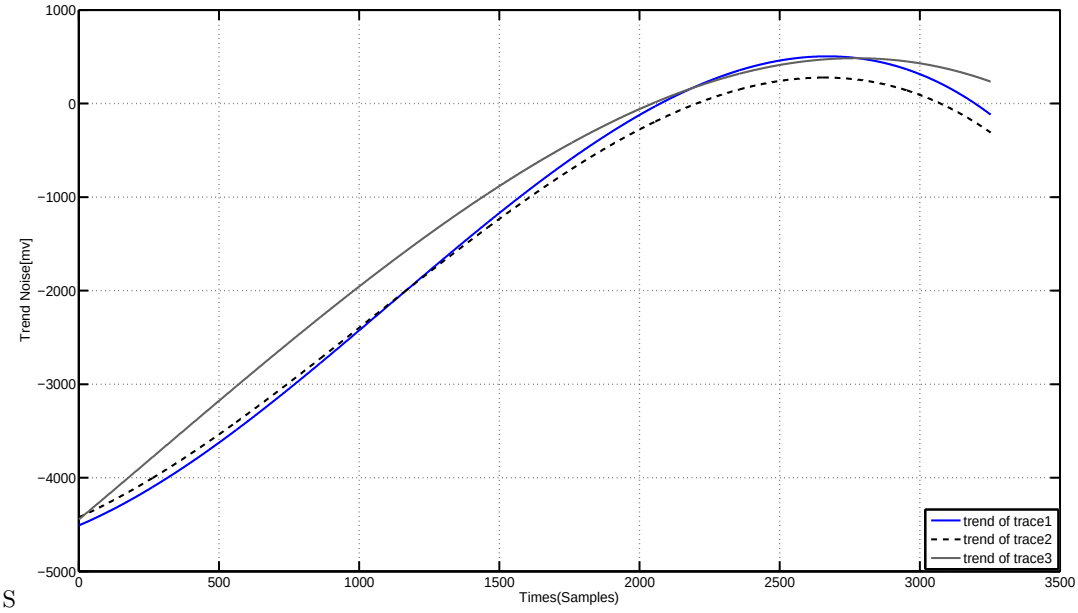


Fig. 2. One Real Trace in DPA Contest v2 and Its Corresponding De-trended Trace by LSM

constant which in this case could be eliminated by very simple averaging. Consequently, the presence of trend noise has nothing to do with the performance of power analysis attack.

Case 2. Drifts of power traces due to the trend noises are variable. Namely, trend noise at the interesting point is a stochastic variable rather than a constant. Certainly, the trend noises will reduce the SNR of the power traces. Therefore, the trend noises in this case will result in the decrement of the performance of power analysis attacks.



S

Fig. 3. Trends in Three Real Power Traces

Actually, trend noises inherent in multiple power traces are different from each other. For example, three trend noises approximated by using LSM for three real power traces published in second stage of DPA Contest are shown in Fig.3. These three power traces corresponds to AES encryption of three random plaintexts under the same secret key.

3.2 The Negative Effects of Trend Noise on Side-Channel Attacks

In section 3.1, we have shown that there really exist some trend noises in real power traces. Next we will show how and to what extent the level of trend noise influences the performance of power analysis attacks. In order to clarify this, we still perform a series of CPA attacks on a set of real power traces from DPA Contest v2. Specifically, we use a data set consisting of 20,000 power traces, whose secret key is 0x08 2E FA 98 EC 4E 6C 89 45 28 21 E6 38 D0 13 77. This data set belong to the group of sets DPA_contest2_public_base_diff_vcc_a128_2009_12_23. We divide our CPA experiments into eight categories, the details of which are summarized in Table.1.

We note that this paper mainly considers, instead of its source, *the existence of trend noise and its (negative) effects on side-channel cryptanalysis*. Source of trend noise also is an important and pertinent question, yet it is not within the scope of this paper.

Table 1. Our CPA Attacks on Real Power Traces from DPA Contest v2

Experiment Label	Description of the Experiment
CPA	perform CPA attack on the original power traces
TR(constant)+CPA	estimate the mean trend of original power traces, subtract the trend from the original power traces, and then perform CPA attacks on the resultant power traces
TR(linear)+CPA	estimate the trend by fitting with a linear polynomial, subtract the trend from the original power traces, and then perform CPA attacks on the resultant power traces
TR(quadratic)+CPA	estimate the trend by fitting with a quadratic polynomial, subtract the trend from the original power traces, and then perform CPA attacks on the resultant power traces
TR(cubic)+CPA	estimate the trend by fitting with a cubic polynomial, subtract the trend from the original power traces, and then perform CPA attacks on the resultant power traces
TR(quartic)+CPA	estimate the trend by fitting with a quartic polynomial, subtract the trend from the original power traces, and then perform CPA attacks on the resultant power traces
TR(quintic)+CPA	estimate the trend by fitting with a quintic polynomial, subtract the trend from the original power traces, and then perform CPA attacks on the resultant power traces
TR(sextic)+CPA	estimate the trend by fitting with a sextic polynomial, subtract the trend from the original power traces, and then perform CPA attacks on the resultant power traces

The results of our eight groups of experiments are shown in Fig.4, in terms of the relationship between SR and the number of traces. Fig.4 shows that SR of CPA attacks on power traces after trend removal is much higher than that on the same power traces without trend removal, which implies that trend removal can effectively improve the performance of power analysis attacks.

Among those experiments, SR of CPA attacks on power traces with trend removal using non-constant polynomial is much higher than that on the same power traces with trend removal using the mean trend. Specifically, it is shown in Fig.4 that the number of required power traces for a CPA attack on original power traces (without trend removal) to achieve a SR of 0.8 is 11,300, while that of TR (constant) +CPA is 9,350 (which is 17% less than that for CPA) and that of TR (quintic) + CPA is 6,200 (which is 45% less than that for CPA).

Another interesting point is that, in our experiments, the SR of CPA attacks on power traces with trend removal using quintic polynomial is the highest (which may not be the optimal globally if we

consider other degrees higher than six)[1]. Therefore, ***in the rest of this paper, we used trend removal with quintic polynomial ONLY in our work***.

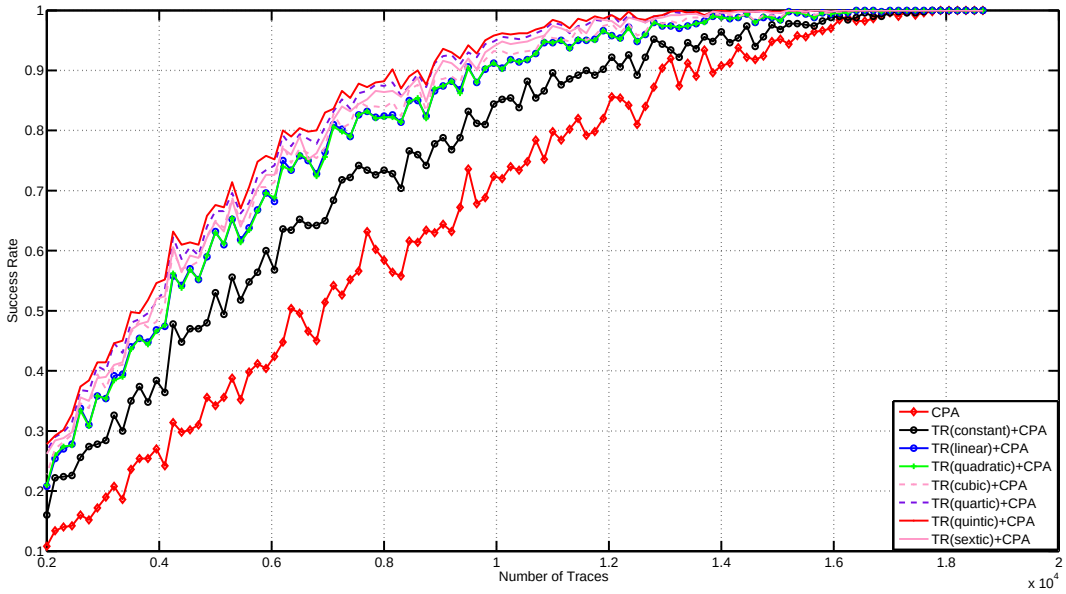


Fig. 4. CPA Attacks on Original Traces and on the Same Traces after Trend Removal with Different Polynomial Degrees

Next, we will investigate the relationship between the level of trend noise and the performance of correlation power analysis attacks, in order to show how does the performance of CPA attack change with that of trend noise. For this purpose, we will take CPA attacks on simulated traces instead of real traces[2].

In our simulated attacks, we assume that all the noise of simulated traces is caused by trend noise. We select the output of the 1st S-box of the first AES round to be the target intermediate value. We generate 6,000 simulated power traces corresponding to the encryptions of 6,000 random plaintexts under the same secret key. In this simulation scenario, the composition of one power trace is defined as (8).

$$P = P_{exp} + P_{trend} \tag{8}$$

As has been proved, SNR has a positive effect on the SR of CPA attack. In general, the higher the SNR, the higher the SR. Therefore, in simulation experiments, we fixed the variance of useful side-channel leakage $Var(P_{exp})$, and then varied the variance of the trend noise $Var(P_{trend})$ (which measures the level of trend noise of power traces). Note that in this experiment, we did not make any assumption about the shape of the trend noise.

We start the experiment with a fixed secret random key and 6,000 random plaintexts, and then generate the simulated power traces corresponding to the encryption of these random plaintexts under the same key. Next, choose $SNR = 0.25, 0.5, 1, 2, 4, 8, Infinite$, where $SNR = \frac{\sigma(P_{exp})}{\sigma(P_{trend})}$. Finally, perform CPA attacks on the generate sets of simulated power traces, the results of which are shown in Fig.5.

It is shown in Fig.5 that the SR of CPA attack decreased gradually with the increasing of $\sigma(P_{trend}$. This implies that the more trend noise in power traces is, the more negative effects it has on power analysis attacks.

[1] Note that how to choose, in a black-box context, the (optimal) degree of polynomial remains an open issue in the context of side-channel cryptanalysis. We will consider researching this issue in our future work

[2] In order to examine the effects of different levels of noise, we take simulation based experiments commonly accepted in the field of side-channel cryptanalysis.

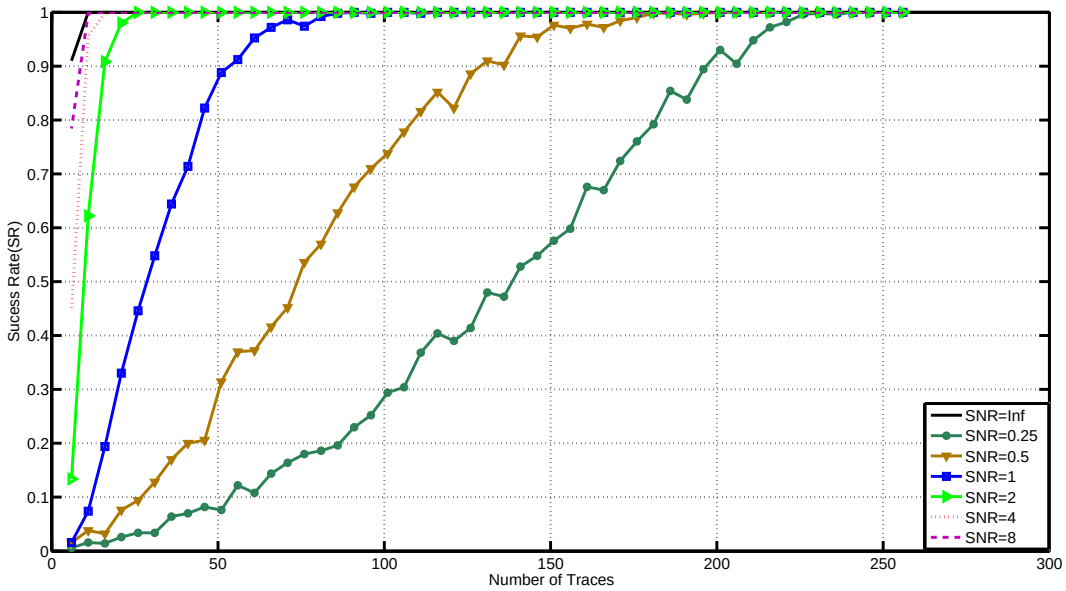


Fig. 5. CPA Attacks on Simulated Traces with Different Levels of Trend Noise

4 Advantages of LSM in Dealing with Trend Noise over Other Existing Noise Reduction Methods

In this section, we will examine the capabilities of LSM and other existing noise reduction methods in eliminating the trend noise from power traces, by performing a series of CPA attacks on four sets of real power traces published in the second stage of DPA Contest[3].

4.1 Experiment Settings

In order to compare the capabilities of LSM and other existing noise reduction methods [6][7][8]in dealing with trend noise, we design a group of CPA attacks on real power traces from group of sets DPA_contest2_public_base_diff_vcc_a128_2009_12_23. Note that each set of these power traces corresponds to the encryption of 20,000 random plaintexts under one secret key. Similarly, we also divide our CPA experiments into eight categories, the details of which are summarized in Table.2. **Note that, Wavelet in Table 2 refers to the noise reduction method in [6], Wavelet1 refers to that in [7], and PCA refers to that in [8]**.

4.2 Experiment Results and Analysis

The results of our eight groups of experiments on power traces of DPA contest v2 are shown in Fig.6 respectively. Specifically, our results are averaged over randomly chosen 16 sets of power traces out of the whole 32 sets of power traces contained in DPA_contest2_public_base_diff_vcc_a128_2009_12_23. Interestingly, it is shown in Fig.6 that the best experiments displayed is associated with a process of trend removal. Fig.6 shows that in this situation trend removal can increase success rate of CPA largely. Denote the number of power traces required to achieve a SR of 0.8 by CPA attack in an experiment setting **x** by **NT(x)**. For ease of understanding and for convenience, we will re-present the experiments' results in Table.4.2, using NT(x). It is clearly shown in Table.3 that, for any x in Wavelet+CPA, Wavelet1+CPA, PCA+CPA, NT(TR+x) to NT(x) ratio is always less than 1. This implies that existing noise reduction methods are not capable of completely eliminating the trend noise, and applications of non-generic noise reduction targeted certain noise of specific shape (i.e. trend noise in the paper) serves an effective way to enhance the performance of power analysis attacks. It also shows

[3] One could use another public sets of power traces, on his own, to repeat our experiments. For example, one may consider the use of power traces in DPA contest v3, if they were publicly available.

Table 2. Our CPA Attacks on Real Power Traces from DPA Contest v2

Experiment Label	Description of the Experiment
CPA	perform CPA attack on the original power traces
Wavelet+CPA	perform Wavelet transform in [6] to the original power traces, and then perform CPA attacks on the resultant power traces
Wavelet1+CPA	perform Wavelet transform in [7] to the original power traces, and then perform CPA attacks on the resultant power traces
PCA+CPA	perform PCA transform in [8] to the original power traces, and then perform CPA attacks on the resultant power traces
TR(quintic)+CPA	remove the trend in the original power traces using LSM with a quintic polynomial, and then perform CPA attacks on the resultant power traces
TR(quintic)+Wavelet+CPA	remove the trend in the original power traces using LSM with a quintic polynomial, perform Wavelet transform in [6] to the resultant power traces, and then perform CPA attacks on the final power traces
TR(quintic)+Wavelet1+CPA	remove the trend in the original power traces using LSM with a quintic polynomial, perform Wavelet transform in [7] to the resultant power traces, and then perform CPA attacks on the final power traces
TR(quintic)+PCA+CPA	remove the trend in the original power traces using LSM with a quintic polynomial, perform PCA transform in [8] to the resultant power traces, and then perform CPA attacks on the final power traces

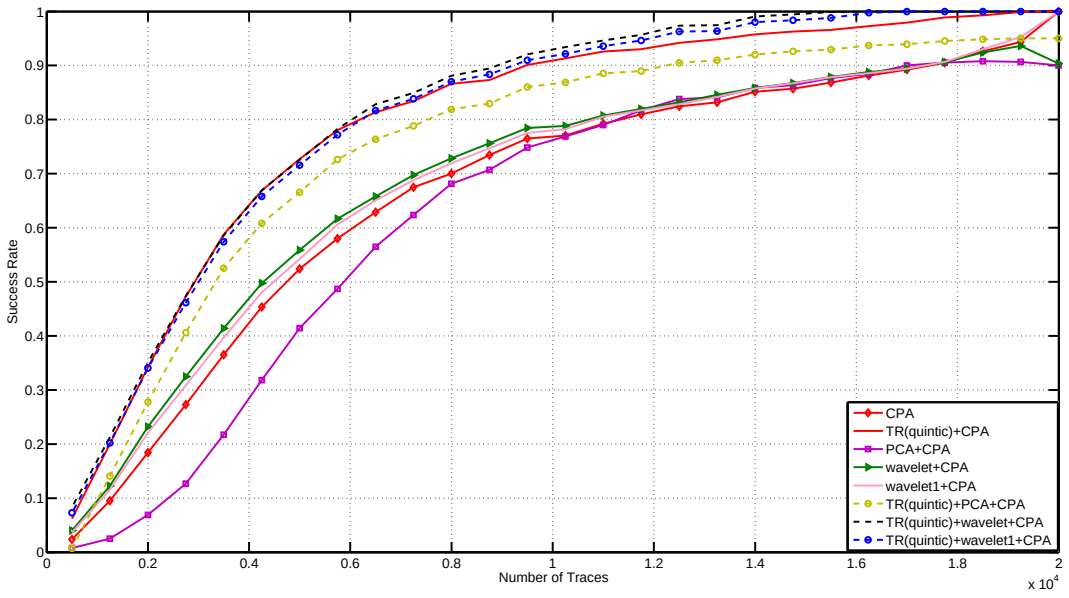


Fig. 6. CPA Attacks on Real Power Traces with Different De-noising Methods

Table 3. Relative Effectiveness of Noise Reductions in Terms of NT(x)

$\frac{NT(TR+Wavelet+CPA)}{NT(Wavelet+CPA)}$	$\frac{NT(TR+Wavelet1+CPA)}{NT(Wavelet1+CPA)}$	$\frac{NT(TR+PCA+CPA)}{NT(PCA+CPA)}$	$\frac{NT(TR+CPA)}{NT(CPA)}$
0.54	0.55	0.68	0.59

in Fig.6 that $NT(TR + PCA + CPA) < NT(CPA) < NT(PCA + CPA)$, we think the phenomena that $NT(CPA) < NT(PCA + CPA)$ coursed by PCA which is not under our consideration in this paper.

Note that in Fig.6, the curve for Wavelet+CPA , that for Wavelet1+CPA, and that for CPA are very close to each other. In this paper, we adopt wavelet transform using the "Symlet" family wavelet (which seems to be the best) on real power traces from an unprotected FPGA implementation of AES. In [6], the authors perform attacks on power traces from an unprotected implementation of DES on a smart card, and used the highest peak in differential power traces to assess the performance enhancement. In [9], the authors did NOT specify any parameters for wavelet transform being used. Considering all these facts, we purposely did NOT do any comparison of these three methods.

5 Conclusions and Future Work

The leakages of cryptographic module often contain a variety of noises. It has been turned out that the presence of these noises has considerable negative effects on side-channel attacks exploiting these leakages. Therefore, in practice, to reduce the noises included in side-channel leakages usually results in the performance enhancement of side-channel attacks. As far as noise reduction methods are concerned, most existing ones treat all different forms of noises as a , instead of dealing with each kind of them respectively. Contrary to existing methods, this paper examines the existence of noise of specific shape in side-channel leakages and its negative effects on the attacks. This kind of specific noise is called trend. Furthermore, we also explore the effectiveness of applying some trend removal methods.

We perform correlation power analysis attacks on a set of real power traces published in the second stage of DPA Contest, as a case of study. Our results show that there contains a considerable amount of trend noise in real power traces. The existence of trend in power traces has non-negligible negative effects on the performance of the attacks. For example, when SR of the CPA reaches 80%, the number of traces needed by CPA on traces with trend removal is only 55% of that on the same set of traces without trend removal. Additionally, in order to characterize the relationship between the level of trend noise and the performance of power analysis attack, we carry out a set of simulation experiments.

Another important observation in this paper is that most existing noise reduction methods that do not take the specific shape of noise into consideration have a limited capability in dealing with trend noise. For example, when the SR of CPA reaches 0.8, the number of power traces needed by CPA on traces with both trend removal and existing noise reduction(such as Wavelet and PCA) is about half of that on the same power traces with existing noise reduction only.

It could be deduced from the work of this paper that most existing noise reduction methods treat all different forms of noises as a whole, and they usually do not take the specific shape of noise into consideration. Therefore, there may be some room for further improving the performance of power analysis attacks, if other special noise reduction methods targeted noises of specific forms are taken. In a word, the work in this paper evidently show that to identify noise of specific shape in side-channel leakages from any other noises, and then to devise effective methods to reduce and/or eliminate this noise, is an important perspective on the study of side-channel cryptanalysis.

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. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. CRYPTO 1996, LNCS 1109, pp.104-113, 1996.
2. P.Kocher, J.Jaffe, B.Jun. Differential Power Analysis. CRYPTO 1999, LNCS 1666, pp.388-397,1999.
3. D.Agrawal, B.Archambeault, J.Rao, P.Rohatgi. The EM Side-Channel(s). CHES 2002, LNCS 2523, pp. 29-25,2002.

4. E.Brier, C.Clavier, F.Olivier. Correlation Power Analysis with a Leakage Model. CHES 2004, LNCS 3156, pp.135-152, 2004.
5. S.Mangard, E.Oswald, T.Popp. Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer-Verlag Press, 2007.
6. X.Charvet, H.Pelletier. Improving the DPA attack using Wavelet transform. Non-Invasive Attack Testing Workshop 2005. Available at `http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper14.pdf`.
7. Y.Souissi, M.Aabid, N.Debande, S.Guilley, J.Danger. Novel Applications of Wavelet Transforms based Side-Channel Analysis. Non-Invasive Attack Testing Workshop 2011. Available at `http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/01_Souissi.pdf`.
8. L.Batina, J.Hogenboom, J.Woudenberg. Getting More from PCA: First Results of Using Principal Component Analysis for Extensive Power Analysis. CT-RSA 2012, LNCS 7178, pp. 383-397,2012.
9. F.Standaert, T.Malkin, M. Yung. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks.EUROCRYPTO 2009, LNCS 5479, pp.443-461,2009.
10. S.Mangard, E.Oswald, F.Standaert. One for all-all for one: unifying standard differential power analysis attacks. Information Security, Vol.5, No.2, pp.100-110, 2011.
11. K.Hung Chan, J.Hayya, J.Ord. A Note on Trend Removal Methods: The Case of Polynomial Regression versus Variate Differencing. Econometrica, Vol.45, No.3, pp.737-744, 1977.
12. J.Denholm-Price, J.Rees. A Practical Example of Low-Frequency Trend Removal. Boundary-Layer Meteorolog, Vol.86, No.1, pp.181-187, 1998.
13. J.Bendat, A.Piersol. Random Data: Analysis and Measurement Procedures. Addision-Wiley Press, 2011.
14. M.Luaces, V.Luaces, M.Ohanian. Trend-removal in corrosion processes using neural networks. WSEAS 2006. AIKED'06 Proceedings of the 5th WSEAS International Conference on Artificial Intelligence, Knowledge Engineering and Data Bases. WSEAS Stevens Point, 2006.