Study on the efficiency and fault tolerance of block cipher algorithm based on energy analysis

Hao Wang

Changchun University of science and technology

Abstract

Block cipher is one of the most widely used cryptographic systems. It is a kind of symmetric cipher algorithm, which uses the same key for encryption and decryption. In essence, the block cipher is a permutation with a key, which divides the data into groups with equal length and is converted to the same length. At present, the main block cipher algorithm has high security, it is difficult to be mathematically analyzed. However, the mathematical analysis method is mainly aimed at the analysis of the text and the cipher text, and has some limitations in the security analysis of the encryption device. Since (1) is proposed to study the operating time of timing attacks since, side channel attack and defense has gradually become the cryptography is one of the important branches. Unlike the traditional brute force crack, or the account of the weakness of the password theory, the side channel attack analysis of the password algorithm to the physical realization of the process of certain intermediate values of the leakage of information, thus obtaining the key. Time, electromagnetic wave, and even sound can be used as the side channel information of the attack code system. In addition, the energy consumption analysis is one of the most effective means of side channel attack.Attackers usually want to attack as fast and efficient as possible, we use this as the starting point to propose a more flexible based on the two - step distance of the bit collision attack, which uses the energy track distance model and the idea of a bit by bit. Take the algorithm as an example, select a full zero express and a special expressly factory each strictly contains a wide range of the same byte, the second is, the other bits are. And key of XOR box input values were obtained, each box of the input value is the change of key bytes of the bit and the Hamming weight before and after the operation also change. Due to input the corpse does not cause any bit change and therefore input tightly, through the comparison of different box input value of Hamming weight difference whether and input the same, you can infer the corresponding key bytes of the bit is equal.Therefore, under the different energy analysis, the different structures of the box of the anti - attack. The design of the algorithm can be considered in the case of different attack method in the case of the security strength to meet specific needs.

Keywords

block cipher; energy analysis; collision attack; fault tolerance attack.

1. Introduction

Research on the objective law of cryptography password change, has a long history. In the ancient times of war, people used the secret letters and special symbols to convey the news. These letters and symbols are the embryonic form of the code. Along with the popularization of the password and the research of the password, the password is more and more attention. In many famous historical events, it is very important to decipher the password information successfully. For example, in the Second World War, the United Kingdom to decipher the German side of the password, the password, this incident prompted the United States to Germany war, and thus achieved a comprehensive victory in the war of two. From another point of view, this historical event also illustrates the importance of communication security. In cryptography, the original information is known as the text, and the text is converted to the form which is not readable. This conversion process is called encryption, and decryption is the inverse operation of encryption. In the 21st century, a thought for a good password system, even if the attacker knows the password algorithm used, as long as the key is not compromised, the password system should be safe. This idea is called principle.

Energy analysis is one of the most effective side channel attack methods, and the other information such as electromagnetic frequency, frequency and even sound can be used to analyze the security of cryptographic devices. Energy analysis is not the mathematical characteristics of the cryptographic algorithm, but the energy consumption in the process of running the code. The instantaneous energy consumption of cryptographic devices depends on the data and the corresponding operation, which is the basic idea of the power analysis attack.

In addition, the combination attack is one of the research hotspots in the side channel attack,. A combination of multiple side channel attack methods is proposed, and they are combined to attack and energy analysis. And the energy analysis attack and the electromagnetic attack attack are combined and the related template induced attack is put forward. The research found that side channel attacks can also be combined with the method of mathematical analysis.

Because of the rapid development of information technology, the security analysis of cryptographic devices has important practical significance. This paper focuses on the problem of fault tolerance and efficiency of block cipher algorithm based on the energy analysis.

2. Preparatory knowledge

1.This chapter briefly introduces the background knowledge and related tools, which mainly include the introduction of block cipher, cipher device, the knowledge of energy trace, and several methods of energy analysis.

2.The block cipher is a kind of symmetric cipher algorithm, which divides the data into a group of multiple equal lengths, and uses the determined encryption and decryption algorithm to deal with the packet data.

3.Cryptographic devices for storing keys and implementing cryptographic algorithms. Cryptographic devices are composed of a number of components that can be divided into two major categories: the components of the password operation and the components of the storage password operation data. Important components, including special cryptographic hardware and the universal hardware and software password, memory and interface, these parts can implemented using a cryptographic chip combination, also can only by virtue of a single password chip to achieve. Currently common single chip password devices have smart cards, tokens, etc..

4.Intrusion type attack. Requires an attacker to disassemble the password device, direct access to the password module or device components. Semi intrusive attack. Also need to disassemble the password device, but in addition to the authorization interface, the attacker does not carry out other electronic contact with the device. Non intrusive attack. Requires an attacker to observe the password device's subtle operation, or direct manipulation of cryptographic devices.

5.The essence of energy analysis is to obtain the key by analyzing the energy consumption of cryptographic devices. For different operation and processing data, the energy trail shows that the spike shapes are different. An attacker can use this feature to analyze a specific energy trail, which is called simple energy analysis.

3. Fault tolerant linear collision attack

Construction of feature template template attack, the attack method based on the information disclosure of the cryptographic device data, and the operation of correlation, in the attack process for obtaining the information disclosure the matching template, so as to effectively reduce Milang the search space.

An attacker to calculate Hamming weight of the median value and the corresponding trace energy correlation coefficient, and sorted according to the obtained multiple correlation coefficient of the size of the candidate key value. In the related energy analysis part of the test chain attack, the attacker gets a set of key candidate values, and determines the range of the value of the key to improve the success rate of the attack.

Classification	Leakage model	Matching pattern
"Vertical" attack	Differential energy analysis Correlation energy analysis Mutual information analysis	Template attack Statistical method Mutual information analysis
"Lateral" attack	Algebraic attack	Collision attack

Test chain attack can correct the error caused by the correlation energy analysis part, but if the collision attack part of the error, it will lead to attack failure. In order to recover the key efficiently, an attacker usually wants a chain to contain all the key bytes (i.e., an equation). In the definition of a chain from the beginning of the free variables to the relevant equation is concluded as a path.

In this chapter, the related strengthening collision attack to construct a with fault tolerance chain path, and will allow the link and correlation power analysis combined, the fault-tolerant linear collision attack. In order to reduce the false positives, the key byte candidate values are sorted by correlation energy analysis, and the threshold values are filtered. Finally, the error correction mechanism is used to determine the position of the error, and the search is performed to recover the correct key, which can greatly improve the attack efficiency. Compared with the test chain attack, the fault tolerant linear collision attack is more practical and effective. The experimental data show that the standard deviation of the noise, the success rate of fault tolerant linear collision attack and test chain attack are achieved, and the former is only required to select the number of energy trace required. The value range of the energy trace amount can be adjusted according to the value of the standard deviation of the noise. In the simulation experiment, the influence of partial threshold on the success rate is analyzed, and the range of the threshold is also discussed. Further development of fault tolerant linear collision attack is further extended to a number of symmetric cryptographic algorithms, which can be applied to the crack of a collision attack.

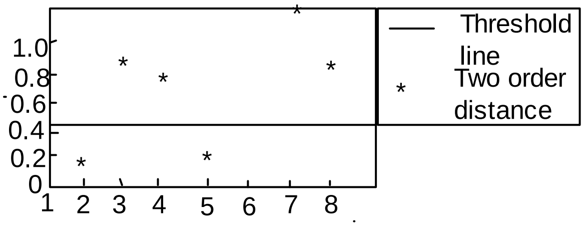
4. Bit collision attack based on two order range

In the CHES2010 meeting, Moradi et al proposed a correlation enhanced collision attack based on hardware implementation, however, their attack method is effective in practical operation. Because of the associated enhanced collision attack by byte, so at least the need to attack the average energy of each attack. During the attack, the attacker needs to carry on the average of the amount of energy trace on the oscilloscope, and then manually storage; or need to store the original energy into the computer, and use the average. The process of collecting, storing, and the average energy trace is too complicated and time consuming. In this chapter, we give a more flexible collision attack, which is based on the energy trace distance model and the bit by bit comparison. In addition, we provide two kinds of distance discrimination models to achieve bit collision attack. The experimental data show that the collision attack based on the two order range is more effective than that of the related enhanced collision attack. Finally according to the third chapter introduces the fault tolerant linear collision attack, we use bit collision attack tectonic link capacity, improving the fault tolerant linear collision attack for fault-tolerant bit collision attack.

Due to the associated enhanced collision attack (refer section 2.4.3) at least 256 energy trail, so in the actual operation of the need to spend more time. We use the Agilent oscilloscope to collect the original energy trace, then calculated an average trace of energy. Data is stored in a computer by a low performance oscilloscope.

We use the model to build the experimental environment for AT89S52 cryptographic chip, and use the Agilent oscilloscope to collect the original trace of energy. For each of the average energy traces, the average operation of the original energy trace is collected, and the sampling points are selected for each energy trail. Experiments are carried out with the first two boxes of the algorithm, taking into account the possible of all the cases, we choose two specific key bytes of experiment.

Based on second-order distance bit collision attack eventually recover dense pot byte XOR value. This result and related strengthening collision attack (the experimental map denoted by) attack the same result. Strengthen the collision attack requires at least a trace of energy, that is traversing a box of plaintext, the grouped according to intermediate values of the Hamming weight, corresponding to the Hamming weight group includes a 1,8,28,56,56,70,56,28,8,1 a trace of energy. Because of the energy dependence of the model, the information obtained from the group with the number of the number of the energy trace is greatly disturbed by the noise of the Yu Hanming's weight. Bit collision attack only requires an energy trail, the total number of energy traces can be assigned to a group, so in the same noise environment, the interference in the same noise environment is less than that of the enhanced collision attack.

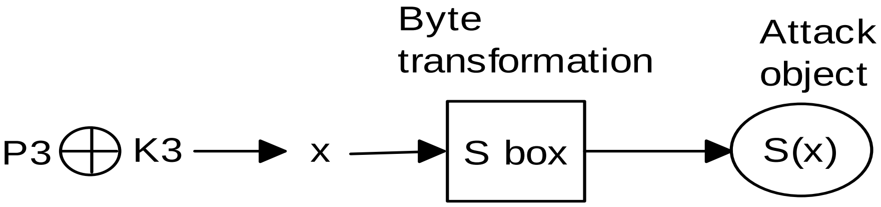


Summary: this chapter gives the basic idea of the first order and two order of energy, and proposes a bit collision attack based on the two order range. This attack can recover the dense steel, and only need average energy trace. We provide two kinds of distance models for attack.

5. Study on the relationship between the box width and power analysis attack efficiency

Block cipher is one of the main stream cipher systems. In the United States federal government's National Standards Agency to determine the data encryption standards for the safety of the federal data processing standards rely on the calculation of the difficulty of the calculation of the algorithm and the time required for a long time. Years, the National Institute of standards and technology research on the began soliciting advanced encryption standard, after several shoe selection algorithm in 2003 was identified as the standard algorithm. In this chapter, we first explain the differences of the three block cipher algorithms, and the main structures and their boxes. Secondly, the thesis studies the efficiency of the three algorithms and the structure of the box, which are respectively related to the energy analysis, the template attack, and the two order range. Simulation experiments are carried out to evaluate the attack efficiency, and to compare the safety strength of the box.

Because of the linear rule of the input data of the block cipher algorithm, the output value of the attacker chooses the box as the research object, and the correlation coefficient of the correct key is different from the correlation coefficient. So the related energy analysis is the output value of the box.



After the establishment of the template, the need for energy and template matching, to find the nearest template. We use a simple template that consists of a mean vector that can be matched by a least square method. Firstly, a clear text is selected randomly, and then the corresponding energy is encrypted and recorded repeatedly, then the average operation is performed to obtain an average energy trail. Using the least square method, the average energy trace and the corresponding box of the full template matching

Summary, this chapter in order to make up for the shortcomings of the mathematical analysis method to assess the safety of the box, using the relevant energy points analysis, template attack and bit collision attack based on the two - step distance, the security assessment of different box structures is carried out. The box structure of the three algorithms is introduced, and the structure of the attack is assumed. Then the main ideas and methods of the simplified template attack are described, and the simulation experiments are carried out on three kinds of attack methods. The success rate of the four kinds of box structures is statistically studied.

6. Conclusion and research plan

This paper focuses on the research of cipher chip in block cipher power analysis attacks, we thought were given than the existing attack methods more effective fault-tolerant linear collision attack and second-order distance bit collision attack, and for three different box structure of the correlation energy analysis and mould plate attack efficiency research. In the third chapter, we construct the link capacity, based on proposed fault-tolerant linear collision attack, and gives an error correction mechanism. Method to construct the link capacity et al test chain based by according to the linear relationship between the specific case and other different box collision attack structure key bytes. Chain advantage lies in its integrity and fault tolerance, it restores all dense steel only need to determine a key bytes as free variables, and can correct errors collision attack. In the link capacity based on, we will the correlation power analysis and related strengthening collision attack with the proposed ratio test chain attack more effective fault-tolerant linear collision attack. Further research plan is as follows:

According to the energy of attack is based on the combination attack with diversity, we in the chain of using only the two energy analysis method of attack. In the follow-up work, we can try to replace the correlation coefficient energy analysis, or with other attack types, to further improve the efficiency of attack. In this paper, we only include the energy analysis of the block cipher system. Because of the elliptic curve and so on, we will carry out the relevant research. Further analysis of the strength of the algorithm, and according to the work we have done, to study whether there is a reliable defense strategy.

Reference

[1] Feng Dengguo, Wu Wenling, Zhang Wentao, block cipher design and analysis of Tsinghua University press, Beijing.

[2] Ceng Yonghong, Ye Xuming anti differential power analysis attack on the box circuit design Computer Engineering].

[3] Zhang Peng, Deng Gaoming, Zou Cheng, differential power analysis attacks in signal processing and analysis of microelectronics and computer.

[4] Li Zhiqiang, Yan Yingjian, a Erpeng differential power attack sample selection method of computer application.

[5] Yan Yingjian, Guo Jianfei, Li Moran and other groups code Hamming weight discrimination function selection method of Microelectronics.

[6]A.shamir,E,Tromer,Acoustic,Cryptanalusis:On Nosy People and Noisy Machine Eurocrypt 2004

[7] Duan Erpeng, Yan Yingjian, Liu Kai for the cryptographic chip attack point selection and application of Computer Engineering.

[8] Wu Wenling, Feng Dengguo, announced on America Qing Si Han, a candidate of software algorithm.