An Improved DPA Attack on DES with Forth and Back Random Round Algorithm

Cai-Sen Chen[1], Xi Yu[2], Yang-Xia Xiang[2], Xiong Li[3], and Tengrun Li[4]

(Corresponding author: Cai-Sen Chen)

Ministry of Science Research, The Academy of Armored Forces Engineering[1]
No.21 Dujiakan Street, Fengtai District, Beijing City 100072, China,
Department of Information Engineering, Academy of Armored Force Engineering[2]
No.21 Dujiakan Street, Fengtai District, Beijing City 100072, China
School of Computer Science and Engineering, Hunan University of Science and Technology[3]
No.2 Taoyuan Road, Yuhu District, Xiangtan City, Hunan Province 411201, China
Kunming communication period, Kunming Railway Administration[4]
Kunming communication section, Kunming Railway Bureau, Yunnan province 650051, China
(Email: caisenchen@163.com)

(Received Jan. 07, 2016; revised and accepted Mar 10 & Apr. 9, 2016)

Abstract

The power leakage problems of smart card chip during the process of DES encryption are analyzed, we propose two attack algorithms on DES with forth and back random round algorithm respectively, include the accumulative attack algorithm and segmented attack algorithm. We provided an improved analysis algorithm based on the segmented attack by using a new correctional factor: the cliffy characteristic of the peak value. Finally, the first round key of DES was recovered successfully, and the DES key was deduced. It proves that the countermeasure with forth and back random round cannot t protect the security of smart card. We implement the DPA attack on DES with forth and back random round algorithm in the mathlab simulation experiment environment, the experiment results show that the feasibility and effectiveness of DPA can be improved by the advanced algorithm.

Keywords: Accumulative attack algorithm, DES algorithm, differential power analysis (DPA) attack, forth and back random round, segmented attack

1 Introduction

The traditional cryptanalysis methods are invalid with the improvement of the cryptographic algorithms and the increases of key length, a new cryptanalyst analysis algorithm was proposed based on the leakages information during the process of cryptographic chip, such as execution time, power consumption, etc. This attack algorithm was defined as Side Channel Analysis (SCA), which is a new direction of the cryptanalysis. Due to the features of chip circuit, there are side channel leakages during the process of encryption for smart card. The experiment result had proved that these leakages were closely related to the data and the key during the process of the cryptographic execution. As the high facility of implementation, low consumption, Side Channel Attack has become a new hotspot in the research field of cryptanalysis [11].

Paul Kocher proposed Power Analysis (PA) attack [9] in 1998, and gave three methods of it at the same time, Simple Power Analysis (SPA), Differential Power Analysis (DPA) and Correlative Power Analysis (CPA) [8, 15]. Due to its low consumption, fast speed, Power Analysis attack can collect the power consumption of the smart card to crack the key without breaking the chip, which could cause a large threat to safety of the smart card. SPA attack cracks the key using one or a few power consumption curve directly or indirectly, without a large number of statistical analyses. While DPA attack requires collecting a large number of power consumption curve, the attackers do not need to know the detail information of the target device, they only need to know which cryptographic algorithm was performed, so this attack has strong resistance to the noise [5].

Recently, study of DPA attack on smart card had achieved some progress. Literature [12] proposed a method to analyze power consumption using Neural Network, which combines the advantages of SPA and DPA, and even could restore the key with only one power consumption curve. Literature [4] provided a series statistical test methods of DPA attack. Literature [3] built the basic power simulation model for the first time, and literature [1] applied the basic power simulation model to smart card chip. Nowadays, based on the model, more effective models have been proposed [6, 13, 14]. Brier presented a method of correlation coefficient which has become a new direction of the DPA study [2].

In order to improve the safety of the chip to prevent DPA attack, literature [10] put forward a countermeasure method for linear and nonlinear part during the process of DES encryption, which could randomize the intermediate values based on the software programming of MASK [16], and make the power consumption and intermediate values are not correlative, so it can prevent the power attack, which has become a hot area of DPA countermeasure research. However, the small amount of MASK has not sufficient randomness, and it requires long operation time and large power consumption, then researchers presented a random round model implemented in hardware. Radom round concealed the real interval [15] of DES encryption with pseudo random input/output and round number. Dummy round resistant countermeasures on the basis of the random round position can be divided into two kinds, forth-back dummy round and middle dummy round. This article mainly focuses on the study of DPA attack against DES algorithm with forth-back dummy round [7].

2 DES and DPA Model

2.1 DES Algorithm

DES faces a security challenge as its fixed and short key, but due to its fast speed and low consumption, nowadays most of smart cards still use the DES as a security method. Each round in 16 rounds of DES there are 8 looking up S-box table operation. The input of S-box is a 6-bit subkey XOR with a 6-bit R register value, and the output of S-box is a 4-bit data. And then the 32 bit output will be restructured, XOR with the value of L register, then L and R register value changed each other. Each round deals with data in the same way. Figure 1 shows the first round encryption process.

Put 64 bit input plaintext into left part L_1(32 bit) and right part R_1(32 bit), in which R_1 will be 48 bit after expansion, and then get 32 bit through S box after R_1 XOR with subkey Key_0. The 32 bit XOR with L_1 becomes the R_2, while this round R1 become next round.

$$\begin{aligned} L_2 &= R_1 && (1)\\ R_2 &= L_1 \oplus f\left(R_1, Key_0\right). && (2) \end{aligned}$$

Function f indicates these steps of plaintext expansion, exclusive, data compression and displacement, which is nonlinear operation steps in the process of encryption.

2.2 Analysis Model of Power Consumption

In power analysis attacks, the attacker needs to make a relationship between the data and the power consumption of the attacked device. In the practical implementation, they are not a direct linear relationship; attacker only needs to know the relative value of power consumption instead of the absolute value. Commonly we use the Hamming-distance model (HDM) and Hamming weight model (HWM).

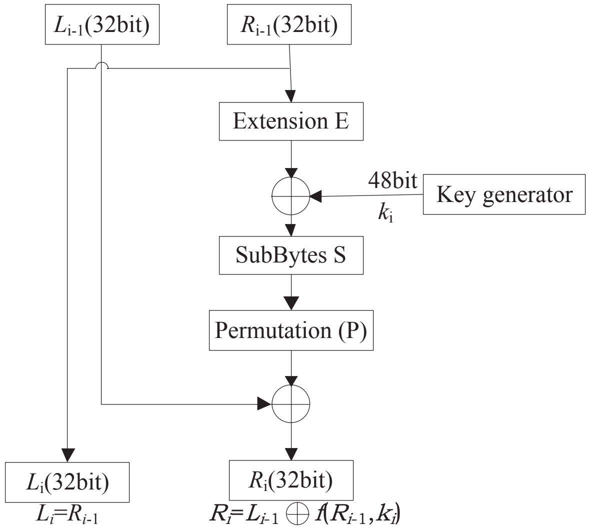

Figure 1: The i_{th} round of DES encryption process

A device of digital circuit may make a flip in a moment, it will produce dynamic power consumption (replaced with power in the follow), and thus the more device flips, the more power consumption. Therefore, the number of device flips can be relative with the relative value of the power consumption, which is the basic principle of HDM. HDM generally can be used to describe the power consumption of the bus and register.Attackers will get the corresponding information through establishing a linear relationship between the number of device flips from timing start to end and power consumption using HDM. Theoretical studies show that power consumption of device flip before and after is linear correlative with the hamming distance of binary data before and after.

$$P = k * HD\left(V_0, V_1\right) + d. \qquad (3)$$

k and d is the constant decided by the device characteristics.

From the point of SPA, it obtains the hamming distance information, detects the size of relative power consumption. From the point of DPA, it takes hamming distance as a function to attack the power curve. The biggest drawback of HDM is that the attacker must know the initial value and the final state to calculate the correct hamming distance, but in reality it is not necessarily to get these two values.

HWM is much simpler than HDM. In HWM, attackers assume that the size of power consumption is proportional to the number of the bit 1 in the processing value V_1, which is also the HW of value V_1.

$$P = k * HD\left(V_1\right) + d. \qquad (4)$$

k and d are the constant values which are decided by the device characteristics.

The advantage of HWM is that it doesnt need to know all the status value of circuit unit, and just needs the hamming weight of a certain status, to construct the corresponding relationship between power curve and value. All experimental results in this article are based on HWM.

2.3 Principle of Differential Power Attacks

Nowadays most of the integrated circuits are composed of CMOS, the energy consumption of CMOS can be divided into two parts: static and dynamic energy consumption. The former refers to the components without any data processing, namely the circuit without own energy consumption of gate flip; the latter refers to the energy consumption of gate flip, in addition to static energy, when internal element or output signals changes.

In the common CMOS circuit, the total energy consumption of the circuit is mainly caused by dynamic energy consumption, and the dynamic energy consumption is mainly related to the data processing. According to the type of energy consumption described before, it can be seen that the dynamic energy consumption is associated with the change of the data, which is a large proportion of the total energy consumption in the circuit, so the energy consumption of the circuit mainly depends on the data processing, it is also the physical circuit basis of energy attacks.

The DPA attack mainly includes two steps [8]: waveform acquisition and data analysis. Power waveform acquisition is on the hardware part, this article mainly use the simulation software, so it mainly relates to data analysis, the detailed steps are as follows:

1) Encrypt different plaintexts N groups and measure the power consumption curve in the first round of the DES operation process $\{P_i|1 \leq i \leq N\}$.

2) Select a bit of the output value of the first S box operation in the first round as a function D, with b indicates the bit value, called intermediate value. It is easy to know that all depends on the key K and plaintext M to b, which can be indicated as D(K, M). Make a guess on related value when attacking to get the corresponding intermediate value. According to the intermediate value, N groups power consumption curve can be divided into two categories:

$$S_1 = \{P_1|D = 1, 1 \leq i \leq N\} \quad (5)$$

$$S_0 = \{D = 0, 1 \leq i \leq N\} \quad (6)$$

3) The average power consumption of set S_1 and S_0 calculated separately:

$$A_1 = \frac{1}{S_1}\sum S_1(i) \quad (7)$$

$$A_0 = \frac{1}{S_0}\sum S_0(i) \quad (8)$$

Among them, S_1 and S_0 indicates the number of power consumption curves corresponding collection:

$$|S_1| + |S_0| = N. \quad (9)$$

4) The difference value between them is:

$$T = A_1 - A_0. \quad (10)$$

If the key is guessed correctly, and then the classification of the power consumption curves is right, that is to say, all the curves of $b = 1$ points to S_1, and the rest curves of $b = 0$ are assigned to S_0, so there is an obvious peak in power consumption curves. If the key is not right, the peak of T will be very little or no.

Classifying collection equate with classifying collection using a random function. As the mathematical statistics theory, when using a random function divides collection into two, elements in the two collections tend to infinity; the difference of average between the two subsets will tend to 0. If the sample space of power consumption curves analysis is big enough, the chosen model appropriates and the effects of sampling noise is small enough, we will get the difference power consumption curves with the peak after the above difference statistical method, the position of the peak is the guessed key. According to the above method calculated, we can obtain the key corresponding to the first S box and repeating to acquire the key corresponding to rest S boxes. Finally, we will obtain the 48 bit key actually used in this way and guess the rest 8 bit in exhaustive method to acquire the complete 56 bit key. Such workload is $2^6 \times 8 + 2^8 = 768 \leq 256 = 7.2 \times 10^{16}$. Detailed algorithm is shown in Figure 2.

3 Differential Power Analysis of DES Implemented With Forth and Back Random Round Algorithm

3.1 DES Implemented with Forth and Back Random Round Algorithm

Generally, the principle of DPA attacks on smart card DES chip is aligning to find the starting position of DES data encryption by filtering the power wave, then cracking the key of the first or 16^{th} round of DES encryption. Based this principle, C. Herbst puts forward a defense algorithm using random round, namely before or after or in the middle of the DES encryption joining a random pseudo rounds, whose rules and operations are the same, but each round input is not plaintext instead a random number, while the real DES encryption still encrypt plaintext make the normal output.

Due to the number of random round in DES encryption becomes more and more, the ability of resistance to the DPA attacks becomes also stronger. However the more

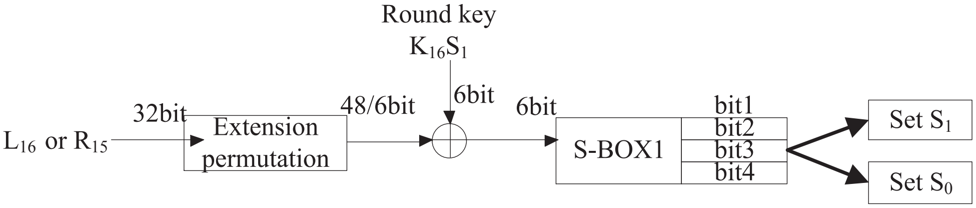

Figure 2: Distinguish between power consumption function

the number of random round and the more widely distribution is, the slower speed of chip CPU is, some smart card used forth and back random round model are shown as in Figure 3.

Figure 3 shows the relationship between power consumption when plaintext encrypted and random round. The number of random round each encrypted is not fixed and the real encryption interval of DES algorithm is uncertain, so even if attackers have got the power consumption curves, they also don't know the position of the real encryption interval.

3.2 Two Kinds of DPA Analysis Attacks Against DES Algorithm

3.2.1 Accumulative Attack Algorithm

Figure 4 shows the average cumulative power consumption of the previous round (DR + 1) before the accumulative attack algorithm. This method can be regarded as a derivation of alignment operation: the average power consumption as the first round and make it contains the power consumption of the first round or even complete real DES algorithm indirectly. This method can guarantee that attack contains useful information in the first round, just with bigger noise which generated from random round.

According to the principle shown in Figure 4, we will put forward a concrete algorithm.

In the accumulative attack algorithm, we accumulate the former (DR+1) power wave, then average, and treat it as the new first round of DES algorithm. Because the maximum number of dummy rounds is DR, the front (DR+1) rounds include at least the first round of DES. The new first round contains real first round and noise due to other rounds, so we attack the new round to get the key by using DPA.

3.2.2 Segmented Attack Algorithm

Compared with the accumulative attack algorithm, nodes and methods of segmented attack algorithm are different. Algorithm 1 chooses the former (DR+1) rounds and add power consumption together to get the average power consumption, as the first round of the DES, while Algorithm 2 does not accumulate power wave, but to attack each former (DR+1) rounds respectively. As shown in Figure 5.

Algorithm 1 Accumulative attack algorithm

```
Begin
input: M; //the set of plaintext, each plaintext indicated as $M_i$, $i$={1,..., size($M$)};
Wave; //the set of power consumption curves, each curves indicated as $Wave_i$, $i$=1,..., size($M$), corresponding to plaintext;
DR; // the maximum number of random round;
DRinput; //input of each random round;
output: number; //the possibility sort of key corresponding to 8 S-box;
Subkey($i$); //the subkey corresponding to each S-box
while $j < size(M,1)$ do
    while $i < (DR+1)$ do
        Temp=Temp+Wave($i$) //a loop of waveform accumulation
        Wave($j$)=Temp/(DR+1) //make it as "the first round" after accumulation
    end while
end while
DPA algorithm
number;
Subkey($i$);
End
```

According to the principle in Figure 5, we will put forward concrete algorithm.

The basic idea of Algorithm 2 is that: from left to right, we regard each round as imaginary "the first round" of DES, and get each subkeys of them by using DPA. Each round of the same S-box has subkey possibility sorting by order from high to low, and store the top 10 subkeys in the set $KeyRank(1)$; we put all $KeyRank$ sets of the same S-box together and find the key with highest occurrence probability and top ranking, and then the subkey is the correct key of the S box. Repeat the process for each S box, we will find all the right subkeys.

4 The Simulation Experiment Results And Complexity Analysis

4.1 Simulation Experiments

Due to the laboratory conditions limited, this article makes simulation experiments on matlab to verify the re-

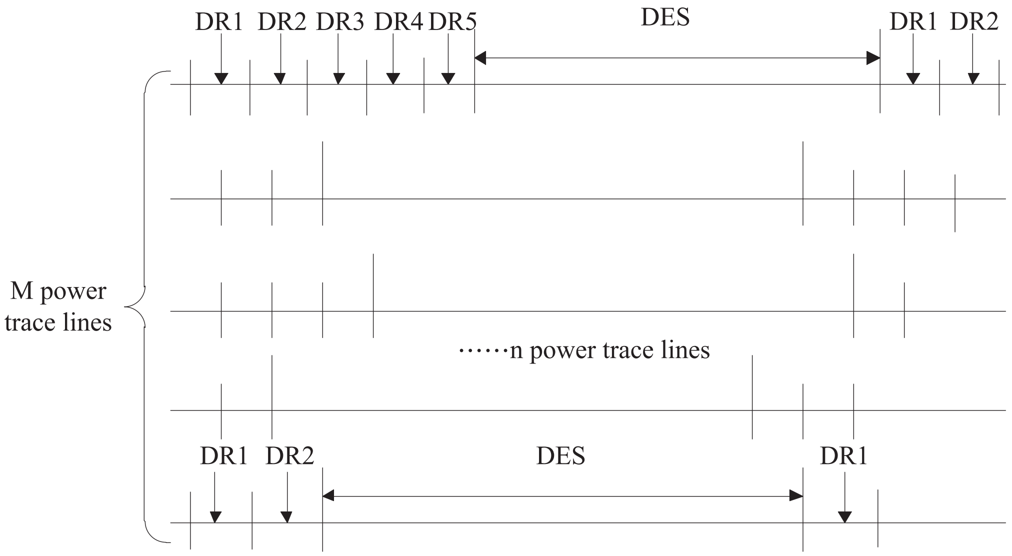

Figure 3: Forth and back random round model

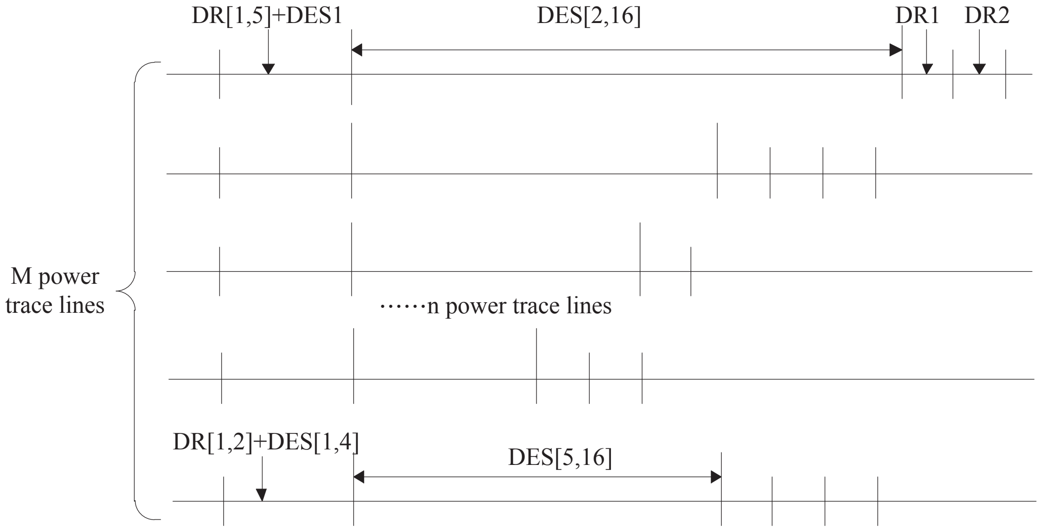

Figure 4: The principle of the accumulative attack algorithm

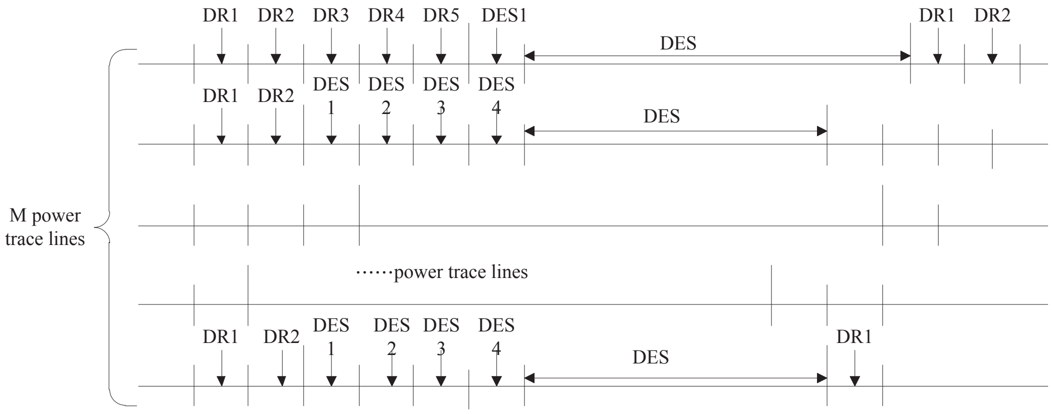

Figure 5: The principle of the segmented attack algorithm

Algorithm 2 Segmented attack algorithm

```
Begin
input: M; //the set of plaintext, each plaintext indicated as $M_i$, $i$=1,..., size($M$);
Wave; //the set of power consumption curves - each curves indicated as $Wave_i$, $i$=1, ..., size($M$), corresponding to plaintext;
DR; // the maximum number of random round;
DRinput; //input of each random round;
output: KeyRank($i$) // the possibility sort of key corresponding to 8 S-boxi=1, ..., DR, DR+1, the size is 8*64;
Number; // the possibility sort of (DR+1) corresponding to 8 S-box, the size is (DR+1)*64
while $i < (DR + 1)$ do
  while $j < size(M, 1)$ do
    DPA algorithm
    KeyRank (j);
  end while
end while
Number(i)=KeyRank($j$)(i,:);// extract (DR + 1) KeyRank ($j$) of the same line Number as all the lines of the Number (I)
End
```

search content. As already stated, the study results of Hamming Weight Model have shown that the results of power consumption sampling in simulation experiments are basically identical with the actual. The target of experiment is the first round of DES keys, setting the maximum random number of previous round is 5 and the length of key is 64.

4.2 The Results of the Experiment

Based on the accumulative attack algorithm and the segmented attack algorithm above mentioned, we make the simulation experiment on MATLAB and put forward an improved algorithm based on the results of segmented attack algorithm.

4.2.1 The Results of Accumulative Attack Algorithm

According to accumulation attack algorithm introduced in Algorithm 1, we design programming ideas to acquire subkey and its possibility sort corresponding to each S-box using MATLAB, and the most likely key is the right one.

Table 1 shows the possibility matrix (size is 8 * 64) of key corresponding to 8 S-boxes. The probability is derived from the height of peak in the DPA attacks corresponding to each subkey, and t the larger the peak value is, the higher the possibility of it. Each row of the matrix represents the 64 guessing keys corresponding to S-box, ordered from big to small of the peak value, and the first column represents the key with the highest peak values.

Table 1: the possibility sort of subkey corresponding to 8 S-boxes based on accumulation attack algorithm

	subkey								
Sbox	1	2	3	4	5	6	7	...	64
1	29	47	24	4	35	8	28	...	52
2	48	46	37	45	47	20	27	...	55
3	39	35	10	37	43	41	42	...	22
4	55	26	10	20	34	42	60	...	25
5	39	52	1	36	60	14	48	...	42
6	44	16	23	57	48	48	51	...	37
7	16	21	54	22	28	28	48	...	27
8	14	26	38	10	25	25	29	...	2

Experiments show that when the number of power consumption track become bigger and bigger, for the same key, the number of the first column is more stable, which is the right sort of subkey remains about the same.

Table 2: The success rate of accumulative attack algorithm

Power Trace Line Number	Correct Key Number	Incorrect Key Number	Success Rate(%)
50	1	7	12.5
80	1	7	12.5
100	3	5	37.5
200	4	4	50
300	6	2	75
400	6	2	75
700	7	1	87.5
1000	7	1	87.5
1300	8	0	100
2000	8	0	100
3000	8	0	100

Table 2 statistics that the success rate of the DPA attacks to DES algorithm using accumulative attack algorithm. It is shown that we can break the DES algorithm by 1300 power consumption curves of key at most in accumulative attack algorithm.

4.3 The Results of Segmented Attack Algorithm

According to Algorithm 2, we make the simulation experiment on MATLAB and get the key corresponding to each S-box.

The maximum number of random round is 5, the round of segmented attack algorithm is 6, and the results of each round as a row of Table 3 shown, in addition, each column is sorted by the possibility (the larger the peak value is, the higher the possibility of it)of the subkey. Selected the

Table 3: The guessing key sort of S2-box

	subkey								
Round	1	2	3	4	5	6	7	...	64
1	11	49	3	2	53	57	26	...	15
2	37	27	45	4	20	63	39	...	56
3	37	48	46	47	38	51	63	...	1
4	37	4	47	19	48	28	46	...	20
5	37	48	46	27	39	56	11	...	17
6	37	4	50	27	45	3	38	...	19

top 10 columns, we make a statistical about occurrences of each guessing subkey with KeyRank, and the results shown in Figure 6.

As Figure 4.1 shown, the subkey corresponding to S-box is 37. According to the method cycled, we can obtain the key corresponding to 8 S-boxes. Table 4 shows the success rate of segmented attack algorithm.

4.4 An Improved Analysis Algorithm with an Introduced Modifying Factor

Compared with Table 2 and Table 4, we can see that when the success rate of attack reaches 100%, the used sample size of segmented attack algorithm is larger than accumulative attack algorithm. In principle, due to average all power consumption curves in accumulative attack algorithm, the noise will be increased anyway, while segmented attack algorithm is not, it is piecewise attack, only compared occurrences and ranking position of each period key to find the correct one in the end, which means Algorithm 1 with high noise while Algorithm 2 with large workload. However, theoretically, Algorithm 2 needs less power consumption curves, but in fact the opposite is true. After repeated experiments, we found that the right key not only depends on the ranking position but also the frequency at the same time in Algorithm 2, and sometimes these two factors are conflicts with each other, so it is too difficult to find a balance.

Verified by the experiment, when a number of guessing subkeys occurred at the same time, the probability of that one of these same frequency subkeys nearby is smaller, which probably to be the correct subkey. Therefore, we should join a correction factor, the steepness of peak, which means occurrences of the right key nearby is few.

As shown in Figure 7, the occurrences of the location corresponding to subkey 37, 46, 47, achieve the maximum. Identify the right values, we should take the steepness of peak into consideration. From the graph, compared with other two numbers, the frequency nearby key 37 is much smaller than itself, so the location of key 37 is the correct key.

Added random round, we measure 3000 power consumption curves corresponding to 100 random keys, calculated according to the Algorithms 1 and 2 respectively, and join the steepness of peak, to get the success rate of these two algorithm in different circumstances using true and false subkey (see Table 5).

In conclusion, two algorithms crack the key successfully, just the workload different. Algorithm 1, by contrast, the calculation of time and effort is less than the Algorithm 2, but easily affected by noise, so the Algorithm 1 is suitable for the situation which accuracy is not high but short time requirements of random, while Algorithm 2 can be applied to the situations which is high precision of key crack regardless of the time cost.

5 Conclusions

In this article, in view of the dummy round defensive measures, we make study on the DPA attack with DES algorithm of smart card. Firstly, according to the dummy round defensive feature, we present two kinds of DPA attack, accumulative attack and segmented attack algorithm; Secondly, we apply these two algorithms respectively to simulation experiments for smart card in MATLAB, which crack the key successfully and give the attack rate of both; Finally, introduced the modifying factor, we acquire the improved algorithm against segmented attack algorithm, in order to reduce the number of power consumption curves required for the attack.

The analysis of experimental results shows that the two kinds of attack algorithm is feasible, in addition, the running time and accuracy of each algorithm determines the scope of application. Next, based on the existing research, we will make efforts to further expand the design for the DPA attack algorithm using completely dummy round, and provides reference for a smart card password cracking.

Acknowledgments

The authors would like to thank anonymous reviewers for their valuable comments. This research was supported by the National Natural Science Foundation of China under Grant No. 61402528. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. L. Akkar, R. Bevan, P. Dischamp, and D. Moyart, "Power analysis, what is now possible?" *Lecture Notes in Computer Science*, vol. 1976, pp. 489–502, Springer, 2000.

[2] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," *Lecture Notes in Computer Science*, vol. 37, no. 22, pp. 8004–8010, Springer, 1998.

[3] S. Chari, "A cautionary note regarding evaluation of aes candidates on smart-cards," in *Advanced Encryp-*

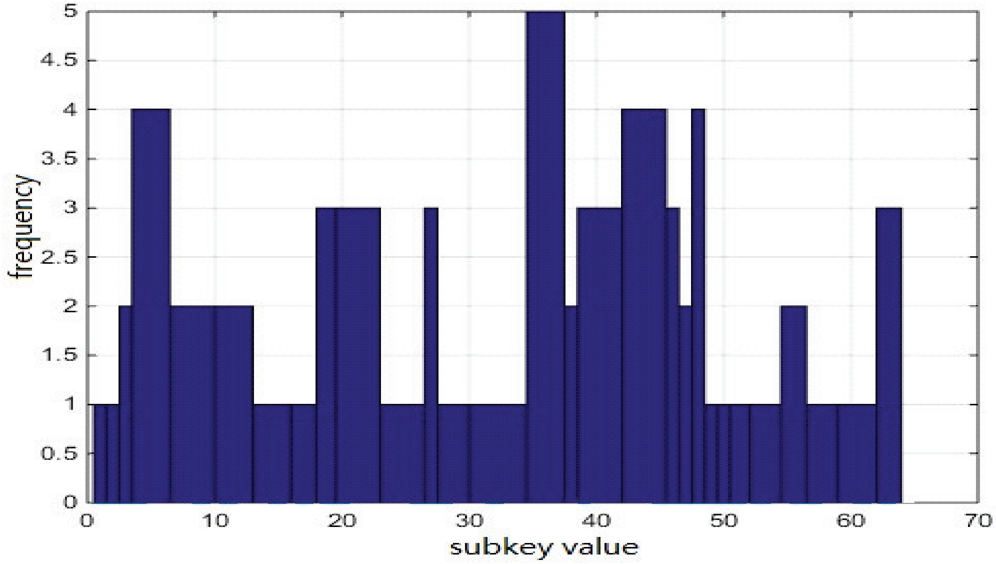

Figure 6: The key frequency of S2-box

Table 4: The success rate of segmented attack algorithm

power trace line number	correct key number	incorrect key number	success rate(%)
80	1	7	12.5
100	1	7	12.5
200	2	6	25
300	3	5	37.5
500	4	4	50
700	5	3	62.5
1000	6	2	75
1500	7	1	87.5
2000	8	0	100
3000	8	0	100
4000	8	0	100
5000	8	0	100

Table 5: Analysis results of success rate for two algorithms

	true: $false > 8:0$	**true:** $false > 7:1$
Accumulative attack algorithm	93	100
Segmented attack algorithm	95	99

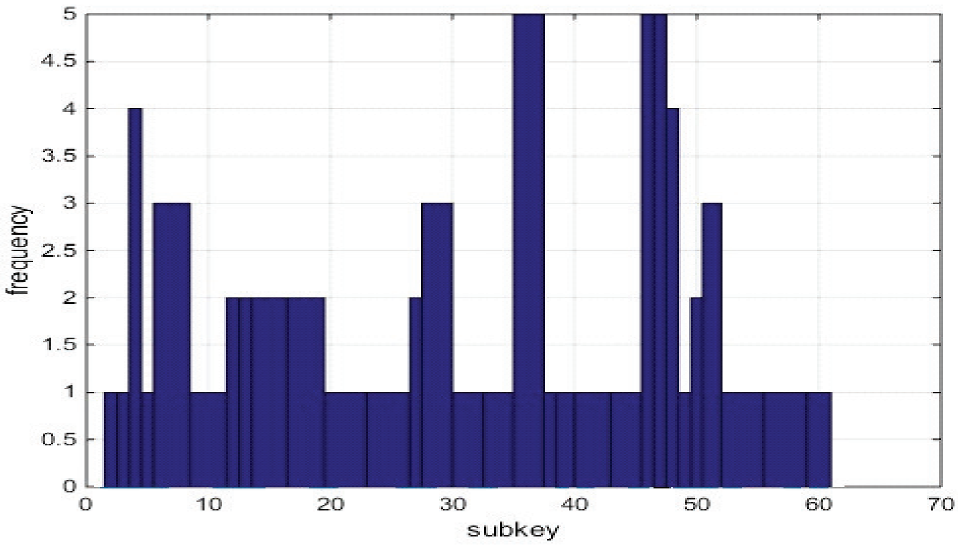

Figure 7: The frequency statistics of key corresponding to S2-box

tion Standard Candidate Conference, pp. 133–147, 1999.

[4] J. S. Coron, P. Kocher, and D. Naccache, *Statistics and Secret Leakage*, Springer Berlin Heidelberg, 2015.

[5] D. L. Delivasilis and S. K. Katsikas, "Side channel analysis on biometric-based key generation algorithms on resource constrained devices," *International Journal of Network Security*, vol. 3, no. 1, pp. 44–50, 2006.

[6] Y. Fei, Q. Luo, and A. A. Ding, *A Statistical Model for DPA with Novel Algorithmic Confusion Analysis*, Springer Berlin Heidelberg, 2012.

[7] C. Herbst, E. Oswald, and S. Mangard, "An aes smart card implementation resistant to power analysis attacks," in *Applied Cryptography and Network Security, Second International Conference (ACNS'06)*, pp. 194–206, 2006.

[8] L. I. Jing and L. I. Lin-Sen, "Differential power analysis method for des encryption in IC card chip," *Computer Engineering*, vol. 39, no. 7, pp. 200–204, 2013.

[9] P. C. Kocher, J. M. Jaffe, and B. C. Jun, "Differential power analysis," in *Advances in Cryptology (CRYPTO'99)*, LNCS 1666, pp. 388–397, Springer, 1999.

[10] S. Mangard, E. Oswald, T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer, 2008.

[11] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[12] Z. Martinasek and V. Zeman, "Innovative method of the power analysis," *Radioengineering*, vol. 22, no. 2, pp. 586–594, 2013.

[13] A. Moradi, M. Salmasizadeh, M. T. M. Shalmani, and T. Eisenbarth, "Vulnerability modeling of cryptographic hardware to power analysis attacks," *Integration the VLSI Journal*, vol. 42, no. 4, pp. 468–478, 2009.

[14] E. Peeters, F. X. Standaert, and J. J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integration the VLSI Journal*, vol. 40, no. 1, pp. 52–60, 2007.

[15] F. Yan, *The Study of Attacks and Defenses Based on AES Algorithm*, Master's Thesis, Beijing Jiaotong University, 2013.

[16] Z. Zhuang, J. Chen, and H. Zhang, "A countermeasure for DES with both rotating masks and secured S-boxes," in *Tenth International Conference on Computational Intelligence and Security*, pp. 410–414, 2014.

Caisen Chen was born in 1983. He received his master's degree in computer software and theory and a Ph.D. degree in network security technology from Ordnance Engineering College in 2009 and 2011, respectively. Dr. Chen now is a lecturer of Academy of Armored Force Engineering in Beijing, and his current research interests include information security and implementation attack analysis on Cryptosystems. He also researches the security of mobile device.

Xi Yu was born in 1992. She received her B.S. degree in information security from Sichuan University in 2014. She is currently a M.S. student in Department of Information Engineering, Academy of Armored Forces Engineering, Beijing, China. Her main research interest includes information security and side channel analysis of block ciphers. Email: yuxijxx@163.com.

YangXia Xiang was born in China in 1981.She received the Diploma in Computer Science and Technology from the University of Air Force Engineering,China, M.Sc in computer software architecture from Ordnance Engineering College,China.She now is a lecture at the Department of Information Engineering in Academy of Armed Force Engineering. Her current research interests include computer system and net work security.

Tengrun Li was born in China in 1990. She holds a B.Eng. in Communication Engineering, an M.Eng. in Communication and Information Systems , from the Beijing Jiaotong University. Her current research interests include bypass attack and defense.

Xiong Li was born in China in 1984. He received his master's degree in mathematics and cryptography from Shaanxi Normal University (SNNU), China in 2009 and Ph.D. degree in computer science and technology from Beijing University of Posts and Telecommunications (BUPT), China in 2012. Dr. Li now is a lecturer at School of Computer Science and Engineering of the Hunan University of Science and Technology (HNUST), China. He has published more than 40 referred journal papers in his research interests, which include cryptography and information security, etc. He has served on TPC member of several international conferences on information security and is a reviewer for more than 20 ISI indexed journals. He is a winner of the 2015 Journal of Network and Computer Applications Best Research Paper Award.