

Power Analysis Attack Based on FCM Clustering Algorithm

Gao Shen, Qiming Zhang, Yongkang Tang, Shaoqing Li and Ruonan Zhang

ABSTRACT

With the development of information technology over the world for decades, information security is called an important issue in today's society. As a hardware carrier for information security, cryptographic chips have become an important issue in academia. In this paper, we propose a power analysis attack based on FCM (Fuzzy C-Means) clustering algorithm. Our method clusters the energy traces according to their intrinsic similarity, and classifies the energy traces according to the Hamming distance energy model. The correct key is found by comparing the similarity between the clustering result and the classification result. In order to eliminate noises, ICA (Independent Component Analysis) is involved. The simulation experiment uses AES cipher algorithm as the attack object. HSPICE simulation is performed on the first round of 8-bit s-box circuit under 40nm process. Experimental results show that our method is effective.

1 INTRODUCTION

Today is an information society. The security of information has become an important issue. As key to the security of information systems, the cryptographic chip plays a central role in this field. Therefore, the research on the attack and protection methods of cryptographic chips is of great significance.

Side Channel Attack (SCA) is a non-intrusive attack technology. It extracts the physical information such as running time, electromagnetic radiation and energy consumption when the crypto chip is running normally. These kinds of physical information is related to the data processed by the cryptographic device and the operations performed, which called data dependency and operational dependency. So we can find the key of the crypto chip by analyzing relationship between the physical information, plaintext and cipher text. Mathematical and statistical methods is involved during this process.

Power analysis attack is a kind of SCA method since it uses power consumption of the device as side channel information. The energy consumption changes with time is called energy trace. Power analysis attack takes advantage of the fact that the instantaneous energy consumption of a cryptographic device depends on the data processed by the device and the operations performed by the device.

FCM clustering algorithm is a kind of machine learning method and is widely used in various fields such as image recognition and speech recognition. The
process of dividing a collection of physical or abstract objects into multiple classes of similar objects is called clustering. A cluster generated by clustering is a collection of objects. Objects in the same cluster are similar, and objects in different clusters are different.

In this paper, we propose a power analysis attack method based on FCM clustering algorithm. First, fuzzy clustering is performed on the energy traces according to their intrinsic similarity. Then, energy traces are classified according to the Hamming distance energy model under different key hypotheses. Next, we compare the clustering result with the similarity of the classification result under each key hypothesis. Finally, the key hypothesis corresponding to the maximum similarity is considered the attack result. The method is validated by simulation experiments.

2 RELATED WORK

In the field of SCA, academia has developed various attack methods for decades.

In 1996, American scientist Paul Kocher proposed a time analysis attack method[1]. This method performs attack by precisely measuring the encryption time of the cryptographic chip. Paul’s method successfully complete the key cracking of the Diffie-Hellman key exchange protocol and the RSA cryptographic algorithm. Paul Kocher's research pioneered the SCA. He provided a novel idea which is more efficient and accurate than traditional mathematical analysis.

In 1998, Paul Kocher studied the energy consumption of cryptographic devices when processing different instructions and data in the working process. He proposed an energy analysis attack method. The method analyses and cracks out the key by calculating the energy and key correlation of cryptographic devices [2]. Then Paul Kocher published a differential power analysis attack (DPA) in 1999 [3].

In 2000, Quisquater first proposed the concept of using electromagnetic radiation. He proposed two methods--simple electromagnetic analysis (SEMA) and differential electromagnetic analysis (DEMA) [4]. He believe that power consumption information is only one-dimensional in time series, while electromagnetic radiation information contains time and space so the information contained is more advantageous. At the same time, he also proposed some corresponding defense measures, including low-power design, parallel logic, Faraday cages and distributed parallel architecture.

In 2002, Suresh Chari [5] proposed a new attack method called template attack. This method controls a cryptographic device that is similar to or the same as the attacked device, and builds a template based on the device. The power consumption information generated when the attacked device is running is collected. The power consumption information is used to match the established template. If the matching is successful, the final crack key is considered to be the previous matching key.

In 2011, Hospodar [6-7] pointed out that template attacks are multi-classification problems, and some techniques in machine learning are just
good at dealing with classification problems. On this basis, the application of machine learning technology to power analysis attacks is proposed for the first time. He successfully implemented the AES attack using the least squares support vector machine (LS-SVM).

In 2012, Hera [8] successfully used the SVM algorithm to crack the complete key of the DES cryptographic algorithm loaded on the 8-bit smart card. This is the first time that the SVM algorithm was used to attack the complete key.

In 2013, Chou [9] proposed an unsupervised model for power analysis. Based on this model, the key used in the different rounds of encryption process was successfully obtained. The correct attack results were successfully obtained and the attack efficiency was improved. In addition to SVM, Martinasek [10-11] proposed a method of combining neural networks with energy analysis attacks. This method combines the advantages of SPA and DPA. And this method successfully cracks the first byte of AES.

3 OUR PROPOSED METHOD

The framework of our proposed method is shown as the figure 1.

The input of our proposed method is energy traces and the corresponding plaintext data. Firstly, attack point selection and denoising are performed on the energy traces. The processed energy traces will proceed to the next steps. On the one hand, the energy traces are clustered according to their intrinsic similarity and the cluster center is obtained. On the other hand, the energy traces are classified based on the simulated energy, and obtains the classification center. The simulated

Figure 1. The framework of our proposed method.
energy is obtained by Hamming distance energy model processing the plaintext and the guessed key. After all the keys have been guessed, the clustering center and the classification center under all key hypothesis are compared one by one. The key hypothesis corresponding to the classification center with the largest similarity is considered the correct key.

Next, the various steps of our method will be specifically explained.

3.1 Attack Point Selection

In a power analysis attack, there are often many sampling points per cycle, and some of them have little effect for attack. Instead, because of the presence of noise and sampling points’ introduction of too many unrelated factors, power analysis attack faces noise superposition. Noise superposition will weak the attack effect, increase the space complexity, and increase calculation time. Therefore, it is necessary to reduce the number of sampling points in the energy trace that participate in the power analysis attack.

The following will start with the logic blocking and delay characteristic of the gate circuit. Based on these two phenomena we explain how to select the appropriate attack points and energy traces in the cryptographic device for power analysis attack.

3.1.1 LOGIC BLOCKING

Logical blocking means that for the logic of each stage, its state flipping probability of each stage is gradually decreasing. The following is an example of NAND gate to illustrate the concept of logical blocking.

The state probability of the NAND gate can be shown in the figure 2. In (p0, p1), p0 represents the probability that the port state is "0", and p1 represents the probability that the port state is "1".

![Figure 2. State probability of the NAND gate.](image)

For the two-input NAND gate, when the state probability of the input port A, B is (1/2, 1/2), the state probability of the output port C is (1/4, 3/4). The C port will be 0 only if A=B=1. The probability of the C port flipping is 2*1/4*3/4=3/8.

The main cause of logic blocking in CMOS circuits are NAND gates and NOR gates. For the NOR gates, the same logic can be used to derive the logic blocking state. Due to the presence of logic blocking in the circuit, changes in the input signal do not always cause changes in the output.

So for the actual circuit, the change in the input signal does not cause all the gates to flip. When data enters the combinational logic circuit from the register, the
data passes through the gates one after another until the next set of registers. The state flipping probability is gradually decremented one level by one level.

3.1.2 DELAY CHARACTERISTIC

In actual CMOS circuit, the combination logic circuit is always cascaded by many stages of gate circuits. Ideally, there is no delay in the logic gate, and the state change of the input will immediately cause the state change of the combination logic circuit. All the gates change their states instantaneously at the same time. However, because the transmission of the gate circuit has a delay, the stepwise driving of the combined circuit gate causes the change of the gate state not to be synchronously. The entire circuit completes the change within a period of time, instead of a certain moment. This phenomenon is called delay characteristic.

3.1.3 METHOD TO SELECT ATTACK POINT

For a combination logic circuit, the delay characteristic causes the successive flipping of the gates when inputting a signal excitation. That's the reason why power analysis attack samples a series of energy values during one clock cycle.

Due to the logic blocking, the flip rate of the former gate is larger than that of the latter stage, so the energy consumption value will also be relatively large. At the same time, due to the existence of the delay characteristic, the circuit energy consumption waveform will be expanded in time. The pre-stage gate will be flipped first, and the post-stage gate will be flipped where after. Therefore, in the energy trace of one clock cycle, there is a tendency that the energy value decreases with time.

Taking the s-box circuit as an example, the first s-box circuit of the AES cryptographic algorithm is simulated by HSPICE. The simulated energy consumption data is obtained for analysis, as shown in the figure 3.

Figure 3. Energy trace of s-box. Abscissa is time and ordinate is current value. The figure of all the energy traces below has the same abscissa and ordinate as this figure.
As can be seen from the figure 3, except some occasional transient spikes, the energy consumption of the circuit is basically reduced with time. The energy consumption value of the pre-stage gates is significantly higher than the post-stage gates'. When the clock edge arrives, the data begins to flow out of the register and enters the combinatorial logic circuit, at which point the energy consumption value begins to increase rapidly. The energy consumption value at the pre-stage gates is large, and the contribution is also large in the energy analysis. Since the pre-stage gate circuit obtains the data directly from the register, this part has the greatest correlation to the plaintext and the key (the part indicated by the red circle in the figure 3). So this part of the energy consumption value can be extracted for power analysis attack.

3.2 ICA for Energy Trace

For the actual collected energy trace, it will reduce the efficiency of the power analysis attack and even cause the attack to fail due to the inclusion of Gaussian white noise such as intrinsic noise and additive noise. Therefore, it is necessary to adopt an appropriate denoising method to process the collected energy traces, which will improve the signal-to-noise ratio and reduce the influence of noise.

Independent Component Analysis (ICA) is a very effective data analysis tool proposed in recent years. It is used to extract the original independent signal from the mixed data. In this paper, the FastICA algorithm is used. Compared with the common ICA algorithm, FastICA has the advantages of fast convergence, no need to select step parameters, and finding any independent components of non-Gaussian distribution by using a nonlinear function directly. Figure 4 is energy trace before denoising and figure 5 is energy trace after denoising.

3.3 Clustering of Energy Traces

Due to the similarity between the energy traces, they can be clustered by FCM clustering algorithm. The FCM algorithm is a partition-based clustering algorithm. Its idea is to make the similarity between objects divided into the same cluster the largest, and the similarity between different clusters the smallest.
FCM divides n vectors \( x_i \) (\( i = 1, 2, \ldots, n \)) into c fuzzy groups, and finds the cluster center of each group. The value function of the non-similarity index is minimized. The FCM causes each given data to determine the extent to which group it belongs to with a membership value between 0,1. In accordance with the introduction of fuzzy partitioning, the membership matrix U allows elements with values between 0 and 1. The normalization rule limits that the sum of the memberships of a data set is equal to 1 as formula (1).

\[
\sum_{i=1}^{n} u_{ij} = 1, \forall j = 1,\ldots, n \quad (1)
\]

The value function of FCM is formula (2).

\[
J(U, c_1, \ldots, c_c) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c} \sum_{j=1}^{n} u_{ij}^m d_{ij}^2 \quad (2)
\]

After mathematical calculation, it can be known that the condition for making formula (2) the minimum is as formula (3) and formula (4).

\[
c_i = \frac{\sum_{j=1}^{n} u_{ij}^m x_j}{\sum_{j=1}^{n} u_{ij}^m} \quad (3)
\]

\[
u_{ij} = \frac{1}{\sum_{k=1}^{c} \left( \frac{d_{ij}}{d_{kj}} \right)^{2/(m-1)}} \quad (4)
\]

From the above two necessary conditions, the calculation process of the FCM algorithm can be transformed into an iterative process as follows.

Step 1: Initialize the membership matrix \( U \) with a random number with a value between 0 and 1, and make it satisfy the constraints in equation (1).

Step 2: Calculate c cluster centers \( c_i \) (\( i=1,\ldots,c \)) using equation (3).

Step 3: The value function is calculated according to equation (2). If it is less than a certain threshold, or if its change from the last value function is less than a certain threshold, the algorithm stops.

Step 4: Calculate the new U matrix with equation (4). Go back to step 2.

### 3.4 Classification of Energy Traces

For each possible key value \( k \), a hypothetical intermediate value corresponding to the plaintext under a particular cryptographic algorithm is calculated. These possible values are recorded as vectors \( k = (k_1, \ldots, k_K) \). Where \( K \) represents the number of all possible values of \( k \). Given the plaintext vector \( d \) and the key hypothesis \( k \), we can easily calculate the hypothetical intermediate value \( f(d, k) \) using all \( D \) cryptographic runs and \( K \) key hypotheses. The next step is to map the assumed intermediate value to the energy consumption. We can simulate the energy consumption of the device caused by each hypothetical intermediate value through the Hamming distance energy model. Finally, the energy traces are
classified according to the assumed energy consumption, and the classification center is obtained.

### 3.5 Similarity Comparison

The classification center obtained under each key hypothesis is compared with the clustering center. The comparison criterion adopts the Euclidean distance criterion. The clustering center of the energy traces will have the highest similarity with the classification center under the correct key hypothesis. The key corresponding to the maximum similarity is the correct key.

### 4 EXPERIMENT AND RESULT ANALYSIS

The simulation experiment uses AES cryptography as the attack target. Under the 40nm process, the first round of 8-bit s-box circuit of AES cryptographic algorithm is simulated by HSPICE. The sampling interval is 1ps and the working period of the circuit is 8ns. The simulated energy consumption data is obtained by inputting different plaintext data. The acquisition of the simulated energy consumption value requires three steps, netlist generation, HSPICE simulation, and waveform file generation. The 2000 sets of plaintext are encrypted, and the key is 198. In the process of encrypting each plaintext, the energy consumption data is sampled. 2000 sets of power consumption data are obtained, and each set of energy consumption data is sampled by 1600 points. Figure 6 shows the energy trace corresponding to one of the plaintexts.

![Figure 6. Energy trace corresponding to one of the plaintexts](image)

After getting the 2000 sets of energy traces, we use our proposed method to do data processing. Then we get the attack result as figure 7. As shown in the figure 7, after data process of 2000 sets of plaintext and energy traces, the only obvious spike appears on the abscissa 198 in the attack result. The attack result indicates that the attack is successful.
We wonder how the attack results would be if we decrease the number of samples. In theory, the attack effect will gradually weaken until the attack fails, because our method essentially uses mathematical statistical analysis methods. The reduction of the samples will naturally lead to such expected results. So we set the number of samples as 1500, 1000, 500 and 300 to explore this variable’s influence on the attack.

As we can see from figure 7 to figure 11, as the number of samples decrease, the only spike at abscissa 198 gradually becomes inconspicuous and eventually disappears. The results means that the attack effect gradually weakens and eventually fails. And the results are consistent with our theoretical prediction.
5 CONCLUSION AND FUTURE WORK

In this paper, we propose a power analysis attack method based on FCM clustering algorithm. This method is an attempt to cross the machine learning method and the power analysis attack discipline, and is also a supplement to the existing system of energy analysis attack.

In the future work, considering the characteristic of fuzzy clustering of FCM algorithm, we will construct a model to calculate the confidence of the attack result based on the membership matrix of FCM. And in this paper, we only considered one variable—number of samples, and used only one energy model—Hamming distance model. We will study more variables’ influence on attack results and attack results’ confidences. We will also experiment on the actual chip instead of just doing a simulation experiment.

REFERENCES

1. Kocher P C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems[C]//International Cryptology Conference on Advances in Cryptology. Springer-Verlag, 1996:104-113.
2. Oswald D, Paar C. Breaking mifare DESFire MF3ICD40: power analysis and templates in the real world[C]//International Conference on Cryptographic Hardware and Embedded Systems. Springer-Verlag, 2011:207-222.
3. Kocher P, Jaffe J, Jun B. Differential power analysis[C]//Advances in cryptology—CRYPTO’99. Springer Berlin/Heidelberg, 1999: 789-789.
4. Quisquater J J, Samyde D. Electromagnetic analysis (ema): Measures and counter-measures for smart cards[M]//Smart Card Programming and Security. Springer Berlin Heidelberg, 2001:200-210.
5. Chari S, Rao J R, Rohatgi P. Template Attacks[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2002:13-28.
6. Hospodar G, Mulder E D, Gierlichs B, et al. Least squares support vector machines for side-channel analysis[J]. Center for Advanced Security Research Darmstadt, 2011: 99-104.
7. Hospodar G, Gierlichs B, De Mulder E, et al. Machine learning in side-channel analysis: a first study[J]. Journal of Cryptographic Engineering, 2011, 1(4): 293-302.
8. He H, Jaffe J, Zou L. Side channel cryptanalysis using machine learning[J]. CS229 Project, 2012.
9. Chou J W, Chu M H, Tsai Y L, et al. An unsupervised learning model to perform side channel attack[C]//Pacific-Asia Conference on Knowledge Discovery and Data Mining. Springer, Berlin, Heidelberg, 2013: 414-425.
10. Martinasek Z, Zeman V. Innovative Method of the Power Analysis[J]. Radioengineering, 2013, 22(2):586-594.
11. Martinasek Z, Hajny J, Malina L. Optimization of Power Analysis Using Neural Network[M]// Smart Card Research and Advanced Applications. Springer International Publishing, 2013:94-107.