PROCEEDINGS OF SCIENCE

A Survey of Side-Channel Attack and Security Assessment for Cryptographic Equipment

Dong-xin Guo
Department of information Engineering, Ordnance Engineering College
Shijiazhuang, 050003, China
Email: 810644463@qq.com

Kai-yan Chen[1a], *Yang Zhang[b], Xiao-han Wang[c]*
Department of information Engineering, Ordnance Engineering College
Shijiazhuang, 050003, China
E-mail: [a]chen-wu2013@163.com;[b]youngzhxm@126.com;[c]wxh2225@126.com

Xiao-yu Zhang[d],Zi-yan Xu[e]
Department of information Engineering, Ordnance Engineering College
Shijiazhuang, 050003, China
E-mail: [d]18811785953@163.com;[e]1508785745@qq.com

In order to understand the development of current channel energy analysis technology and protection strategy, at the same time, we will lay the foundation for establishing safety evaluation system about Encryption device in the next stage. We analyzed the side-channel attacks of the current mainstream encryption algorithms. The side-channel attack is classified by combining the specific operations of the algorithm that are easily attacked by the attacker. Aiming at the more popular DPA attacks, the paper focuses on the corresponding protection strategies, including the first-order DPA attack defense strategy and the second-order DPA attack defense strategy. Finally, the evaluation index of the current safety assessment system is summarized, and the effect of each index is elaborated.

CENet2017
22-23 JULY 2017
Shanghai, China

1 This study is supported by the National Natural Science Foundation of China (Grant No.51377170),the Young Scientists Fund of the National Natural Science Foundation of China (Grant No.61602505) and the National Natural Science Foundation of China (Grant No.61271152).

PoS(CENet2017)042

1. Introduction

With the depth of the development of information technology, Internet of things, such as the concept of Internet has been put forward, the types and numbers of information products growing, mobile payment, smart card, social networking platform and other information products to bring convenience to people also implied Many security risks. Information security has become the focus of attention in the 21st century countries, both in the civilian areas or in the military field, the disclosure of important information may cause undetectable loss.

In 1996, Paul Kocher [1] proposed the use of encryption equipment in the encryption process of side channel information (time) to attack the encryption device, breaking the traditional encryption algorithm design ideas, from the perspective of physical information analysis and research. After the side of the channel attack, security [2] and security assessment [3] has become a hot topic in the field of cryptography.

This paper is divided into three parts: The first part is mainly to summarize the research progress of the current mainstream encryption algorithm (including AES, DES, RSA, ECC). The second part mainly discusses several protection methods used to resist the side-channel attack, and focuses on the protection strategy of DPA attack, and puts forward the current problems. The third part is to explain the work of encryption equipment side-channel information security assessment related fields, and lay a solid foundation for further research.

2. Side-channel Analysis Based on Encryption Algorithm

At present, the mainstream encryption algorithm can be divided into symmetric and asymmetric keys according to the key. The corresponding key cryptosystem can be divided into two fields: the common key system and the public key system. Here we are on the two encryption system in the mainstream of the encryption algorithm to understand the bypass attack in the field of related algorithms research status and characteristics.

2.1 Side-channel Attacks Based on the Common Key System

The main feature of the common key system is that the corresponding encryption algorithm uses a symmetric key, that is, the same key to encrypt and decrypt the information, his biggest feature is the speed, you can quickly encrypt a large number of data, and because the key Management is more difficult, so the security of the key is weak. Here we are for AES, DES two classic algorithms for analysis.

2.1.1 Side-channel Attack Based on AES Algorithm

AES algorithm is the advanced encryption standard, it is the National Institute of Standards and Technology (NIST) in response to new security threats, after a long screening, the final alternative to DES as a new encryption standard. AES encryption algorithm has not only been adopted by the relevant government departments, and has a non-confidential, open operation, permanent free and so on, therefore, AES has been around the world government, financial institutions, important departments widely used.

Below we briefly describe the AES algorithm, AES algorithm belongs to the block cipher algorithm, packet length is fixed 128 bits, the key length is divided into three, respectively,

128,192,256 bits. With the increase of the key length, the greater the cost of cracking the key, this article mainly on the AES-128 introduced.

The algorithm requires a total of 11 rounds of encryption, including four encryption operations, including AddKey (AddRoundKey), byte substitution (SubBytes), row shift transform (ShiftRows), mixed column transform (MixColumns). The first round is the clear and initial round key key round key operation, the second round to the tenth round of the same operation, followed by byte replacement, row shift transformation, mixed column transformation, round key plus, the last round For byte substitution, row shift transform, round key plus. The following Figure1 shows the entire AES encryption process.

In the field of side-channel analysis, we have done a lot of research on the characteristics of AES algorithm. In order to solve the key of AES encryption algorithm, we usually need to find the key-related operation. The papers by analyzing the intermediate value of sensitive information in AES encryption algorithm, respectively, the S box, key expansion algorithm and key loading process were attacked, proved that the AES algorithm there are many vulnerable intermediate value[4,5,6,7]. Since the round key is derived from the last round of the key through the nonlinear transformation, so as long as the recovery of one of the wheel key we can get any other round of the subkey, the first method select the first round of the first S box output as a point of attack [8] , using DPA [1] side-channel analysis method, successfully decipher the key. In the final round of encryption, the second method uses the relationship between the table index value, the ciphertext and the corresponding subkey, and the relationship between the Cache hit rate and the encryption time is proposed [9]. Based on the Cache hit information under the side-channel attack. The final method is achieved by combining the actual and easy-to-use plaintext with the first two rounds of encryption operations or by combining the ciphertext with the last round of encryption operations to obtain the key [10].

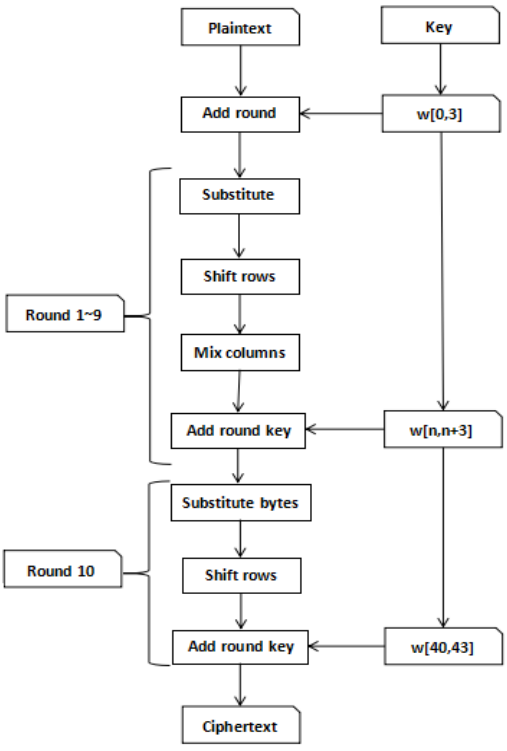

Figure 1 : AES encryption process

2.1.2 Side-channel Attack Based on DES Algorithm

DES (Data Encryption Standard) is data encryption standards, by the United States National Bureau of Standards tender, the National Security Agency assessment, launched in 1977. DES algorithm has the characteristics of fast running speed and high security. Although the security of DES algorithm is challenged with the development of computer technology and cryptography, it still occupies an important position in the development of packet cipher algorithm.

At present, there is a lot of research on the side-channel algorithm of DES algorithm at home and abroad. Because the key is the key information in the packet cipher algorithm, the attacker obtains the key to mean the leakage of the encrypted information, so the focus of the side-channel attack is to find The key information related to the operation, through the relevant operation of the side-channel information leaked key to crack.

In the round iteration process, the first step extension function E expands the 32-bit information to be encrypted into 48 bits, the second step 48 bits to be encrypted information and the corresponding 48-bit subkey, and the third step is The S-box converts the 48-bit information to 32 bits, and finally the replacement P replaces the 32-bit information to complete a round of iterations. Round operation process shown in Figure2.

Therefore, when the attacker knows part of the plaintext, you can attack for the key plus operation, S box operation and P replacement operation; when the attacker knows the ciphertext or part of the ciphertext, you can expand the operation and key operations Attack, because the

DES algorithm 48-bit sub-key has a combination, more difficult to crack, the attacker often through the specific algorithm in some of the characteristics or laws of the key crack to simplify, because the S-box operation is 6-bit data is converted to 4 Bit data, so in order to facilitate the

actual attack. One of the method by dividing the 48-bit subkey into 8 groups, each 6, each crack only 6-bit key, the key combination of only 64, reduced Crack the key calculation, and successfully on the IC card on the DES key to crack [11]. At the same time in the S box operation, the input data is 6 bits, the output data is 4 bits, after a large number of operations will lead to the output collision phenomenon, that is, different input leads to the same output. Another method uses this feature to reduce the search space of the key and successfully implement the key cracking method, which is based on the DES collision algorithm based on the DES algorithm [12,13,14,15].

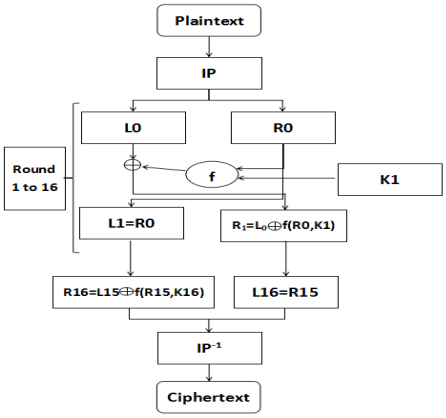

Figure 2 : DES encryption process

2.2 Side-channel Attack Based on Public Key System

Public key system is characterized by the corresponding encryption algorithm using asymmetric key, that is, the use of public key to encrypt the information, the use of private key to decrypt the information, the key management is more efficient, but the speed of encryption and decryption Slower, not suitable for large-scale data encryption. Here we focus on RSA, ECC two typical algorithms for specific analysis.

2.2.1 Side-channel Attack Based on RSA Algorithm

RSA algorithm is designed by the three American scientists in 1977, using a new design ideas, the use of large integer is not easy factorization principle, the key is divided into public key and private key, the public key used to encrypt information , The private key used to decrypt the encrypted information. Specific encryption and decryption algorithm shown in Figure3.

From Figure3, we can see that the variables n and e are the public key, d is the private key, m is the civilization, c is the ciphertext, p and q are decomposed by the large number n, the private key formula is:

$d = e^{-1} \bmod ((p-1)(q-1))$ (2.1)

Eq2.1 was resolved by Eq2.2.

$ed = 1 \bmod ((p-1)(q-1))$ (2.2)

From the formula Eq2.2, we can see that the public key e is known that the attacker wants to obtain the private key d, we must get the value of p and q, which is the general idea of cracking the RSA algorithm. In practical applications, n the number of bits is 1024 or more, the n decomposition is almost impossible to complete, in order to obtain the private key, by the formula we can usually use the decryption process of leakage and private key d related side-channel information to complete the crack. In first method, the key of the RSA public key cryptography is solved by acquiring the operation time of the key power operation, and finally the complete decryption key is obtained [16]. In second method, we focus on the RSA algorithm to find the precalculation table of the RSA algorithm based on the window algorithm. The sampling data Cache timed attacks, which successfully crack the 340 bits of the RSA algorithm 512-bit key, Greatly narrowing the search space for the key [17].

Because of the key-related operation in the RSA key generation algorithm, the key can be solved by analyzing the characteristics of the key generation algorithm. Final method is combined with the side-channel attack on the key generation algorithm for iterative bit-by-bit attack, the same successful reduction of the key search space [18,19,20,21].

Public key	n:The product of two prime numbers p and q (p and q must be kept secret) e:e and (p-1) (q-1) are prime
Private key	d: e-1 mod ((p-1)(q-1))
encryption	$c=m^e \bmod n$
Decrypted	$m=c^d \bmod n$

Figure 3 : RSA encryption and decryption algorithm

2.2.2 Side-channel Attack Based on ECC Algorithm

ECC (Elliptic Curves Cryptography), that is, elliptic curve encryption algorithm. Like the RSA algorithm, it is also a public key algorithm, which is more secure and efficient than other public key algorithms. The mathematical basis of the algorithm is as follows: Define the elliptic curve on a finite field, take two points K, G on the elliptic curve, let K = kG, where scalar k is an integer less than n and n is the order of point G. According to the elliptic curve of the addition rule, if known k, G, then easy to get K, if known K, G, not easy to get k. Designers use this feature, proposed in 1985, where point G is called the base point, k is the private key in the algorithm, and K is the public key in the algorithm.

At present, the object of the side-channel attack against the ECC encryption algorithm mainly involves the operation related to the key k. In the key generation algorithm, the public key K is generated by the base point G and the private key k, Leading to different characteristics of the side-channel signal leakage. Common method by generating equipment to generate a public key when the leakage of electromagnetic signals, the analysis of the private key to crack [22,23].

In the data decryption process, there is a key and the operation of the data to be decrypted, the attacker can analyze the operation of the side-channel information, the key attack. Another method in the decryption process, because the key is 1 and the key is 0 when the computing power consumption is different, through the precision instrument measurement, unprotected ECC algorithm successfully side-channel attack Crack the key [24].

3. Protection Strategy

The principle of side-channel attack is that the side-channel information disclosed by the device is dependent on the intermediate value of the encryption algorithm in the device. And the protection strategy is to hide or eliminate this relationship as much as possible through various means. At present, the protection strategy for side-channel attack mainly includes concealing technology and masking technology. The literature "Overview of side-channel Analysis for

Cryptographic Chip" has been described in detail, by hiding the technology, that is, by changing the side-channel signal of the device to be randomized or equalized; masking technology, which is concerned by the attacker's center Value side-channel information is transformed so that the side-channel information is not dependent on the intermediate value.

Hidden technology can be divided into two categories, the first category is in the side-channel information on the time dimension to improve, by changing the implementation of each

password algorithm during the operation of the corresponding correspondence between the time, so that side-channel information tends to randomize, attack Difficulty increases, the specific measures are: random insert pseudo-operation, out of order operation. The second type is optimized on the amplitude dimension of the side-channel information. By randomizing or fixing the energy consumption in the same clock cycle, the attacker can not extract the valid information from the energy consumption trajectory. The specific measures are: increase the noise and reduce the signal Wait.

Masking technology mainly includes Boolean mask and arithmetic mask,because the masking technique can eliminate the dependency of critical information and energy consumption without changing the energy consumption characteristics of the device, this technique has been paid more and more attention by researchers, and differential energy

analysis (DPA) attack is the most popular Energy analysis attacks, so this chapter will focus on the DPA mask technology research status outlined. Anti-DPA mask technology can be divided into anti-first-order DPA attack protection strategy, anti-second-order DPA attack defense strategy and anti-high-level DPA attack defense strategy.

3.1 Anti-first-order DPA Attack Protection Strategy

In the attack process, the attacker to use the DPA attack only use an intermediate value can be completed key cracking, so called first-order DPA attack. The first-order DPA attack defense strategy is to deal with the security threat generated by the first-order DPA attack on the device. The median value of the algorithm is transformed by masking, so that the median of the mask is independent of the intermediate value of the algorithm and is effectively protected The key key in the device algorithm. About the first-order DPA protection strategy [25,26], here is not one by one description, but the prevalence of the following problems:

(1) The protection strategy using the product class masking technique does not satisfy the independence, that is, the intermediate value of the algorithm is not completely independent from the median value of the mask. When the intermediate value is 0, the mask has zero value , Vulnerable to zero DPA attacks. We also can see that the combination of the Boolean mask and the product mask also has the risk of being attacked by zero-value DPA [27].

(2) Mask reuse problem, mainly including three cases. The first case is the same mask and multiple intermediate values; the second case is the same mask for multiple encryption operations; the third case is in the arithmetic operation and Boolean operations using the same mask. The above three cases will be different degrees by the first-order DPA method of attack.

Therefore, when the mask scheme does not satisfy the independence or some error occurs in the concrete realization, the first order DPA attack can carry on the key crack. In order to deal with the first-order DPA attack defense strategy, the attacker proposed a second-order DPA attack, attacking the masking technology through some kind of joint leakage.

3.2 Anti-second-order DPA Attack Protection Strategy

A second-order DPA attack is an attacker who can predict two intermediate values during attack and can use both predictions in an attack. The anti-second-order side-channel attack protection strategy is a second-order DPA attack on the characteristics of the equipment protection strategy. At present, there are few researches on the protection strategy of the second-order side-channel attack in China. The main strategy is to use the two or more different masks to make the attacker unable to crack the key through the second-order DPA attack. Second-order power analysis of the DES algorithm to achieve the program [28] using the same mask associated with the two intermediate value of the joint information disclosure of this feature, through two different random mask to the intermediate value is divided into three , The attacker gets any two intermediate values, due to the different masks, the same can not break the key.

4. Safety Assessment

At present, in the field of side-channel attacks is mainly on the attack methods and protection strategies for a large number of research, in the equipment side-channel safety assessment of less research, for this basic situation, this chapter mainly on the current safety

assessment of the general process of introduction, through Analysis of the current status of the study, lay a solid foundation for future research.

Side-channel safety assessment process: First, the researchers to establish a research model, that is, research equipment model and side-channel adversary model, the more detailed description of the model, the evaluation accuracy will be higher;The evaluation index must be able to effectively reflect the safety performance of the equipment, the current use of more include: success rate, signal to noise ratio, sample size, guess entropy, etc. Finally, the first two steps in the basis of the first two steps On the establishment of side-channel safety assessment model, and the feasibility of the model to verify. Throughout the assessment process, the assessment of indicators has been an important factor affecting the quality of the assessment system, the following we present the more popular assessment of the indicators outlined.

① Success Rate, refers to the specific adversary environment, the success of the correct crack the probability of the target device key, the advantage is more effectively reflect the equipment side-channel safety performance, but the need for a large number of side-channel attack experiments, resulting in more Accurate data values.

② SNR is the ratio of the signal component to the noise component in a measurement. In the side-channel analysis attack, the signal-to-noise ratio represents the ratio of the available information to the total information when the target device runs the encryption algorithm. Can be more objective to reflect the side-channel information security equipment.

③ Sample Size, refers to the specific side-channel environment, based on the attack on the opponent to crack the key required sample size. The larger the sample size, the higher the cost of cracking the key.

④ Guess Entropy, refers to the side-channel rivals in the equipment after the attack, still need to complete the workload, the greater the workload, indicating the higher the safety of equipment side-channel, the greater the cost of the attack.

⑤ Mutual Information, specifically the introduction of mutual information game theory into the product design and attack side of the decision-making process, combined with mutual information quantification method, the security of information equipment assessment.

5. Conclusion

At present, the encryption algorithm is divided into two categories, one is the common key system, the typical algorithm AES, DES, etc .; one is the public key system, the typical algorithm ECC, RSA and so on. In this paper, a brief overview of the side-channel attacks related to the above four encryption algorithms is presented. It is found that the attacks are mainly related to key-related operations in the encryption algorithm, including subkey generation operations, subkey encryption operations, and public key Key and private key generation operation.

In this paper, the defense strategy of anti-DPA attack is summarized, and the security vulnerabilities of masking technology are analyzed. The next step is to study the anti-high-order DPA of information equipment. Attack strategy to lay the foundation.

At present, there are few researches on safety assessment in the field of side channel energy analysis, this paper summarizes the evaluation process and summarizes the current popular evaluation indexes, and paves the way for the next stage of safety evaluation system.

References

[1] Kocher P, Jaffe J, Jun B. *Differential power analysis* [G].LNCS 1666:Proceeding of CRYPTO(),Santa Bartara, California,USA, Springer, 1999:388-397

[2] Miró Bonet Margalida. *Conceptual models:a power strategy with professional implications.*[J]. Enfermeria Clinica,2010,20(6)

[3] Poussier R, Grosso V, Standaert F X. *Comparing Approaches to Rank Estimation for Side-Channel Security Evaluations*[M].Smart Card Research and Advanced Applications.Springer International Publishing, 2015

[4] Fang M, Kai-Yong X U, Yang T C.*AES intermediate variables vulnerability recognition based on side channel attacks*[J]. Application Research of Computers, 2013, 30(5):1536-1539 (In Chinese)

[5] Priyadarshini Patil,Prashant Narayankar,Narayan D.G.,Meena S.M.. *A Comprehen -sive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blow -fish*[J]. Procedia Computer Science,2016,78

[6] David Smekal,Jakub Frolka,Jan Hajny. *Acceleration of AES Encryption Algorithm Using Field Programmable Gate Arrays*[J]. IFAC PapersOnLine,2016,49(25)

[7] H Siregar,E Junaeti,T Hayatno. *Implementation of Digital Signature Using AES and RSA Algorithms as a Security in Disposition System* [J]. IOP Conference Series: Materials Science and Engineering,2017,180(1)

[8] Huang L Y. *Principle and simulation of differential power analysis attack based on AES encryption device*[J]. Information Technology, 2013 (In Chinese)

[9] GM Deng，Q Zhao，P Zhang，KY Chen.*Cache Hit Side Channel Attack Based on AES*[J].Computer Engineering,2008 (In Chinese)

[10] Ming Li. *Decryption New to AES – a Side Channel Analysis*[J]. Journal of Xingtai Polytechnic College, 2009 (In Chinese)

[11] Jing Li, Lin-Sen Li. *Differential Power Analysis Method for DES Encryption in IC Card Chip*[J]. Computer Engineering, 2013, 39(7):200-204 (In Chinese)

[12] Lin K C, Deng G M, Zhao Q. *A Method of Side Channel Collision Attack Based on DES*[J]. Modern Computer, 2011 (In Chinese)

[13] Guo J, Yan Y, Yu J.*On Side Channel Collision Attack Against DES Cryptogra -phic Algorithm Implemented with FPGA*[J]. Computer Applications & Software, 2014 (In Chinese)

[14] Ji Hong Lian,Kai Chen. *Implementation of DES Encryption Algorithm Based on FPGA and Performance Analysis*[J]. Applied Mechanics and Materials,2012,1503 (130) (In Chinese)

[15] Xue Mei Li,Li Li. *Implementation of the DES Algorithm on EDA Box*[J]. Applied Mechanics and Materials,2013,2418(325) (In Chinese)

[16] Chen C S, Wang T, Zheng Y Y.*Timing Attacks and Defenses on RSA Public-key Algorithms*[J]. Computer Engineering, 2009, 35(2):123-125 (In Chinese)

[17] Chen C S, Tao W, Guo S Z.*Research on Trace Driven Data Cache Timing Attack Against RSA*[J]. Chinese Journal of Computers, 2014 (In Chinese)

[18] Kunal Gagneja,John Singh. *Survey and analysis of security issues on RSA algorithm for digital video data*[J]. Journal of Discrete Mathematical Sciences and Cryptography,2016,19(1)

[19] Kunal Gagneja,John Singh. *Survey and analysis of security issues on RSA algorithm for digital video data*[J]. Journal of Discrete Mathematical Sciences and Cryptography,2016,19(1)

[20] Vuillaume C, Endo T, Wooderson P.*RSA key generation: new attacks*[M]. Constructive Side-Channel Analysis and Secure Design.Springer Berlin Heidelberg, 2012:105-119

[21] R. Rajaram Ramasamy,M. Amutha Prabakar,M. Indra Devi,M. Suguna. *Knap -sack Based ECC Encryption and Decryption*[J]. International Journal of Network Security,2009,9(3)

[22] Bauer A, Jaulmes E, Lomné V.Side-Channel Attack against RSA Key Generation Algorithms[M].*Cryptographic Hardware and Embedded Systems – CHES 2014*. 2014:223-241

[23] Zhang P, Chen K Y, Zhao Q. *The Classified Technique of ANN for SEMA Attack against ECC on PDA*[J]. Microelectronics & Computer, 2006, 23(11):137-139 (In Chinese)

[24] Lang Li, Yang L, Ken-Li Li.*Research on side-channel attack methods of ECC*[J]. Application Research of Computers, 2013, 30(3):889-890 (In Chinese)

[25] Cui X, Li R, Wei W.*A Hardware implementation of DES with Combined Counter -measure ASgainst DPA*[C].International Conference on Asic. IEEE, 2013:1-4 (In Chinese)

[26] Wang C W, Yuan L, Ding G L.*Pretection Technique of Anti DPA-attack Circuit Based on FPGA Platform*[J]. Modern Electronics Technique, 2010 (In Chinese)

[27] Trichina E, Seta D D, Germani L. *Simplified Adaptive Multiplicative Masking for AES*[C].Cryptographic Hardware and Embedded Systems - CHES 2002, International Workshop, Redwood Shores, Ca, Usa, August 13-15, 2002, Revised Papers. DBLP, 2002:187-197

[28] Cao Kai,Lu Hai-ning,Deng Feng,gu Da-Wu,*A Des Implementation Against Se -cond Order Power Analysis*[J],Information Technology,2015(12):38-41 (In Chinese)