Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 169-174
doi:10.4028/www.scientific.net/AEF.6-7.169

Insert Random Time-Delay Defense High Order Side-Channel Attack

Jianbo Yao[1, a], Tao Zhang[2,b]

[1] Department of Computer Science,Zunyi Normal College, Zunyi, Guizhou Province, China

[2] Westone Corporation, Chengdu, Sichuan Province, China

[a] yaojianbo007@gmail.com, [b] zhangtao@uestc.edu.cn

Keywords: Cryptographic chips, Higher-order side-channel attack, Advanced encryption standard, Random delay, Power attack

Abstract. Side-channel attack is a non destructive physical attacks method. The current cryptographic algorithms are vulnerable to higher-order side-channel attack. To defense high order Side-channel attack, in this paper, a new countermeasure based on inserting random delay is proposed to secure AES against higher-order side-channel attack. By inserting a redundant instruction, it is expected to reduce the correlation between the leakage and the inside operations, and thus make the statistic analysis infeasible. The simulation shows the method is efficiency.

Introduction

Cryptosystem security is a widely attention important questions. Normally, the Cryptosystem safety is measured with used by cryptographic algorithm complexity. However, when cryptographic algorithm is used to physical implementation, the algorithm complexity is not the only safety standard, even theoretically safety cryptographic algorithms, also may be due to the physical implementation and become insecure. Recently, the Cryptosystem security threats from a new Cryptosystem analysis, Side-channel attack [1][2][3]. Different from the traditional password analysis method, Side-channel attack is a use of Cryptosystem operation divulges information, such as the execution time, power consumption and electromagnetic radiation etc, combining statistics theory quickly cracked Cryptosystem of new methods. The attacker just get a small amount of power curve, can in a few minutes fast cracked DES cryptographic algorithm [4]. The latest research results shows that almost all the cryptographic algorithm, hash function of the physical implementation are vulnerable to Side-channel attack [5].

Current Cryptosystem anti Side-channel attack defensive method mainly adopts increase noise signals, reduce information leakage intensity, insert random time-delays and using random mask defense method, these defense of the core idea is to reduce Side-channel leakage information and internal operation of the correlation between, thus make the general Side-channel attack methods are difficult. However, a recent study shows that even if used these defense, the attacker may through advanced signal processing technology, high order attack technology and template attack technology to crack the Cryptosystem [3][6].

In order to defense higher-order side-channel attack, combined with the safety realization of AES algorithm, this paper proposed the insert random time-delays defense high-order side-channel attack. The simulation experiments to verify the effectiveness of this method is analyzed.

The remainder of this paper is organized as follows. Section 2 introduces side-channel leakage model and high-order attack model. Section 3 is side-channel attack analysis and defense design for AES algorithm. Section 4 is simulation experiment and analysis. Finally, a conclusion is presented in section 5.

Side-channel attack

Side-channel leakage model. Side-channel attack is a non destructive physical attacks method. The principle is to use all Side-channel information when Cryptosystem performing operations to crack the Cryptosystem, Side-channel leakage shows as Fig.1:

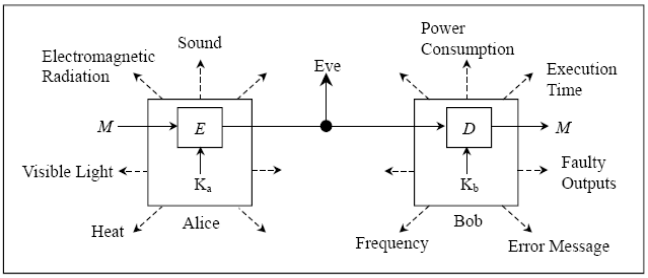

Figure 1: Side-channel leakage model

In order to describe the physical equipment of Side-channel leakage and Micali first proposed based on Turing machines abstract model [7], this model including an abstract virtual Turing machines A and a physical Turing machines P, the relationship shows as formula (1).

$$P = (L(), A) \tag{1}$$

where $L(.)$ is the abstract leak function. The state sets while Turing machines in operation shows as formula (2).

$$State = (S_1, S_2, ..., S_m) \tag{2}$$

The attacker gets leakage of information corresponding with the matching state.

$$L = (l_1, l_2, ..., l_m) \tag{3}$$

Side-channel attack using the Cryptosystem in various kinds of information leak when performing operations, combined with statistical analysis method cracked Cryptosystem.

N order side-channel attack model. Side-channel attack is based on statistic theory physical attacks method, to save his general, on $n(n \geq 1)$ order side-channel attack principle of instructions. N order side-channel against attack process may be divided into two stages: leakage information collection phase, key the analysis phase [7].

Leaked out in information collection phase, the attacker by cryptographic algorithm implementation details, determination and password attack related n running states $RS = (S_{i1}, S_{i2}, ..., S_{in})$. Then the password n times independent operation, collect the leak information and establishment relevant leak vectors $LS =< L_1, L_2, ...L_N >$.

Key analysis phase mainly using statistical tools for side-channel information analysis and presumably keys, can be divided into three steps:

1) Assumptions: establishing two different assumptions $H_0 : \{K_i \text{ is } 0\}$ and $H_1 : \{K_i \text{ is } 1\}$ for key K_i.

2) Classification: choose the appropriate divisional function $\phi(P_i, K_i)$, and according to the output will leak vector LS is divided into two sets:

$$\begin{cases} LS_0 = \{L_i \mid \phi(P_i, K_i) = 0, L_i \in LS\} \\ LS_1 = \{L_i \mid \phi(P_i, K_i) = 1, L_i \in LS\} \end{cases}$$

Respectively calculating the average signal:

$$\begin{cases} \overline{D_0} = \dfrac{1}{\mid LS_0 \mid} \displaystyle\sum_{O_i \in LS_0} O_i \\ \overline{D_1} = \dfrac{1}{\mid LS_1 \mid} \displaystyle\sum_{O_i \in LS_1} O_i \end{cases}$$

3) Comparing: calculation difference $\Delta D = \overline{D_0} - \overline{D_1}$, if $\Delta D = \overline{D_0} - \overline{D_1}$, then hypothesis H_1 is established, key is 1. Otherwise, the key is 0.

Higher-order attack technology makes the attacker in effectively obtain n a key point after the leakage of information related to the password, system is analysed through hypothesis testing.

Side-channel attack analysis and defense design for AES algorithm

Side-channel attack analysis for AES algorithm. AES algorithm main arithmetical unit consists of four reversible function composition: bytes replace function, row shift function, columns mixed function and round keys plus function. One round keys plus operations vulnerable to one-order side-channel attack, shows Algorithm 1, the attacker only obtain T1 moment the leakage of information can pass first-order side-channel attack cracked the keys Key.

Algorithm 1：No mask(PTi)

{

T1: $result = PTi \oplus Key;$

…others operation…

}

To defence first-order side-channel attack, the existing literature mainly uses the mask technology [8]. Shows Algorithm 2, in T2 moments in introducing a random number keys again add moments T3 computation.

Algorithm 2：Random mask(PTi)

{

T2: Produce a random number $Mask$， $Mask = rand();$

$MPTi = PTi \oplus Mask;$

T3: $result = MPTi \oplus key;$

…others operation …

}

Although this method can defence first-order side-channel attack, but the attacker can pass T2 and T3 moment leakage information association second-order side-channel attack, the key information can still be cracked.

Higher-order side-channel attack success requires two necessary conditions: enough sample swatches, each key related state of accurate samples values. Based on the analysis of AES algorithm side-channel attacks, the paper from weaken the Angle of attack and necessary conditions proposed new defence.

AES algorithm design defense side-channel attack. To defence higher-order side-channel attack, adopt the method of inserting random time-delays, make the attacker can obtain accurate leakage of information, thereby reducing statistical attacks success rate. In order to obtain a random time-delays way through software produces a random, respectively follow different operation, shows Algorithm 3.

Algorithm 3: InsertDummyInstruction ()

{

$index = rand();$

switch (index mod p) {

case 0: execute operation 0; break;

case 1: execute operation 1; break;

…

case p-1: execute operation p-1; break;}

}

This algorithm is based on the uniform random probability executed p the different redundant instructions, this command does not change the operation result of cryptographic algorithm, only causing a random offset in computation time at attack point. When performing operations in every

round keys AES algorithm, before key related state joining a redundant instructions InsertDummyInstruction (), respectively.

Algorithm 4: Secure round addition(PTi)

{

InsertDummyInstruction();

T2: Produce a random number $Mask$， $Mask = rand()$;

$MPTi = PTi \oplus Mask$;

InsertDumyInstruction();

T3: $result = MPTi \oplus key$;

…others operation …

}

As shown in the algorithm 4, before mask $Mask$ produce and before key exclusive or operation, all uses redundancy instruction method, obtain a random delay, and makes the attacker is difficult to directly obtain the accurate information for leak points. Therefore, this method can effectively defence higher-order side-channel attack.

Simulation experiment and analysis

For AES algorithm of round keys plus operations, this paper to the energy attack as an example, through the simulation experiment to verify the validity of the defence method of analysis by inserting random time-delays.

Experimental Settings. In order to acquire password chip energy information disclosed in operation, of energy consumption is analysed by Hamming weight of the leakage model, At the same time not considering the influence of noise signals to experiment, this is because in the differential energy attack, different assumptions leakage information contained in the noise signals can be difference operation mutual offset.

Experimental analysis. For two different situations for key $Key = 0,1$, the effectiveness of the defence method is reflected by the difference results.

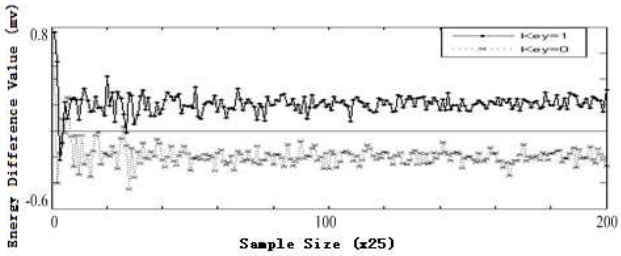

Figure 2: High order difference energy attacks

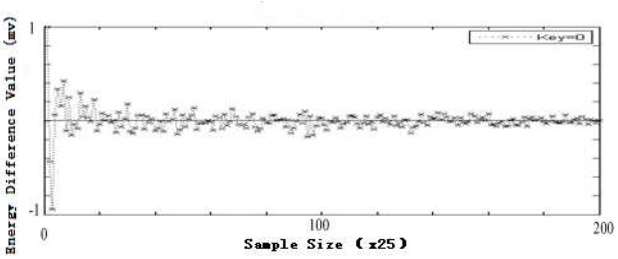

Figure 3: High order difference energy attacks defence (key=0)

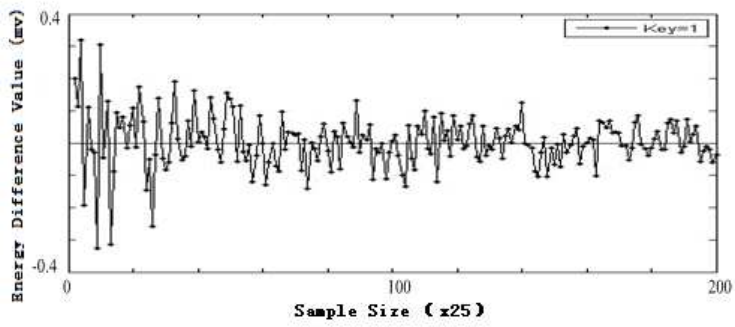

Figure 4: High order difference energy attacks defence (key=0)

When difference value is positive, Key analysis result is 1, whereas 0. In order to verify the validity of defence method in experiment (1), (2), experimental validation sample size from 2 to 5000, each in turn increase 25 samples. In the experiment (1) using random mask defence method. Attackers can analysis password through 2 orders energy attack, the difference results as shown in Fig.2. When energy curve sample size over 1000 when the difference results respectively trend constants (key is 0difference results tend to -0.2, key is 1 difference results tend to 0.2). So the method based on random mask and cannot be effectively defence second-order difference energy attack.

In the same condition of experiment, in experiment (2) using insert random time-delays defence method, key $Key = 0$ and 1, the difference results as shown in Fig.3 and Fig.4. Whatever keys $Key = 0$ or 1, as energy curve Numbers increased, the difference results have been energy attacks around 0 fluctuate and therefore the attacker can not guess out accurate the key information by statistic analysis from the experiment.

Through the above simulation experiments confirmed: the defence method based on the mask is vulnerable to higher-order bypass attack, and insert random time-delays defence method is able to effectively defence complex higher-order attack.

Conclusion

Side-channel attack is a new password attack methods, almost all the password equipment is vulnerable to side-channel the threat of attack. According to the emergence of new higher-order side-channel attack technology, this paper analysis higher order side-channel attack from the angle of information leakage and attack principle. Combined with the AES algorithm safety realization, this paper propose insert random time-delays defence method, and through the simulation experiment has proved that this method can effectively defence complex high order difference energy attacks.

Acknowledgments

This research was supported by The Governor Specialized Fund Item of Guizhou Province for Excellence Science, Technology and Education Talent under grant Qian-sheng-zhuan-he-zhi No.(2009)27; The Science and Technology Foundation Item under grant Qian-ke-he-J-zhi No.[2009]2275; Doctoral Found item of Zunyi Normal College No.[201213SJJ15].

References

[1] Yongbin Zhou, Dengguo Feng, “Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing”, Physical Security Testing Workshop, USA, 2005.

[2] P.Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Proceedings of Advances in Cryptology -- CRYPTO’96, SpringerVerlag, LNCS 1109, 1996. 104-113.

[3] Elisabeth Oswald, Stefan Mangard, Christoph Herbst, and Stefan Tillich. Practical second-order DPA attacks for masked smartcard implementations of block ciphers. In: proceeding of CT-RSA 2006, LNCS 3860, 2006.192-207.

[4] Tiri, K., et al. Prototype IC with WDDL and differential rounting - DPA resistance assessment. In: Proceeding of Cryptographic Hardware and Embedded Systems, SpringerVerlag, LNCS 3659, 2005. 354-365.

[5] YongBin Zhou, DengGuo Feng. Side channel attacks: ten years after its publication and the impact on cryptographic module security testing. http:// eprint.iacr.org/2005/388, 2005

[6] E. Oswald and S. Mangard. Template Attacks on Masking---Resistance is Futile. In: proceeding of CT-RSA 2007, 2007.12-27.

[7] Paul Kocher. Differential power analysis. In:Proceeding of Advances in Cryptology-CRYPTO’99, 1999, vol.1666, 388-397

[8] Jean-Sébastien Coron A1 and Louis Goubin. On Boolean and Arithmetic Masking against Differential Power Analysis. CHES 2000, Lecture Notes in Computer Science, Volume 1965, Springer 2000:231-237