Improved DPA Attack Method on AES Encryption

S. Lan
Center for Integrated Circuits (IC)
School of Microelectronics
Shanghai Jiao Tong University
China

***Abstract*—Side-channel attack, which is a new technology in the field of cryptography, focus on the power-leak produced by password equipment,such as energyy, time, radiation.DPA (differential power analysis)attack as a method of sidechannel attack, its main method is comparing the peak of curve to determine the key is correct or not. According to the characteristics of AES-128 encryption, this paper uses the method of immobilizing the plaintext data, improving the ratio of SNR, making the correlation close to the high value of 1.Finally finish the DPA attack by the new method, provides researchers useful reference.**

Keywords-AES; side-channel; differential power analysis; correlation

I. INTRODUCTION

The development of information has made the security system become fragile. Traditional encryption used the encryption algorithm stored in devices to complete the encryption operation.Recovering the original key called attack. Traditional attacking methods mainly rely on the mathematical analysis and calculation, such as exhaustive literature attack [1]: used mathematical calculation to search and check all the possible key.As the length of key increasing, the difficulty of these attack method is out of control.In recent years, research on the development of side-channel attack offers many attack method,the most powerful method is differential power analysis(DPA) attack.

The main core idea of DPA attack is to judge on the peak phenomenon of attack curve[2].The traditonal attack curve is correlation curve,which is produced by comparing the energy consumption of assuming key with the actual energy consumption.Using energy simulation model,if the assuming key is right,the correlation between them will be high and correlation will be only.But as to AES realized by hardware devices,all the cryptographic operation are executing concurrently,if attacker choise one operation as attack point,the energy consumption of others will become noise interference,which will made the correlation low.Low correlation means the performance of attack is bad,more energy information will be need.This paper proposes another attack method to avoid the noise interference, provides a practical and beneficial reference for the researchers of AES encryption algorithm.

II. IMPROVED DPA ATTACK

Implementation of encryption algorithm mainly includes software and hardware, this new method is mainly aims at hardware encryption.

A. Weakness of DPA Attack On Hardware Encryption

Assuming an attack scenario, the energy consumption of operation, conversion noise, electronic noise and constant energy consumption are represented by P_{Ex}, P_{Sw}, P_{noise}, P_{const} ,the total power can be calculated as follow[3]:

$$P_{total} = P_{Ex} + P_{Sw} + P_{noise} + P_{const}$$

Power analysis mainly use the operand related energy P_{data} and operation related energy P_{op} , The definition of SNR during DPA attack is :

$$SNR = \frac{P_{exp}}{Var(P_{sw}+P_{noise})} \quad (1)$$

$$\rho(H,\ P_{total}) = \frac{\rho(H,\ P_{Ex})}{\sqrt{1+\frac{1}{SNR}}} \quad (2)$$

Most of the DPA attack choose S-box as the attack point[4].In the software encryption process, each S-box transformation are executed sequential-lly, which makes the correlation high and concentrated, But unlike software encryption process, hardware encryption basic on pure hardware structure, its structure determines in the running process of encryption devices, the encryption operation are with high concurrency. Figure 1 shows the wrong results of traditional DPA attack of hardware encryption. As can be seen from the figure, the high correlation coefficient is not only, the amulti-peak phenomenon means the attack effect is not ideal.

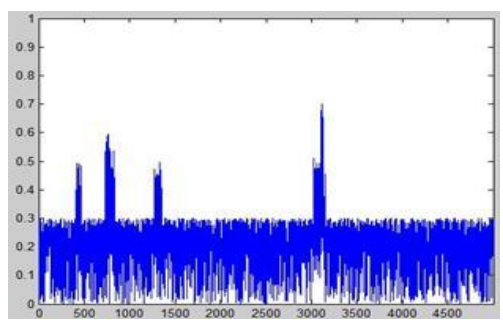

FIGURE I. WRONG ATTACK RESULT.

B. Improved DPA Attack Method

During the process of AES, The 16 S-boxes will finish the look-up operation, it makes the analysis of one S-box will be greatly influenced by the switching noise produced by the other S-boxes, and this noise is random.

It can be seen from the relationship between SNR and the correlation coefficient. Duing to poor SNR, the attack process

makes the correlation coefficient shows a very low tendency; greatly affect the derivation of the correct key.

AES consist of 10-rounds operation, the round-key is produced by the original key.The DPA attacker can recovery original key by recovering the round-key .Not only that, attacker has the condition of seting data, which made this method become possible. Therefore, to avoid the other S-boxes producing noise; attacker can use a fixed value instead of the original data as the input of the other S-boxes. So all the noise which has nothing to do with the attack point can be immobilized to a minimum value. This method can improve SNR greatly; reduce external noise influence during the S-box attack process. It is expressed as follows:

$$\mathrm{F}(S_i) = F\left(S_i, \sum_{k=1,k\neq i}^{16} F(S_k) = \mathrm{HW}(0)\right) \tag{3}$$

The improved DPA attack steps are as follow:

1) Get the data and energy trace.

2) Select the first round of AES to recovery the original key, select one of the 16 S-boxes as the attack point.

3) Determine the attack function F.Its input are 8-bit data and the hypotheses of round-key.

4) Produce new data, make sure the input of S-box attacked unchanged, and change the other bit to make the simulation model of HW to become minimum value, P_{Sw} is converted to P_{Const}.

5) Using simulation model to calculate the energy consumption produced by the assumption key, Recorded as matrix H.Doing the correlation calculation between matrix H and actual energy consumption matrix T, Recorded the result as matrix R, finally get the correct key assumptions from matrix R.

III. SIMULATION RESULTS

Using HW as simulation technology, this paper used the improved coefficient analysis method to attack the first S-box (S1) of AES. The entire 8 bit key is composed of 256 kinds of key. At the same time, based on the method of calculating the HW, making the input of the other S-box produced minmun HW value. The change of energy related to the S1 in maximum value, and power noise of the remaining 15 S-boxes are reduced. The high correlation can be getting, Showed that when input of S-box changes, the sensitivity of data exists and it is strong. While the input of the rest of the S-box does not change, the difference value does not have any effect. From figure 2 and figure 3, in the right key guessing, the highest correlation degree above 0.7, and the wrong key correlation are at about 0.3, curve peak is obvious in right key guessing. Doing the same attack on the S2~S16 and recovering the key finally.

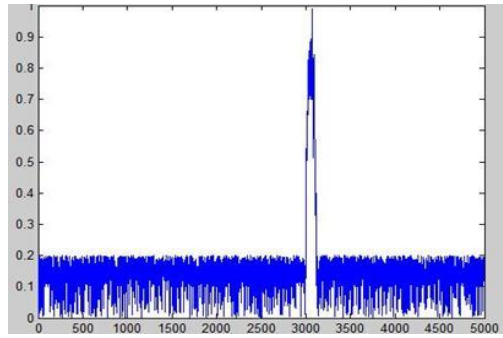

FIGURE II. RIGHT KEY GUESSING (KEY=180).

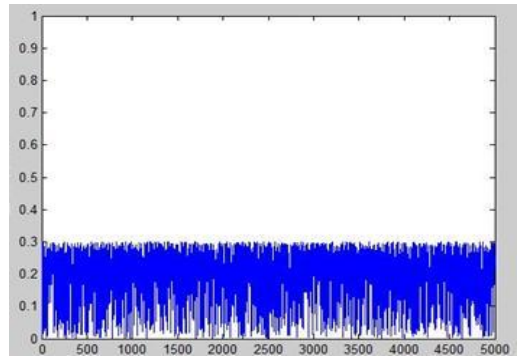

FIGURE III. WRONG KEY GUESSING (KEY=179).

IV. CONCLUSION

Through the calculation of the maximum correlation, DPA attack can get relationship between assuming key and the power consumption. The maximum correlation shows the most likely right assuming key. The traditional DPA attack is very effective for software encryption, but for the operation concurrency in hardware equipment, the DPA attack effect does not appear obvious, some time even wrong attack result. Aiming at the shortcomings of the traditional DPA attack on the hardware encryption equipment, this method improves the DPA attack from the input data, reduces the noise interference between S-boxes to a small range. By doing an actual attack at the intelligent card, the attack result showes that, the performance of this improved method is superior to the traditional analysis method. The attack result showes a single peak and high value phenomenon.

REFERENCE

[1] Johannes Blomer, Jorge Guajardo, and Volker Krummel. Provably Secure Masking of AES. In proceeding of Selected Areas in Cryptography: 11th International Workshop, SAC 2004, pp. 69-83, Springer 2005.

[2] Thomas S.messerge, EzzatA.Dabbish, Examining Smart-Card Security under the Threat of Power Analysis Attacks. IEEE. Transactions on Computers,Vol.51, 2002

[3] Andrey Bogdanov. Multiple-Differential Side-Channel Collision Attacks on AES. CHES 2008, LNCS 5154, PP.30-44, 2008.

[4] Hwasun Chang, Kwangjo Kim. Securing AES against Second-Order DPA by Simple Fixed-Value Masking, [A Thesis for the Degree of Master]. Korea: School of Engineering Information and Communications University, 2004