Journal of Computers Vol. 28, No. 1, 2017, pp. 69-71
doi:10.3966/199115592017022801006

Research on DPA Attack Based on Back and Forth Random Round with DES Algorithm

Tengrun Li[1 *], Genying Wang[1], and Caisen Chen[2]

[1] Department of Electronic and Information Engineering, Key Laboratory of Communiction and Information Systems, Beijing Municipal Commission of Education
Beijing Jiaotong University, Beijing, China
{13125024, gywang}@bjtu.edu.cn

[2] Ministry of Science Research, The Academy of Armored Forces Engineering, Beijing, China
caisenchen@163.com

Received 1 July 2015; Revised 27 July 2015; Accepted 10 August 2015

Abstract. For the smart card chip in the power leakage problem in the process of DES encryption, we put forward accumulative attack algorithm and segmented attack algorithm on DES encryption with back and forth random round which based on the analysis of DPA attack on general smart card and the features of random round, and get all keys rightly and successfully, to prove back and forth random round can't protect security of smart card. At last, by comparing the two algorithms, we give the scope of them.

Keywords: accumulative attack algorithm, back-forth random round, DES algorithm, DPA attack, S box, segmented attack algorithm, smart card

1 Introduction

Traditional password cracking methods are defeated with the improvement of the cryptographic algorithms, a cryptanalyst analysis algorithm is proposed based on the cryptographic chip leakages during the process of execution time, power consumption, etc. The information analysis algorithm, known as Side Channel Analysis (SCA), is the new direction of the code analysis.

Paul Kocher put forward PA attack [1] in 1998, and gave three methods of it at the same time, SPA, DPA and CPA. Power Analysis (PA) attack for smart card [2] is a typical representative of SCA, especially DPA attack. Dummy round was applying to prevent DPA attacks, that using pseudo random input/output and round number to cover real DES encryption interval, and it can be divided into two kinds, back-forth dummy round and middle dummy round. This article will put forward two algorithms based on the DPA attack, to prove that back-forth dummy round does not guarantee the security of smart card.

2 Related Work

In paper [0], Martinasek et al. put forward neural network method for PA attack, which combines advantages of SPA and DPA, sometimes can restore the key even use one power curve; Chari S et al. [0] presented power simulation model on smart cards for the first time, and more effective model based on the prior model has been put forward [0, 0] at present. Up to now, there is no effective means to deal with the back-forth dummy round.

* Corresponding Author

3 System Structure

The main contributions of this paper lies in the following two aspects.

Firstly, we describe DPA attack and back-forth dummy round details. Secondly, we propose accumulative attack algorithm and segmented attack algorithm, aimed at back-forth dummy round.

As presented in Fig. 1, the most important thing in DPA attack is to choose the key related power selection function D. In this paper, we want to get the encryption key of the first round in DES algorithm, and all S-boxes have the same calculation process. In DPA attack, the important thing to crack the key is to find the data encryption starting position, so if we random starting position of DES, attackers can't find real key.

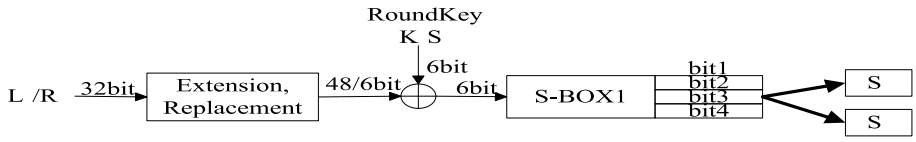

Fig. 1. Power consumption selected function

Fig. 2 shows the relationship between the power distribution of N plaintext encryption and dummy rounds, each position of dummy round is not fixed, and the real encryption DES algorithm interval is uncertain, so even if attackers get power curve, they also don't know where the real encryption interval is.

Fig. 2. Back-forth dummy round model

According to dummy round model, we put forward two new attack algorithms based on DPA attack principle.

3.1 Accumulative Attack Algorithm

In 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. The idea is shown as Fig. 3.

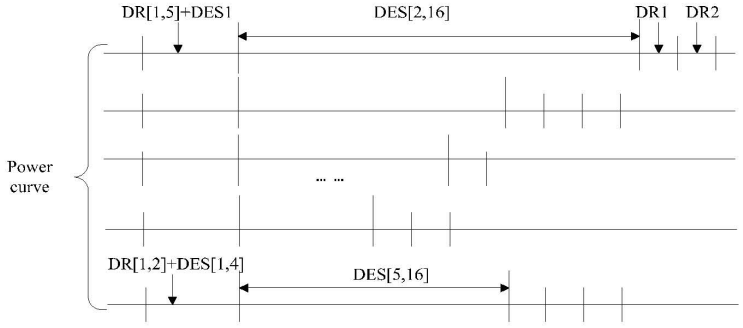

Fig. 3. Accumulative attack algorithm

3.2 Segmented Attack Algorithm

Fig.3 chooses the former (DR+1) rounds and add power consumption together to get the average power consumption, as the first round of the DES, Fig. 4 doesn't accumulate power wave, but to attack each former (DR+1) rounds respectively.

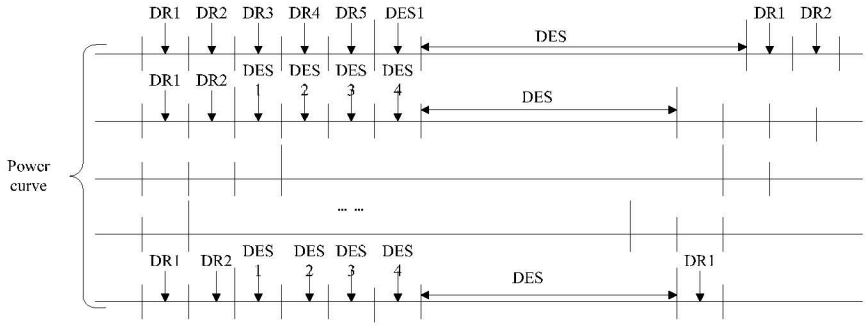

Fig. 4. Segmented attack algorithm

Just as shown in Fig. 4, from left to right, we regard each rounds as imaginary "the first round" of DES, and get subkeys of them by using DPA. Each round of the same S-box has subkey possibility sorting-Keyrank, we put all keyranks 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 Conclusion

In this paper, two methods based on DPA attack for back-forth dummy round with DES algorithm of smart card are proposed. Through the two methods, we can obtain smart card key with dummy round measures existing. By experimental verification, only thousands or even hundreds of power curve and in 1min, card can be successfully cracked.

We also will be based on the existing research, to further expand the design for the DPA attack algorithm using completely dummy round, and provides reference for a smart card password cracking.

References

[1] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Proc. of Advances in Cryptology—CRYPTO'99, 1999.

[2] S. Mangard, E. Oswald, T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer Science & Business Media, New York, 2008.

[3] Z. Martinasek, V. Zeman, Innovative method of the power analysis, Radioengineering 22(2)(2013) 586-594.

[4] S. Chari, C. Jutla, J.R. Rao, A cautionary note regarding evaluation of AES candidates on smart-cards, in: Proc. of Second Advanced Encryption Standard Candidate Conference, 1999.

[5] A. Moradi, M. Salmasizadeh, M.T.M. Shalmani, T. Eisenbarth, Vulnerability modeling of cryptographic hardware to power analysis attacks, INTEGRATION, the VLSI journal 42(4)(2009) 468-478.

[6] Y. Fei, Q. Luo, A.A. Ding, A statistical model for DPA with novel algorithmic confusion analysis, in: Proc. of Cryptographic Hardware and Embedded Systems–CHES 2012, 2012.

[7] Z. Zhuang, J. Chen, H. Zhang, A countermeasure for DES with both rotating masks and secured S-boxes, in: Proc. of Computational Intelligence and Security (CIS), 2014 Tenth International Conference on. IEEE, 2014.