EFFICIENT SOLUTION FOR MISALIGNMENT OF SIGNAL IN SIDE CHANNEL ANALYSIS

Thanh-Ha Le, Jessy Clédière

LETI, CEA, Grenoble, France

Christine Servière, Jean-Louis Lacoume

LIS, INPG, Grenoble, France

ABSTRACT

Side channel analysis like Differential Power Analysis (DPA) has been known as an efficient attack for uncovering secret data of cryptosystems. However, the temporal misalignment of side channel signals is an issue of concern that destabilizes side channel attack efficiency. In this paper, we propose a new method to surmount the misalignment problem in DPA. The performance of the proposed method is then evaluated while analyzing the electromagnetic signals of a synthesized ASIC (Application Specific Integrated Circuit) during a DES (Data Encryption Standard) operation. The experimental results show that our method allows to detect efficiently the secret key with a small number of side channel signals during a short time. Its performance is then compared to that of the original DPA and of the frequency-based DPA, the current solution for the signal misalignment in side channel attacks.

Index Terms— Electromagnetic Analysis, Security, Application Specific Integrated Circuit, Smart Cards, Synchronization.

1. INTRODUCTION

Side channel analysis is any attack based on information such as timing of cryptographic operations, power consumption or electromagnetic emanations gained from the physical implementation of a cryptosystem. The well-known side channel attacks based on power consumption are Simple Power Analysis (SPA) [1], Differential Power Analysis (DPA) [2] and Correlation Power Analysis (CPA) [3]. Electromagnetic signals acquired by dedicated sensors have been also employed as a side channel information for Simple ElectroMagnetic Analysis and Differential ElectroMagnetic Analysis [4, 5].

When performing a side channel attack, the Gaussian noise presented in side channel signals and the temporal misalignment of signals are two issues that can decline the attack efficiency. While the Gaussian noise is mainly generated from the electronic components in cryptographic devices, the signal misalignment is in general unintentionally caused by measurements. However, the latter can be also voluntary added by chip developers to disturb side channel attacks. Although the misalignment of signals is an usual problem while performing side channel attacks, no efficient solution has been proposed until the paper of Gebotys [6]. This work analyzed DEMA attack using signals in the frequency domain to enhance the DPA attack performance. Nevertheless, the Fourier transform requires a complex computation and so the attack duration is quite long. In this paper, we propose an efficient method based on the energy of original signals to solve the misalignment problem among side channel signals. The paper is structured as follows: we start with a background about the existing DPA concepts in Section 2. Our proposed energy-based DPA is focused in Section 3. The performance evaluation of our method compared with the original DPA and the frequency-based DPA are shown in Section 4 followed by conclusions in Section 5.

2. BACKGROUND

In this section, we give a brief overview of DPA concepts. For the sake of simplicity, hereafter, the term DPA is used for both power consumption and electromagnetic analysis. DPA is based on the fact that the power dissipation to manipulate one bit to 1 is different from the power dissipation to manipulate it to 0. To test different keys K_s, DPA uses N cipher/plain texts C_i $(i = 1 \dots N)$ and a selection function $D(C_i, b, K_s)$ which predicts the value of an examined bit b [2]. DPA computes a differential trace $\Delta_D(b)$ as the difference between the average of the traces for which $D(C_i, b, K_s)$ is 1 and the average of the traces for which $D(C_i, b, K_s)$ is 0. Therefore, for the correct key K_s, $\Delta_D(b) \neq 0$ at the instant τ where the bit b is handled. It is then represented by a peak in the differential trace at the instant τ, which is called as *DPA peak*. For incorrect keys, $\Delta_D(b)$ tends to 0 and no significant peak appears. One should note that the DPA peak only clearly appears if the bit b is handled at the same instant τ for all text messages. If the instant τ is not aligned, the magnitude of the DPA peak can be strongly reduced and the attack must be disturbed. In order to enhance the mono-bit DPA, some authors have introduced multi-bit DPA attacks which means that multiple bits are examined instead of only one bit, for example the methods of Messerges [7] and Bevan [8]. The generalized multi-bit DPA has been proposed in [9] and called as Partitioning Power Analysis (PPA).

The time and frequency domains are alternative ways to represent a signal. If a signal is modified in one domain, such modification obviously reserves in other domain, but usually not in the same way. In literature, many researches have studied side channel attacks in the time domain and different techniques have been applied to improve the attack performance. Whereas few research efforts have addressed these attacks in frequency domain. The work of Gebotys [6] is the first one which has examined side channel signals in frequency domain and exploited the following property: a shift of s samples in time domain leaves the magnitude unchanged but adds a linear term to the phase, $2\pi sf$. Two methods have been proposed: *Differential Frequency Analysis* and *Differential Spectrogram Analysis*. The results show that both methods were successful in obtaining the correct key from the PDA device, which is impossible with the original DEMA method in the time domain.

3. OUR PROPOSITION

3.1. Energy-based DPA

The temporal misalignment of side channel signals is originated by different sources depending on embedded system characteristics. The first one is due to the device's architecture, for example the Java architecture of the PDA in [6]. The trigger system to the oscilloscope and noise during measurements are also major causes. The temporal misalignment among side channel signals can be illustrated in Fig. 1. Consider three signals s_1, s_2, s_3 which are not well aligned and suppose that the useful information for DPA is contained in the maximal value (the top of peak) of each signal. We observe clearly that this information of s_1, s_2, s_3 is dispersed in three distinct peaks in the mean curve and by consequence the attack performance can be dramatically reduced.

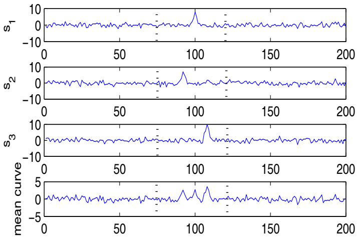

Fig. 1. Misaligned signals

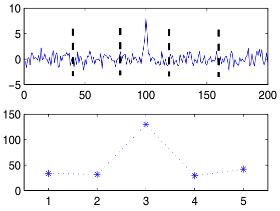

Fig. 2. Original and energy signals

Although the peak is shifted in different positions, it is still limited in a zone (segment bounded by dotted lines in Fig. 1). As a result, the energy of these segments is almost identical and it does not depend on the peak position. This important remark leads us to a "resistant-misalignment" DPA method based on the energy of original signals. Our proposition consists of dividing the original signal in segments of the same length and computing the energy of each signal segment. The samples of each segment will be replaced by its energy to form the energy signal as illustrated in Fig. 2 and summarized in the following algorithm.

```
S = original signal, m = length(S), L = length of segments,
EBS = EnergyBasedSignal(S)
for i  from 1 to m/L
    beginSegment=((i-1)*L+1), endSegment = i*L,
    segment(i)= S(beginSegment:endSegment),
    EBS(i)=<segment.segment>
end
return EBS
```

We then use these energy signals instead of the original ones to compute the DPA signals. Hence, if the instants τ where the considered bit is handled locate at the same segment, the useful information for DPA is always converged in the mean signal. It is obvious that this condition is much less strict than the previous condition where the instants τ must be coincide. Furthermore, energy signals always conserve the difference of power when manipulating one bit to 1 and manipulating this bit to 0. Therefore, the differential attack using energy signals allows to detect the correct key with misaligned side channel signals.

3.2. Attack-efficient metric

In order to evaluate the success of an attack, we define two attack-efficient indexes reflecting the key detection possibility. The first index, noted by i_1, is defined as the ratio between the DPA peak corresponding to the correct key and the highest DPA peak resulted from incorrect keys. These peaks are observed at the same time location τ when the data are handled. If this index is greater than 1, the expected peak is highest one and the key detection is reliable. In contrast, if this index is smaller than 1, there exists another peak higher than the expected peak. So the key detection method is not effective. The second index, noted by i_2, is defined as the signal to noise ratio of the DPA signal corresponding to the correct key. The DPA peak is considered as *signal* and the rest is *noise*. If i_2 is not sufficiently large, the expected peak is covered by noise and may be not observed, i.e. the key detection is impossible.

4. EXPERIMENTAL RESULTS

4.1. Experiment description

In our experiment, we measure the electromagnetic emanations of a synthesized ASIC during a DES operation. Corresponding to each random message used in input, we acquire an electromagnetic signal. An example of electromagnetic signal is depicted by the upper curve in Fig. 3 where we can observe 16 peaks corresponding to 16 rounds of DES. The energy signal calculated from the electromagnetic signal using segments of 100 samples is represented in the lower curve. One may note that the length of the energy signal is 100 times smaller than that of the original signal but it still conserves the form and main information of the electromagnetic signal.

As stated before, the temporal misalignment is a real challenge for side channel analysis. From 3000 measured electromagnetic signals, a histogram reflecting the temporal misalignment of these signals is illustrated in Fig. 4. It represents the position distribution of a peak in side channel signals. We

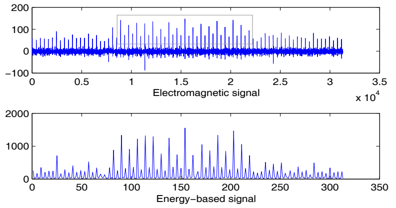

Fig. 3. EM and energy signal

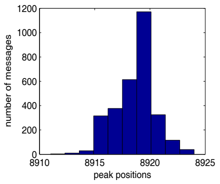

Fig. 4. Peak position distribution

see that the position of this peak spreads in about 15 values, it means that the electromagnetic signals are badly aligned.

4.2. Results and comparisons

In our experiment, 3000 electromagnetic signals were acquired to evaluate the performance of different methods. The useful information for DPA of these signals is mainly contained in the peaks. Hence, the electromagnetic signals can be manually realigned by forcing the maximum value of each peak at a same position. Note however that if the useful information is randomly distributed, the realignment becomes much more difficult. The frequency and energy signals have been computed by dividing electromagnetic signals in segments of 100 samples. For the frequency-based method, the Differential Spectrogram Analysis technique has been applied.

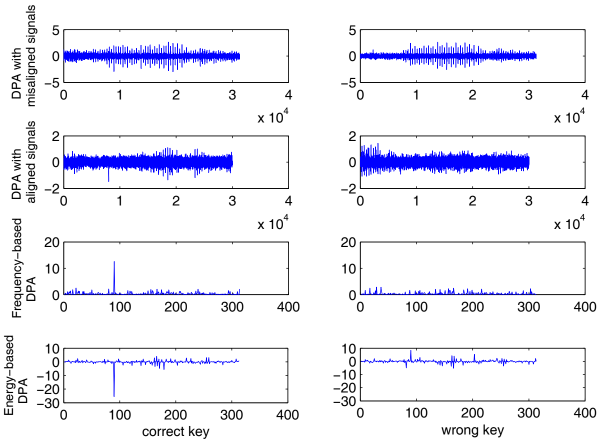

Fig. 5. DPA signals computed from 3000 EM signals

In order to have an idea about DPA signals of the tested methods, we plot in Fig. 5 the DPA signals corresponding to the correct key (left column) and to a wrong key (right column). The DPA signals, the realigned DPA signals, the frequency-based DPA signals and the energy-based DPA signals are presented from top to down. We can easily realize that the DPA method with raw electromagnetic signals performs badly. In fact, the DPA peak is not appeared in the DPA curve corresponding to the correct key and many unexpected peaks raise due to the misalignment. Furthermore, there is no difference between the correct key DPA signal and a wrong key DPA signal (two curves on the top). Therefore, the DPA method with non-aligned electromagnetic signals does not allows to detect the correct key even when 3000 side channel signals are used. When employing the manually realigned signals for DPA computation, the key detection has been slightly improved, i.e. the DPA peak appears in the correct key DPA signal. However, a high noise level still presents in DPA signals and it can cover the DPA peak when the number of side channel signals is reduced. Meanwhile, the frequency-based and energy-based DPA methods perform well and uncover easily the secret key. The DPA peak is highly raised in the DPA signals obtained from these methods.

The performance of tested methods can be estimated by evaluating their indexes i_1 and i_2. The Fig. 6 and 7 represent the variation of i_1 and i_2 according to the number of side channel signals. The key detection is feasible if $i_1 > 1$ and $i_2 > 5$. The first condition is explained in Section 3.2 and the second one is chosen through our experiment results.

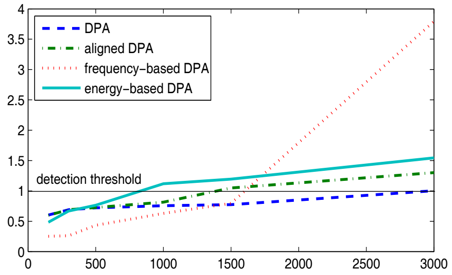

Fig. 6. i_1 evaluation

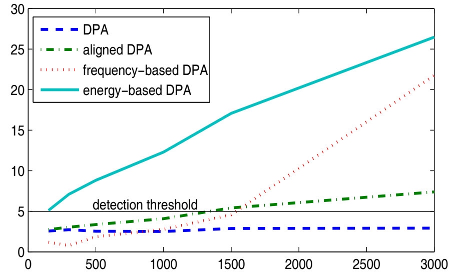

Fig. 7. i_2 evaluation

According to these figures, the performance of the DPA using realigned signals is slightly improved. When we have a large number of side channel signals, for example $N = 3000$, both indexes i_1a and i_2 of the frequency-based method are high, it means that this method is powerful. However when this number is small, these indexes decrease rapidly. On the other hand, the proposed energy-based DPA gives a regular augmentation for i_1 when the number of side channel signals varies from 150 to 3000 and very good values for i_2. If we take into account both indexes, the DPA with raw signals does not allow to find out the correct key. The DPA with realigned signals and the frequency-based method need about 1500 electromagnetic signals while the energy-based method need only 800 electromagnetic. This result can be confirmed by observing the DPA signals of two methods obtained from 800 electromagnetic signals in Fig. 8. The DPA peak corresponding to the energy-based method is clearly raised while the one of frequency-based method is covered by other peaks.

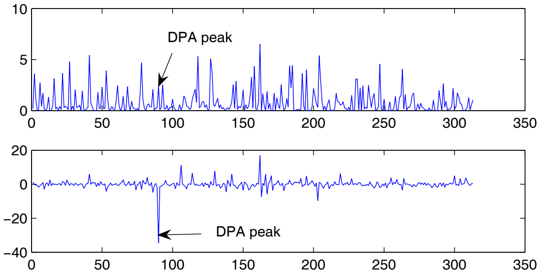

Fig. 8. Frequency-based DPA and Energy-based DPA signals obtained from 800 electromagnetic signals

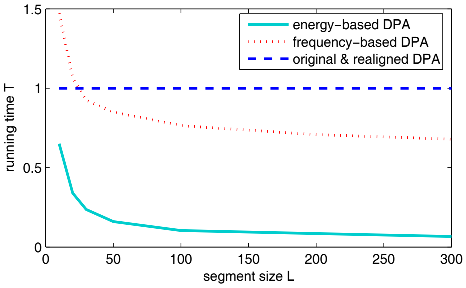

Fig. 9. Running time evaluation

The running time of each method obtained from our experiment is depicted in Figure 9. The number of key hypothesis is $K = 64$, the signal length m is fixed and the number of side channel signals is $N = 1000$. Therefore, the running time of the original and realigned DPA is fixed. Note that we present in this figure the relative running time and consider the duration of the original DPA as a reference. The first remark obtained from Fig. 9 is the running times of the frequency-based and energy-based methods decrease when the segment size L increases. In fact, the size of energy signals and frequency signals is L times smaller than that of the original ones. Therefore, the DPA computation times of these methods are inversely proportional to L. Secondly, the energy-based method is much faster than the others because the energy based method does not require an intense computation such as the FFT one.

5. CONCLUSIONS

In this paper, we have proposed a novel method to surmount the signal misalignment in side channel analysis. Our energy-based method is practical and allows to efficiently detect the secret key with a small number of side channel signals during a short duration. The proposed method has been compared with the original DPA and the frequency-based DPA. Our experiment with electromagnetic signals acquired during a DES operation also validates the performance of frequency-based method, which was originally tested with a device running Rijindel and ECC. The energy-based DPA can be applied in multi-bit DPA and tested in devices running other cryptographic algorithms.

6. REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," 1998, White Paper, Cryptography Research.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *In proceedings of CRYPTO 1999*. 1999, LNCS 1666, Springer Verlag.

[3] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *In Proc. of CHES 2004*. 2004, LNCS 3156, Springer Verlag.

[4] K. Gandolfi, C.Mourtel, and F.Olivier, "Electromagnetic Attacks: Concrete Results," in *In proceedings of CHES 2001*.

[5] J.J. Quisquater and D. Samyde, "Electromagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards," in *In proceedings of e-Smart 2001*.

[6] C. Gebotys, S. Ho, and A. Tiu, "EM analysis on Rijindael and ECC on a PDA," in *In Proc. of CHES*, UK, Sept 2005.

[7] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," May 2002, vol. 51, pp. 541–552.

[8] R. Bevan and E. Knudsen, "Ways to Enhance DPA," in *In Proc. of ICISC 2002*. 2002, Springer Verlag.

[9] T-H. Le, J. Clédière, C Canovas, C. Servière, J-L. Lacoume, and B. Robisson, "A proposition for correlation power analysis enhancement," in *In Proc. of CHES*, Japan, Oct 2006.