PROCEEDINGS OF SCIENCE

Construction of a High Efficient Distinguisher in Differential Power Analysis Attacks

Ying Guo[1]
College of Computer Science and Technology, Hengyang Normal University
HengYang, 421002, China
E-mail: 1352520550@qq.com

Yu Ou[2a]**; Lang Li**[3b]
College of Computer Science and Technology, Hengyang Normal University
HengYang, 421002, China
E-mail: [a]blink_zip@foxmail.com; [b]lilang911@126.com

In differential power analysis attacks (DPA), the distinguisher directly influences the effects Previous research has mainly focused on analyzing how one or more bits of the intermediate value influence the actual power consumption. However, limited study has been conducted on constructing a more effective distinguisher. In this paper, by comparing the effects of several selected distinguishers we have analyzed the structure of the distinguisher with correlation analysis. Then, we have proposed a high efficient distinguisher, named HDF and conducted experiments through AES. HDF has been employed to operate differential power analysis attacks on AES. The results have verified the validity and high efficiency of this distinguisher, HDF.

ISCC 2017
16-17 December 2017
Guangzhou, China

[1]Lang Li(1971-), Ph.D., his research interests include the information security.

[2]This research is supported by the National Natural Science Foundation of China under Grant No.:61572174, National Undergraduate Training Program for Innovation and Entrepreneurship with Grant No.:201710546007, Hunan Provincial Experiment Programs of Learning and Innovation for Undergraduates of China with Grant No.:2017526, the Scientific Research Fund of Hunan Provincial Education Department with Grant No.: 15A029, the Scientific Research fund of Hengyang Normal University with Grant No.: 16CXYZ01, the Science and Technology Plan Project of Hunan Province No.: 2016TP1020, Hunan Provincial Natural Science Foundation of China with Grant No.: 2017JJ4001.

[3]Corresponding Author: Lang Li, email:lilang911@126.com

PoS(ISCC 2017)049

1.Introduction

With the development of encryption technology, embedded cryptographic devices have been applied to all aspects of our society, but the challenges to their security have been brought with more and more attention. In order to enhance the security of those devices, scholars have analyzed the information leakage of device operation with traditional mathematical methods and developed a variety of new cryptographic analysis techniques, such as Timing Analysis (TA)[1], Simple Power Analysis (SPA)[2], Differential Power Analysis (DPA)[3], Correlation Power Analysis (CPA)[4] and Algebraic Side-channel Analysis (ASCA)[5], etc. DPA is widely used because of its low requirement of attack equipment and its easiness to be analyzed and to run attacks. However, DPA usually employs the intermediate variable of one or several bits of the sampling results to construct a distinguisher. For example, Chu and his colleagues [6] have taken the intermediate value of the first bit as a distinguisher, or Chen [7] has compared the effects of different bits of the attack. But the study of how to construct a higher efficient distinguisher is relatively limited. In this paper, we have studied the principle of DPA with correlation analysis, and compared the effects of first bit distinguisher, zero value distinguisher and multi bit distinguisher. We proposed a higher efficient distinguisher[8].

2. Constructing A High Efficient Distinguisher

DPA uses mean difference method or correlation coefficient method to test the correlation between the intermediate and the actual power consumption, on the basis of which we propose a high efficient distinguisher, and we will describe it in details at below.

The random variable X is defined as the intermediate value. The random variable Y is defined as the actual value. Considering the characteristics of the attack point, we choose the better effect of Hamming weight model [9] and $X = HW(V)$. If the j-th sub key is a correct result, then the j-th column of X must be correlated with Y, which is shown as below:

$$P(X,Y) = \frac{\mathrm{cov}(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}} \tag{2.1}$$

Then, their correlation coefficient is:

$$\gamma = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2}\sqrt{\sum (y_i - \bar{y})^2}} \quad (1 \le i \le N) \tag{2.2}$$

In the formula, if γ=a and |a|>0. There is a linear correlation between X and Y. We used $\overline{X}$ to divide X and Y into two parts:

$$X_0 = \{x_{0i} | x_i < \bar{x}\}$$

$$X_1 = \{x_{1i} | x_i < \bar{x}\}$$

And:

$$Y_0 = \{y_{0i} | x_i < \bar{x}\}$$

$$Y_1 = \{y_{1i} | x_i < \bar{x}\}$$

The same linear relationship exists between Y_0 and X_0, Y_1 and X_1. Let $\overline{y_0}$ and $\overline{y_1}$ be the mean value of Y_0 and Y_1, $\overline{x_0}$ and $\overline{x_1}$ be the mean value of X_0 and X_1.

Then

$$\overline{y_0}=k\,\overline{x_0}+b$$

$$\overline{y_1}=k\,\overline{x_1}+b$$

So $|\overline{y_1}-\overline{y_0}|=k|\overline{x_1}-\overline{x_0}|$, because $x_{1i}>\overline{x}$ and $x_{0i}<\overline{x}$, $\overline{x_1}>\overline{x}$, $\overline{x_0}<\overline{x}$, $|\overline{y_1}-\overline{y_0}|>0$.

If r=0, X and Y are relatively independent, Y_0 and Y_1 are random distributions variables. So when i tends to infinity, the $|\overline{y_1}-\overline{y_0}|=0$. We design the HDF distinguisher based on the correlation between intermediate value and actual power consumption.

When we take the mean difference method, it requires a distinguisher to divide the large and the small values of actual power consumption into two parts. Then, the mean difference values are calculated. At the same time, we observe the peak values to guess the key. To better separate the large and the small values of the actual power consumption, we define the actual power consumption as T, and N is the number of plaintexts. The i-th plaintext of actual power consumption is T_i, and the mean value is $\overline{T}$:

$$T_0=\{T_i|T_i<\overline{T}\} \tag{2.3}$$

$$A_0=\frac{\sum T_0}{|T_0|}\quad,\quad A_1=\frac{\sum T_1}{|T_1|} \tag{2.4}$$

Where $|T_0|$ represents the number of elements in T_0 and $|T_1|$ is the number of elements in T_1. Through this method, mean difference calculation is relatively processed well.

We assume that the distinguisher is based on the mean value of power consumption. We use Hamming weight method to obtain the j-th of intermediate values as V_{ij} $(1\leqslant i\leqslant N, 0\leqslant j\leqslant 255)$, then P(V)=HW(V). The j-th of the mean value is defined as:

$$\overline{P_j}=\frac{\sum_{i=1}^{N}P_{ij}}{N}$$

Then the distinguisher D is:

$$D=\begin{cases}0 & P_{ij}<\overline{P_j}\\ 1 & P_{ij}\geq\overline{P_j}\end{cases} \tag{2.5}$$

The actual consumption is divided into two parts:

$$S_0=\{T_i|D=0\}\quad,\quad S_1=\{T_i|D=1\}$$

$$A_{0j}=\frac{\sum_{j=0}^{255}S_{0j}}{|S_{0j}|}\quad,\quad A_{1j}=\frac{\sum_{j=0}^{255}S_{1j}}{|S_{1j}|} \tag{2.6}$$

The difference value is: $\Delta_j=A_{1j}-A_{0j}(0\leqslant j\leqslant 255)$.

The distinguisher represented by formula (2.3), (2.4) and (2.5) is defined as HDF. According to literature [10], [11] and [12], we use HDF to calculate the success ratio of differential power analysis attacks as:

$$\overline{SR} = \frac{\sum_{k_C \in \kappa} SR_{k_C}}{|k|}$$

The actual success ratio is usually calculated by dividing the number of successful attacks by the total number of attacks. According to latter DPA experiments in the following, we have proved that using HDF can effectively reduce the number of random plaintext and improve the efficiency of the attack.

3.Experimental Results and Analysis

In this section, we take AES as an example. Firstly, we carry out the hardware implementation of it. Then we design a software simulation platform which simulates the operation process of AES. This platform can generate random plaintexts and automatically run differential power analysis attacks.

3.1 Hardware Implementation of AES

We have implemented AES in Verilog-HDL and used iverilog+GTKWave for simulation. The result is shown in Figure 1. The plaintext, key and ciphertext are displayed in hexadecimal form as showed in Table1.

Plaintext: 3243F6A8885A308D313198A2E0370734

Key:2B7E151628AED2A6ABF7158809CF4F3C

Ciphertext: 3925841D02DC09FBDC118597196A0B32

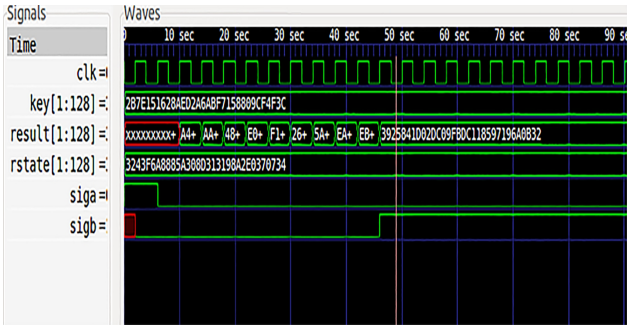

Figure 1 : Hardware Implementation of AES

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

Table 1: Key of AES in Hexadecimal Form

3.2 Attack Results and Analysis

We have conducted three experiments to compare the effects of different distinguishers in DPA to verify the high efficiency of the HDF distinguisher.

In experiment 1, we take the Maximum bit discrimination as distinguisher. At least 5000 plaintexts are required to crack the key accurately. DPA wave form is shown in Fig. 2. The position of the graduation value 43 appears at the peak, and coincidentally the first byte of the key 2B decimal is 43, which proves that the key is successfully cracked. We also found the peak of Fig. 2 is not very obvious. When the number of plaintext increases to 20000, the peak value gradually becomes clearer. Other than the peak position, the values at other locations tend to be stable, and the success ratio of attack is close to 100% (see Fig. 3).

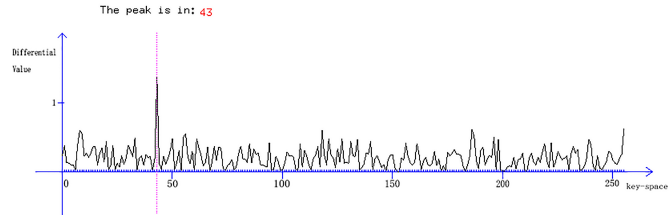

Figure 2 : The DPA Wave Form of the Maximum Bit Discrimination (5000 Plaintexts)

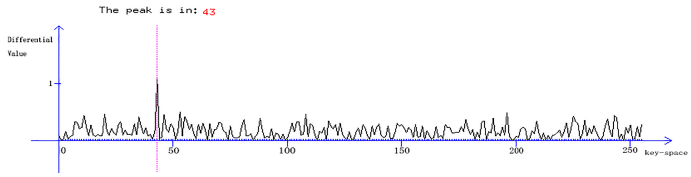

Figure 3 : The DPA Wave Form of the Maximum Bit Discrimination (20000 Plaintexts)

In Experiment 2, we take the Zero discrimination as distinguisher. This method requires a very large number of plaintexts where the peak is not obvious, so errors are relatively easy to appear in experimental results (see Fig. 4).

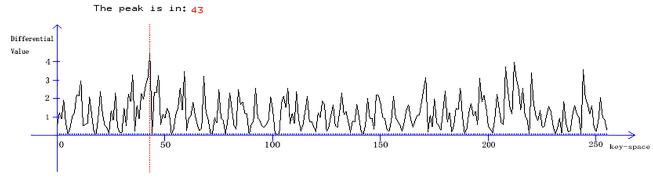

Figure 4 : The DPA Wave Form of the Zero Discrimination

In experiment 3, we present the HDF distinguisher. Altogether 3000 plaintexts and 500 plaintexts have been used. The Fig. 5 and Fig. 6 show the DPA wave forms of 3000 plaintexts and 500 plaintexts, respectively.

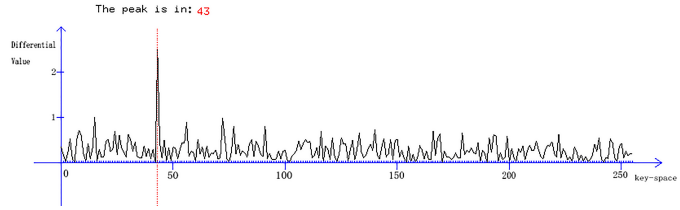

Figure 5 : The DPA Wave Form of the HDF Distinguisher(3000 Plaintexts)

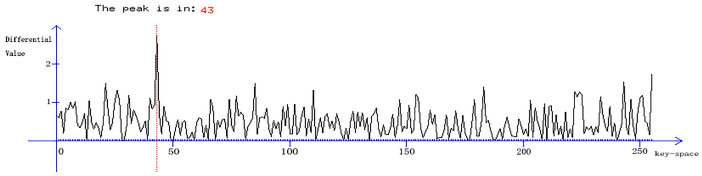

Figure 6 : The DPA Wave Form of the HDF Distinguisher (500 Plaintexts)

A comparison between Fig. 5 and Fig. 6 has been analyzed. When the experiment uses 3000 plaintexts, the peak is very obvious, and the success ratio of attack is close to 100%. When the experiment uses 500 plaintexts, we can also attack the key correctly. Thus, in respect to the effect and the success ratio of attack, using 500 plaintexts reaches a similar result as using 5000 plaintexts shown in experiment 1. Nevertheless, the number of plaintext for DPA has been dramatically reduced when we use the HDF distinguisher. Thus, we can improve the efficiency of DPA by reducing the amount of computation. Also, when the value equals to 4, the distinguisher achieves the same effect. What's more, when we conduct the experiment with sixteen bytes of AES, the HDF distinguisher is able to effectively attack the key.

4. Conclusions

DPA is a very efficient key decryption attack, whose operation is simple and easy to be implemented. For attackers, complicated mathematical computations are not necessary. They can quickly attack the cryptographic equipment without destroying it. The key point of using DPA is to construct a feasible distinguisher, because different distinguishers have different influences on the effects of the DPA. In this paper, we propose a high efficient HDF as the distinguisher. We have shown a comparison between the attack effects of using HDF distinguisher and other distinguishers. The HDF distinguisher reduces the number of plaintext for DPA, which improves the efficiency of DPA by reducing the amount of computation.

References

[1] Ge Q, Yarom Y, Cock D, et al. *A survey of microarchitectural timing attacks and countermeasures on contemporary hardware*[J]. Journal of Cryptographic Engineering, 2016:1-27.

[2] Fabšič T, Gallo O, Hromada V. *Simple Power Analysis Attack on the QC-LDPC McEliece Cryptosystem*[J]. Tatra Mountains Mathematical Publications, 2017, 67(1):85-92.

[3] Kocher P C, Jaffe J M, Jun B C. *Differential power analysis—resistant cryptographic processing*: US, US 8879724 B2[P]. 2014.

[4] Dofe J, Pahlevanzadeh H, Yu Q. *A Comprehensive FPGA-Based Assessment on Fault-Resistant AES against Correlation Power Analysis Attack*[J]. Journal of Electronic Testing, 2016, 32(5):611-624.

[5] Oren Y, Renauld M, Standaert F, et al. *Algebraic side-channel attacks beyond the hamming weight leakage model* [C]. International Conference on Cryptographic Hardware and Embedded Systems. Springer-Verlag, 2012: 140-154.

[6] Chu J, Ding G L, Deng G M, et al. *Design and Realization of Differential Power Analysis for DES*[J]. Journal of Chinese Computer Systems, 2007, 28(11):2070-2073.(in Chinese)

[7] Yu H, Chen K, Zou C, et al. *Creation of Function D and Effect Analysis in DES Differential Power Analysis Attacks*[J]. Computer Measurement & Control, 2012. (in Chinese)

[8] Malkin T G, Yung M. *A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks*[C]. International Conference on Advances in Cryptology: the Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2009:443-461.

[9] Luo P, Feng D G, Zhou Y B. *Power model in power analysis attack*[J]. Journal on Communications,2012, 33 (Z1):276-281 (in Chinese)

[10] Rivain M. *On the Exact Success Rate of Side Channel Analysis in the Gaussian Model*[C].Selected Areas in Cryptography, International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers. DBLP, 2009:165-183.

[11] Fei Y, Luo Q, Ding A A. *A Statistical Model for DPA with Novel Algorithmic Confusion Analysis*[C]. International Conference on Cryptographic Hardware and Embedded Systems. Springer-Verlag, 2012:233-250.

[12] Thillard A, Prouff E, Roche T. *Success through Confidence: Evaluating the Effectiveness of a Side-Channel Attack*[C].International Conference on Cryptographic Hardware and Embedded Systems. Springer-Verlag, 2013: 21-36.