Journal of Electronics and Information Science (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2022.070201
ISSN 2371-9524 Vol. 7 Num. 2

Research on the information security detection technology about encryption chips in automotive environment

Ruiqing Zhai[a, *], Xuebin Shao[b], Rui Zhao[c]

CATARC Software Testing (Tianjin)Co.,Ltd., Tianjin, 300000, China

[a]zhairuiqing@catarc.ac.cn, [b]shaoxuebin@catarc.ac.cn, [c]zhaorui@catarc.ac.cn

*Corresponding author: zhairuiqing@catarc.ac.cn

Keywords: Automotive security chips, security scenarios, fault injection, security advice

Abstract: With the continuous development of intelligent and connected automotive technology, information security issues have become more and more frequent, including remote attacks, network security, and physical manipulation. The automotive security chip is the most basic security foundation for the information security of the intelligent networked vehicle, and its security and encryption vulnerabilities are the most concerned points for the defenders. Security encryption chip testing technology has become increasingly mature through many years, especially the recent years. The encryption chip side channel attack and fault injection attack methods have been widely concerned, which has accelerated the development of chip encryption technology. The essential difference between automotive security chips and general security chips lies in the different using environments and application scenarios, which makes differences in testing methods. This paper mainly expounds the development of security chip testing technology and the main differences between automotive security chips and general security chips. This paper focuses on the possible development trend of injection attacks applied to automotive chips, which provides a reference for the testing technology and protection methods.

1. Introduction

The traditional automotive chip refers to the chip which meets the requirements of reliability test and stress failure test under the specified temperature level. With the continuous development of intelligence and networking automotive, the current definition of automotive chips should also meet more requirements. Automotive chips should aim at zero product defects, and should meet the requirements of quality management system standards in the automotive industry. At the same time, automotive chips should meet the functional safety requirements in the entire life cycle. In addition, automotive chips also need to be considered of meeting the security requirements, such as information security and expected functional security.

This paper mainly discusses the information security issues. Based on the understanding of information security, there is a certain difference between the automotive level and the chip level about information security. The information security issues of automotive may cover network security, interface security, key equipment of in-vehicle network, data security, malware, etc. As for the

information security of chips, the main testing methods are side channel attacks and fault injection, which has also become the main issues need to considered. From another perspective, chip security is also an important part of automotive information security. For example, the current default automotive electronic security is based on the EVITA system and the hardware security module (HSM) [1]. In China, it is clearly stipulated that the OBD system must use the automotive security chip that adopts the national secret algorithm to realize identity authentication and data security. It also proposes to use hardware encryption to protect the security of chip assets. The information security of automotive chips has been taken seriously, because the chip is the key node of automotive information security. The information security of the entire vehicle can be guaranteed only by ensuring the security of the chip.

Chapter 2 of this paper introduces the main security threats of automotive chips, and summarizes the trend of side-channel attacks and fault injection attack methods for automotive chips. Chapter 3 proposes the fault injection method of automotive chips for the existing combined fault testing technology in the laboratory, and adopts relevant test analysis to prove the effectiveness of multidimensional fault injection technology of automotive chips. The fourth chapter summarizes the future development of automotive chip information security, and puts forward some suggestions for automotive chip encryption security technology.

2. Top Security Threats to Automotive Chips

In the environment of automotive chips, the security chip is responsible for encryption operations and encrypted storage. We first need to understand the security usage scenarios faced by automotive chips, before understanding the information security issues of automotive chips in detail. From the perspective of reliability, automotive electronic devices must first be able to resist the influence of factors such as high temperature, high humidity and vibration. From the perspective of connected driving, automotive security chips have higher requirements for encryption rates. The chip need to have fast signature verification capability, which affects the security of automotive data exchanges.

2.1 The security features of automotive chips

The security chip includes cryptanalysis and random number generator modules. For example, the requirements for random number generators of automotive chips are very high. The occurrence of a true random number generator is determined by the changes of some physical quantities. In a complex automotive environment, various effects may affect the random number generation, such as temperature, humidity, electromagnetic interference, etc. Therefore, the randomness test of random number generator of automotive chips is also an indispensable part of automotive chips.

Combined with the reliability requirements for automotive semiconductors in the AEC-Q100 standard, it is necessary to carry out relevant testing and verification of security chips.

2.2 The chip's anti-physical attack ability is insufficient

The side channel analysis and fault injection attacks faced by automotive electronic chips are relatively serious threats. In recently, they are also faced with the possibility of multi-dimensional fault injection attacks. Physical attack methods to automotive security chips includes non-intrusive, semi-intrusive, and intrusive methods. Because some physical attack methods can analyze the encryption key of the chip through the operation mechanism of the security chip, the physical attack method of automobile security chip is so important.

a) Side channel attack of chips: There are many types of side channel attacks. According to the different physical characteristics generated during the execution of the cryptographic algorithm, side

channel attacks can be divided into power consumption attacks, electromagnetic attacks, time attacks, sound attacks, cache attacks, etc. According to the classification of the interface used by the attacker, side channel attacks can be divided into Intrusive attacks, semi-intrusive attacks, non-intrusive attacks. Among the many side-channel attacks, the most commonly used is the power consumption attack. Power consumption attack was proposed in 1996 by Paul Kocher [2] et al. Its working principle is to use the characteristic of different power consumption generated by different operations when the cryptographic algorithm is running to obtain key information. Yu Sai et al. [3] built a software-based power consumption acquisition and analysis platform based on the AES algorithm, and studied the preprocessing method of the collected power consumption signal. Combining principal component analysis and support vector machine (SVM) in learning, a PCA-SVM attack method is proposed. The convolutional neural network in deep learning is applied to power analysis to build a convolutional neural network (CNN). In addition to power consumption attacks, electromagnetic attack is also one of the commonly side-channel attack methods to be used. The working principle of electromagnetic attack is to use the electromagnetic information generated during the operation of the cryptographic chip to obtain the key. Time attack is also one of the commonly used side channel attack methods. This attack method utilizes the time difference by different operations in the cryptographic algorithm. The cracking object of this method is usually the public key cryptographic algorithm, and the time curve of the public key cryptographic algorithm is more obvious than that of the block cipher algorithm.

With the development of science and technology, a variety of new side-channel attack methods have emerged in recent years. Coupled with the uncertainty of the operating environment of the cryptographic chip, the security of the cryptographic chip is increasingly threatened.

b) Research progress of chip fault injection:

1) Qiao Yifei from Huazhong University of Science and Technology [4] proposed a clock fault injection attack scheme for the AES encryption algorithm. This method only requires the wrong injection timing, and there is no limit to the number of wrong bytes injected. By adding a glitch in the specified period of the clock signal, the cryptographic circuit violates the timing constraints and makes mistakes. A clock glitch generator is designed for this purpose.

2) Barenghi et al. [5] exploited power changes to attack software algorithm implementations in AES and RSA. The authors demonstrate that embedded processors can be successfully attacked using very cheap equipment.

3) Raphael A et al. used an enhanced electrical fault model of laser-induced infrared drop to simulate laser-induced faults on large-scale circuits [6].

4) Dehbaoui et al. [7] from the University of Montpellier in France conducted electromagnetic fault injection experiments on the AES encryption algorithm implemented by software and hardware on microprocessors and FPGAs respectively; the experimental results show that the electromagnetic fault injection can be changed by changing the electromagnetic fault injection. It takes time to inject faults into each byte of the AES algorithm, and the electromagnetic fault injection may cause the processor to skip the execution of some instructions; it is also found that the electromagnetic pulse fault injection will make the output of the AES algorithm implemented on the FPGA. The ciphertext produces single-bit or multi-bit faults; the author believes that the reason for the above faults may be transient electromagnetic pulses that lead to timing violations of the circuit.

2.3 The need for hardware security modules

In our research, the attacker mainly invades the automotive terminal system through the external threat surface by carrying out the attack and destruction. The external information security threats cover a variety of attack methods, such as eavesdropping attacks, forgery attacks, man-in-the- middle

attacks, unauthorized access, and denial of service attacks. The corresponding methods are used to evaluate the risks to illustrate the framework. applicability. The V2X security chip based on the national secret algorithm will become the main trend of automotive security [8]. With the continuous improvement of chip attack and technology, the demand for HSM on automotive chips is higher and higher [9].

Based on the research progress on fault injection test technology, the failure injection methods can roughly divided by the chip clock, power, laser, electromagnetic, temperature and other aspects

3. Analysis example based on automotive security chip

Based on the analysis of the safety requirements of automotive chips, this paper uses the relevant analysis methods to conduct a multi-dimensional fault injection test. It concludes the multiple fault injection methods in an automotive environment.

The multi-dimensional fault injection test is mainly carried out by two parts. The first part is the part of collecting error information. This part is completed by hardware and software. The software part controls the specific parameters of each fault injection, and the hardware part realizes the error injection. It is controlled by the host computer software to realize the comprehensive injection of laser, electromagnetic and voltage burr. Multi-dimensional fault injection can include many types.

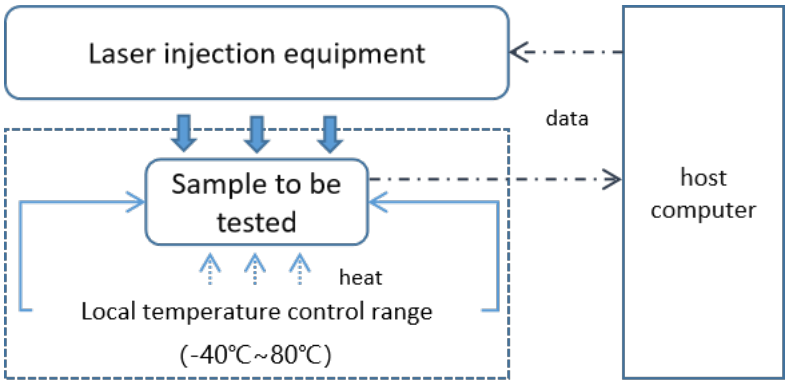

Figure 1: Architecture diagram of multi-dimensional fault injection

After unpacking the chip, we use a microscope to locate the surface area during the normal operation of the chip. We use the device to inject a laser pulse of a suitable size and cause an unexpected errors in the operation of the chip. We can finally analyze the leakage points of sensitive information in the chip. The test environment is shown in the figure.

After two rounds of scanning, the location of the chip vulnerability point found is as follows:

x=2.6, y=5.8
x=2.8, y=5.8
x=3.0, y=5.8
x=2.6, y=6.0
x=2.8, y=6.0
x=3.0, y=6.0
x=2.6, y=6.2

At the above injection point, the chip freezes and then initiates the relay reset.

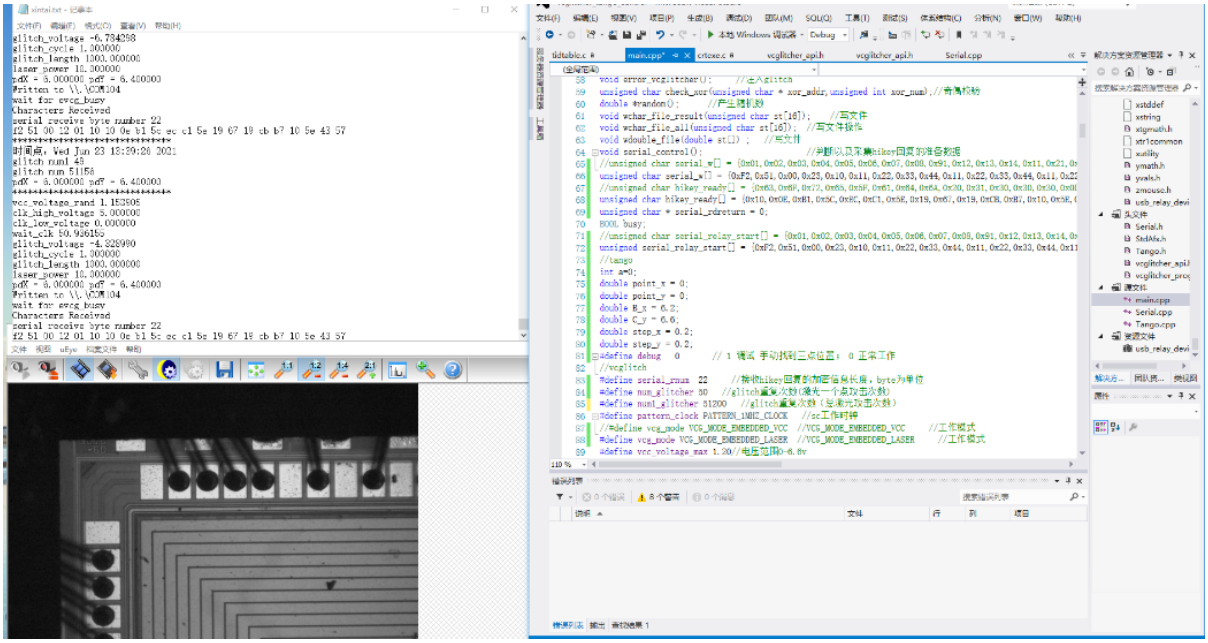

Figure 2: Test Results and Analysis

According to the test results, as the test dimension increases, the number of valid errors exposed by the chip also increases. Therefore, it can be seen that the method of multi-dimensional combined fault injection for chips is effective, which is suitable for safety analysis in complex environments such as automotive environments. It is worth considering adding it to the system of automotive chip safety testing.

At present, with the continuous maturity of the development of fault injection technology, people pay more and more attention to the fault injection methods. Therefore, in the current chip application environment, the fault injection of the chip is more and more difficult to make an error. The multi-dimensional fault injection method proposed by this paper can make the chip fall to error easily.

4. Advice on automotive security chip protection

At present, the relevant security standards for automotive chips are not mature. Although the relevant standards for security chips in the financial and other fields have been completed. But, automotive security chips and financial card IC chips still have different requirements.It seems that they all need to have functions such as security encryption and data protection, however in the current environment of security chips, attacks by some physical means are particularly important. The anti-attack capability of the automotive security chip should be higher than that of the general-purpose security chip. As far as the existing chip application environment is concerned, passing the CC certification is an essential requirement, but the author believes that these are not enough for automotive-grade chips.

Under the different conditions of temperature, the normal operation of the chip must be ensured in the environment temperature range of the automobile grade stipulated by the international regulations. For example, the randomness of the random number generator in the security chip must meet certain requirements to ensure the security of encryption. Therefore, as a car-grade security chip used in automobiles, it must undergo random number generation under high and low temperature and electromagnetic conditions. For another example, although the security chip has passed the security certification in the name of a separate product, its interface state has changed. Therefore, a new side

channel security attack detection must be carried out in the working environment of the chip. In the design stage of automotive security chips, physical attack protection needs to be considered within the design scope. Although some automotive security chips contain some sensors that are resistant to side channel attacks and fault injection, these sensors have not been verified, which resulting in security fails. For the security protection of automotive security chips, this paper puts forward the following suggestions:

Firstly, automotive security chips must have relevant design mechanisms to prevent chip side-channel analysis. From the perspective of chip designers, it is hoped to hide these intermediate information as much as possible. Many chips use methods such as side channel mask defense to avoid side channel vulnerabilities and eliminate algorithm vulnerabilities and information. The hidden danger of leakage has a very effective effect on improving the security of the cryptographic algorithm. As an automotive security encryption chip, it also has related requirements [10]. For example, some chips that record mileage can be easily tampered with by means of side-channel analysis, resulting in some undesirable consequences.

Secondly, the impact of multi-dimensional fault injection testing technology on automotive chip testing needs to be properly considered. Theoretically speaking, the usage scenarios of automotive security chips are diverse and complex. They face a higher range of temperature and humidity, but they also affected by environmental differences such as electromagnetic interference. Error sources are introduced in various ways. Multi-dimensional fault injection is aimed at this point, and it is hoped that based on the general fault injection test method, higher requirements for chip encryption should be put forward.

Finally, it is necessary to carry out the introduction of automotive security chip standards and technical requirements in China quickly. So that, we can provide an important basis for the design of enterprises and the testing of testing institutions.

5. Conclusion

As the key basis for the security application of intelligent networked automotive, security chips need to be widely recognized by automotive industry. Although automotive security chips and financial IC card chips keep pace in the study of encryption and decryption performance. Automotive security chips have richer security features, because its characteristics is directly related to personal safety. So, automotive security chips should have higher security protection levels and security measures than financial IC card chips. Enterprises need to carry out higher-level chip designing, and the automotive industry needs to form a extensive automotive security chip testing mechanism and evaluation system, all of which are the basis for the development of intelligent networked automotive.

References

[1] Sandeep Krishnegowda.Secure Flash,Solutions to Security Issues in Connected Vehicles and Industrial Applications [J]. China integrated Circuit, 2021, 30(06): 45-49.

[2] Kocher F C. Timing attacks on implementations of Diffe-Hellman, RSA, DSS, and other systems [C]. Advances in Cryptology -CRYFTO'96.CRYFTO 19 96. Lecture Notes i n Comput er Science, 1996, 1978: 104-113.

[3] YU Sai. Side Channel Analysis and Implementation Based on Block Cipher Algorithm [D]. University of Electronic Science and Technology of China, 2019.

[4] QIAO Yifei.A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Engineering [D]. Huazhong University of Science & Technology, 2017.

[5] A. Barenghi, G. M. Bertoni, L. Breveglieri, and G. Pelosi. A fault induction technique based on voltage underfeeding with application to attacks against AES and RSA [J]. Journal of Systems and Software, vol. 86, no.7, pp.1864-1878, 2013.

[6] R. A. C. Viera, P. Maurine, J. -M. Dutertre and R. Possamai Bastos. Simulation and Experimental Demonstration of the Importance of IR-Drops During Laser Fault Injection [C]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 6, pp. 1231-1244, June 2020.

[7] Dehbaoui A, Dutertre J M, Robisson B, et al. Electromagnetic transient faults injection on a hardware and a software implementations of AES [C]. 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Los Alamitos: IEEE Computer Society Press, 2012: 7-15.
[8] WANG Xuecong. Research on 5G Internet of Vehicles Security Based on V2X HSM[J]. Information Security Research, 2020, 6(08): 705-709.
[9] ZHAI Teng,Gao Hongling,Guo Qingshuai.Chip hardware security risk analysis and prevention and control suggestions [J]. Industrial Technology Innovation, 2020, 07 (03): 18-23.
[10] WANG Qing, TU Chenyang, SHEN Jiahui. Design and Application of General Framework for Side Channel Attack [J]. Netinfo Security, 2017(5): 57-62.