Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 200-204
doi:10.4028/www.scientific.net/AEF.6-7.200

A Self-Healing Cryptosystem Design Prevent from 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: Side-channel attack, Cryptosystem, Masking method, Self-healing system

Abstract. Side-channel attack is a non destructive physical attacks method. In view of existing cryptosystem of Side-channel leakage of safe hidden trouble, this paper presents a kind of self-healing properties with the cryptosystem design method. Firstly, a new masking method is proposed, and it restricts the side channel measurement by inserting some measure-disabled points into the cryptographic algorithm. And then, a masking update technique is applied for making the side-channel leakage invalid. Compared with previous countermeasures, our method has stronger ability of self-healing and it also resists to complex side-channel attack.

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 improve the Cryptosystem safety ability resistance to Side-channel attack, this paper presents a new defensive method resistance to Side-channel attack, the basic idea of this method is that makes the attacker can obtain sufficient Side-channel leakage information, thus increasing the complexity of the Side-channel attack, On this basis, using mask updated technology enables attackers have shaken the leakage of information failure, to prevent an attacker to Cryptosystem in future threats. Compared with existing defenses method, this method reduces the Cryptosystem information leakage of system security hidden danger, and has strong "self-healing" ability.

The remainder of this paper is organized as follows. Section 2 introduces Side-channel leakage principle and adopting defensive strategy. Section 3 is the new mask technology principle and design method. Section 4 is masking update technology. Finally, a conclusion is presented in section 5.

Side-channel leakage and defenses

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:

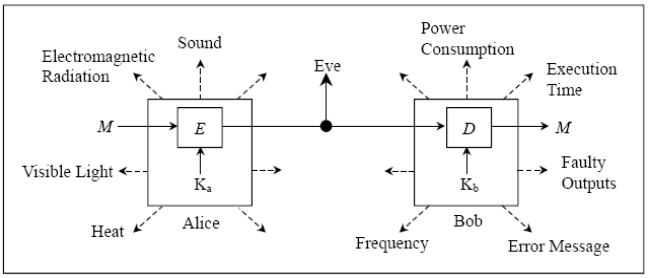

Figure 1: Side-channel leakage model

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.

Defense technology. For defensive Side-channel attack, usually by the defensive strategy is to reduce leakage information and key of the correlation between. At present the main defensive strategy can be divided into three categories:

1) Reduce leakage intensity of defensive: This kind of method mainly adopts leakage safety electronic devices constructing the Cryptosystem, such as Dynamic Differential Logic Circuit, ensure chip in operation of the process and the leakage information will never be as state changes and displays the differences in natures.

2) Reduce statistical correlation of defensive: Mainly in the Cryptosystem circuit implementation increase noise signals, or insert Random disrupt code （Random Mask）.

3) Limit Side-channel signal detection of protection method: In Cryptosystem additional signal monitoring circuit, prevent the attacker to signal detection and monitor.

Existing defensive strategy is mainly use appropriative anti leakage chips or increase security protection circuit to achieve information leakage of defensive, the Cryptosystem overall costs considerably. This paper put forward a new kind of mask technology. By using the existing CMOS device, only need in design on a small amount of improvement can effectively defensive information leakage.

New mask technology and safety analysis

Defense principle. New mask defensive principle is mainly inserts one or more measurement failure point while cryptography algorithm of operation process, making the attacker can not process sampling analysis about Side-channel leakage information at measurement failure point.

To facilitate the presentation, before given measurement failure point definition, firstly state e Micali's the general principle about Side-channel leakage, such as axiom 1 shows [7]:

Axiom 1: calculation and only calculation will leak Side-channel information.

Axiom 1 gives Side-channel leakage producing situations, on the basis of Axiom 1, given measuring effectiveness points are defined as follows:

Define 1: for key related state set $R=\{r_1, r_2, ...r_n\}$, measuring failure point refers to set R does not exist or not participate in operation in the relevant key state, the state will not disclose any Side-channel information.

In Cryptosystem operation process, the attacker through analysis the realization of cryptographic algorithm, determine the key related state set: $R=\{\text{Plaintext, Key, Mask1, Mask2}\}$.

The attacker must obtain all four of relevant state sampling information in set R to carry on statistical analysis. Hypothesis mask 1 does not participate in calculation, the state will not leak information, the attacker even obtain the remaining three state of information are also cannot be carried on statistical analysis.

Design method. The implementation process of cryptographic algorithms will be divided into two stages: key equipment initialization stage, cryptographic algorithm of operational stage. In the initialization stage, through the fixed mask to the primitive key information protection, avoid secret information leak, in operational stage, adopt insert measure failure point, ensures the attacker can not get all the sampling information of related state, thus preventing statistical attacks.

Algorithm 1: Mask key generation algorithms.

Input: original keys Key, fixed mask vector Fix_mask.

Output: mask key FKey, correction parameter FR

(1) Produce p fixed mask: $Fix\_mask = \{f_1, f_2, ...f_p\}$;

(2) Calculation mask keys: $FKey = f_1 \oplus Key$;

(3) Calculation correction parameter: $FR = f_1 \oplus f_2 \oplus ... \oplus f_p$;

(4) Mask Key replacement: instead of the original keys Key specific and fixed mask Fix_mask participation cryptographic algorithm implement.

After cryptography system initialization ended, use mask Key FKey instead of the original keys Key specific participate in calculation, ensuring an original keys security. Due to the introduction of Fix_mask fixed mask for cryptographic algorithm, the final results impact, so need to calculate the correction parameter FR, and corrected result before end of cryptographic algorithm.

Algorithm 2: Measurement failure point generation algorithm

Input: correction parameter FR, random mask vector Rand_mask

Output: output failure point *Inv*

(1) Produce q random mask: $Rand\_mask = \{r_1, r_2, ..., r_q\}$

(2) Calculating new random mask: $Rand\_mask = \{r_1', ..., r_q'\}$

$r_1' = FR \oplus r_1;\ r_2' = r_2; ...;\ r_{q-1}' = r_{q-1};\quad r_q' = r_1 \oplus r_2 \oplus r_3 \oplus ... \oplus r_{q-1};$

(3) Mask key XOR calculation: $m = FKey \oplus r_1';\ m = m \oplus r_2'; ...; m = m \oplus r_q';$

(4) Update correction parameter: $FR = r_1' \oplus r_2' \oplus ... \oplus r_q';$

(5) By the first (3) step, to determine the key related state sets R: $R = \{FKey, Rand\_mask, FR\}$

(6) Determine the measurement failure point.

Safety analysis. Assumptions $p = q = 2$, then the algorithm (1) and (2) respectively determine:

$$FKey = f_1 \oplus Key \text{ ,} \quad FR = f_1 \oplus f_2 \text{ ,}$$

$$r_1' = r_1 \oplus f_1 \oplus f_2 \text{ ,} \quad r_2' = r_1 \text{ ,}$$

In cryptography algorithm of operational stage, in order to attack the original keys Key, the attacker needs to calculate the $FKey \oplus r_1' \oplus r_2'$, monitoring to determine sampling points. Through the following deduction, $FKey \oplus r_1' \oplus r_2' = f_1 \oplus Key \oplus r_1' \oplus r_2' = Key \oplus f_2$ .Attackers may determine the two different sampling set:

$$T_1 = \{f_1, r_1', r_2', f_1 \oplus r_1' \oplus r_2' \oplus Key\}$$

$$T_2 = \{f_2, Key \oplus f_2\}$$

In the collection T_1, the attacker can not obtain sampling information of failure point; in the collection T_2, the attacker can not obtain sampling information of failure point, and state $Key \oplus f_2$ in calculation won't appear, so also cannot sampling.

Mask update technology

The traditional key protection, can pass change regularly key to ensure the security of the system [7], but frequent key replacement for key management and use bring many unchanged. Therefore, in this paper, on the basis of new mask, proposes a timing mask update technology,

The technology does not need to a key for replacement, and only need to mask for timing update, can make the attack received Side-channel the sampler info failure, and can prevent the attacker to the system further threat. Mask the updated technology makes the Cryptosystem can pass timing mask update to rebuild the system security after some effective Side-channel information are obtained, therefore, the Cryptosystem with strong self-healing capability.

Conclusion

The security problem for Side-channel leakage has put forward new requirements to security chip design and production. This paper put forward the new mask techniques and the mask timing updated technology for the construction of the security Cryptosystem resistance to Side-channel attack provides an effective and safe defense strategy.

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] S.Micali, L.Reyzin. Physically observable cryptography. In: proceeding of TCC 2004, LNCS 2951, 2004. 278-296.