Advances in Computer, Signals and Systems (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2023.070813
ISSN 2371-8838 Vol. 7 Num. 8

Research on Vehicle Security Chip Application and Testing Based on Fault Injection

Yujia Li[1,*], Hanbing Wu[2], Xianzhao Xia[1], Ruiqing Zhai[1], Mingyang Li[1]

[1]CATARC Software Testing (Tianjin) Co., Ltd., Tianjin, China
[2]China Automotive Technology and Research Center Co., Ltd., Tianjin, China
[*]Corresponding author

Keywords: Security Chip, Vehicle Application, Physical Attack Testing, Fault Injection

Abstract: As an important hardware technology route for cybersecurity, vehicle security chips have been more widely utilized in the automotive field, especially in intelligent and connected vehicles. This paper analyses the technical requirements and application scenarios of vehicle security chips in the automotive environment. Voltage fault injection and electromagnetic fault injection tests are implemented on the vehicle security chip, and its anti-attack ability can be verified on the basis of the test results.

1. Introduction

With the significant growth in the processing of data and interaction of information in intelligent network-connected vehicles, the regulations and standards of various countries have continuously enhanced the requirements for cybersecurity and data security in vehicles. In this regard, the security chip which can provide cybersecurity functions in vehicle, are increasingly applied in the vehicle field. As a technologically mature chip product, there is already a number of studies that are concerned with the physical attacks and protection design for secure chips. However, fewer researches are directed towards the application of security chips in vehicles. This paper investigates the main application scenarios and technical requirements of security chips in vehicles, and proposes test methods using fault injection technology to verify the ability of vehicle security chips to resist voltage attacks and electromagnetic attacks. In this paper, the regulations and standards addressing the vehicle security chip are introduced in Section 2. Then, Section 3 presents the application of security chips in vehicles in terms of typical application scenarios and application technical requirements. The various physical attacks that the security chip may receive are outlined in the fourth section. The test methods and the test result analysis are discussed in Section 5. Finally, Section 6 concludes the paper.

2. Related regulations and standards

A secure chip, also known as a secure cryptographic processor, is a specialized computer-on-a-chip or microprocessor used to perform cryptographic operations. To enable a certain level of resistance to tampering, it is integrated into a package with a combination of physical security protections [1]. As a key foundation for solving the root of trust in cybersecurity, the application of security chips on the vehicle side results from regulations and standards requirements concerning

vehicle cyber-security.

The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) published “UN Regulation No. 155 - Cyber security and cyber security management system” in August 2020, which came into force in January 2021. The regulation requires that from July 2022, cybersecurity will be the latest mandatory requirement for vehicle access in the Europe Union and that all vehicles must be certified for cyber security management systems and vehicle type approval [2]. In China, a number of policy documents have also been released with explicit requests for enhanced cyber security for vehicles. In addition, mandatory national standards for vehicle cybersecurity are being developed, which presents technical requirements and test methods on vehicle cybersecurity. The standard does not limit the technical solutions for information encryption, but proposes corresponding experimental methods for hardware encryption solutions.

3. The application of security chip in the vehicle

3.1. Main application scenarios

The current security chip in the vehicle integration method is divided into two categories: independent security chip and integrated security chip. The research in this paper focuses on the independent security chip.

The security chip has cyber-security protection capability and can provide security functions with complete dedicated cryptographic algorithm module, true random number generator module, environment anomaly detection and processing mechanism, logic anomaly detection and processing mechanism, memory encryption and access control mechanism, in order to enable the protection of keys and other sensitive data, as well as protection of its own code security.

The independent security chip focuses on the application in the networking interface devices of intelligent connected vehicles such as TBOX, V2X OBU, OBD, gateway and front-mounted ETC OBU. Vehicle security chips applied to TBOX usually have functions such as authentication, trusted transmission of communication data, secure start, secure storage, etc. The security chip loaded by the V2X system is mainly utilized for the verification of the legality of the transmitted data and the secure storage of the certificates. The vehicle gateway security chip can satisfy cyber-security requirements such as identity authentication, trusted transmission of communication data, secure boot, secure storage and secure access control. The security chips used in OBD and digital keys are major for identity authentication and trusted transmission of communication data.

3.2. Technical requirements

In terms of environmental reliability, the main reference is AEC-Q100 "Failure Mechanism Based Stress Test Qualification For Integrated Circuits" [3]. The reliability requirements are determined according to the various application environments in which the security chips are used on vehicles. For instance, security chips used in cockpit systems and intelligent driving systems are usually required to achieve Grade 1 (-40℃-125℃), whereas those for body systems can meet the requirements of Grade 2 (-40℃—105℃) or Grade 3 (-40℃—85℃).

In a similar way, the functional safety requirements for automotive security chips are related to the system in which they are applied in the vehicle.

In the aspect of key performance, for security chips applied to the intelligent driving domain, security chips are mainly applied to OBUs (On board Unit), which have a higher demand for processing performance, especially encryption and decryption computing performance and support for high throughput IO channels, as compared to those applied to other systems. If the security chip does not have a fast signature verification capability, the security of the vehicles' data will be

compromised. At present, the internal high-performance symmetric operation of automotive security chips can reach more than 200Mbps level, and the asymmetric operation rate can exceed 10,000 times/second, which can basically satisfy the current requirements of automotive applications. Moreover, future automotive security chips need to gradually improve processing performance according to the development of vehicle application demand on the cyber security. For the cockpit system and the body system in the security chip, its computing performance does not have particularly high-level requirements, but more emphasis on its anti-attack ability as a security chip, in order to prevent intruders from invading the door and central control system by means of cracking.

4. Physical attacks on security chip

Based on whether the chip is damaged by the attack, the physical attack methods of vehicle security chips can be classified as non-invasive, semi-invasive, and invasive.

4.1. Non-invasive attacks

Non-invasive attack is a non-destructive approach to attack since there is a high probability that a chip can continue to work normally after being attacked. The attack process does not necessitate unpacking of the chip or pre-processing of the chip, and the attack can be carried out even when the chip is functioning as normal. Non-invasive attacks on chips can often be carried out inexpensively because the cost of duplicating and updating their necessary equipment is not high [4].

Non-invasive attacks are divided into two categories: active and passive. Passive attacks, alternatively known as side-channel attacks, do not require intervention with the attacked chip and usually just monitor its signals and electromagnetic emissions [5]. Side-channel attacks were first proposed in 1996 by Kocher [6], who successfully recovered RSA's encryption key using a side-channel attack. Side channel attack is an attack on cryptographic circuits to obtain keys by analyzing leakage information such as power consumption, timing information and electromagnetic radiation. It enables the use of physical information such as energy consumption information, electromagnetic radiation information and voltage leaked by the security chip to develop an attack model to deduce information about the cryptographic key, which triggers the leakage of sensitive information [7]. Active attacks, on the other hand, need to impose signals on the attacked chip, including brute force and glitch attacks [5].

The most common non-invasive attack method is the voltage attack. The attack process will be done on the chip's power supply. Low-voltage attacks and over-voltage attacks, both of which can render the chip's protection circuits ineffective or cause the circuit to function incorrectly, so as to take advantage of the circuit's erroneous state to launch an attack on the chip [4]. Even if the chip is equipped with voltage detection circuitry, the chip might still not be able to resist fast transient [5]. The current analysis is a useful non-invasive attack as well. Reversal of data on the bus causes large dynamic power consumption, therefore fluctuations in chip current can be inferred by measuring them using a high-precision analog-to-digital converter [5].

4.2. Semi-invasive attacks

Semi-invasive attacks entail opening the chip package and performing reverse analyses of the data and operational status of the chip based on the collected image signals, optical signals, and other information[4]. It is more difficult of semi-invasive attacks to execute than non-invasive attacks since they necessitate the attacked chip to be unpacked [5]. Compared to invasive attacks, semi-invasive attacks require the opening of the chip package as well, but do not need to remove passivation layers or create internal interconnections. Therefore, are not as expensive as invasive ones and results can

be obtained faster. [8]

The concept of semi-invasive attacks was first addressed in 2002 when optical fault injection attacks were presented. Theoretically, semi-invasive attacks can be carried out with the help of ultraviolet light, X-rays, lasers, electromagnetic fields and localized heat, etc., separately or in combination. Hardware security analyses can be undertaken with semi-invasive methods in post-production testing, where access is not possible through standard means, such as backside imaging and signal detection of flip-chips and modern deep sub-micron devices [5].

4.3. Invasive attacks

Invasive attacks obtain the information stored in the chip by modifying the chip alignment or directly eavesdropping on the bus transmission information. The attack process consists of destroying the chip package by uncovering, drilling and corroding the chip to reveal the die, and then using photographic analysis, reverse engineering, microprobe, focused ion beam (FIB) and other methods [9]. This kind of attack was implemented as early as the 1990s. In 1999, Handschuh et al. used microprobes to observe the address bus during encryption as well as certain storage values in random memory to simply fetch the key [10].

Invasive attack requires extremely specialized knowledge and expensive attack equipment. It can access the information stored within the chip without limitations and reverse compile it. However, it is prone to leaving traces of the attack or even completely damaging the attacked chip. In addition, chip process enhancements and increased design complexity have the effect of rendering the attack more difficult [4].

5. Test verification

5.1. Test methods

Attack testing for vehicle security chips can be divided into two categories: active and passive. When using active attack testing, the input or operating environment of the chip is controlled so that the vehicle secure chip operates abnormally. By analyzing the abnormal behavior of the chip, key sensitive information such as keys inside the chip is obtained. Fault injection is a commonly adopted approach for active attacks. This paper focuses on testing methods for vehicle security chip using fault injection techniques.

5.2. Fault Injection Test

In terms of whether or not there is contact between the fault injection equipment and the test object, fault injection testing can be classified into two types: contact and non-contact. The contact type, also known as the pin-level fault injection method, requires that the chip pins in the circuit be pinned out and the voltage or current on the pins be altered in a certain way, which causes the internal signals to be varied. The non-contact type mainly affects the operation environment of the chip to trigger the internal current and voltage to change in an unqualified manner so that the output signal changes [11]. The following presents the testing on a vehicle security chip using voltage fault injection (contact type) and electromagnetic fault injection (non-contact type).

5.2.1. Voltage fault injection test

In the test process, firstly, the tester completes the parameter setting of the voltage fault injection equipment, then connects the power output of the voltage fault injection equipment to the power supply pin of the security chip test board, and opens the script tool software to run the cryptographic

algorithm. On the one hand, the voltage value of the fault injection is adjusted many times under certain operating time conditions, and the data returned by the cryptographic algorithms are observed for errors when they are run. On the other hand, the voltage value of the voltage fault injection equipment is kept constant, and the operating time of the fault injection is adjusted from minor to major to observe whether there is any error in the data returned during the operation of the cryptographic algorithm.

When the voltage of the fault injection is set to 3.19V and the operating time is 0.5s, the SM4 cryptographic procedure in CBC mode is executed, and the operation result of the chip under test is shown in Figure 1.

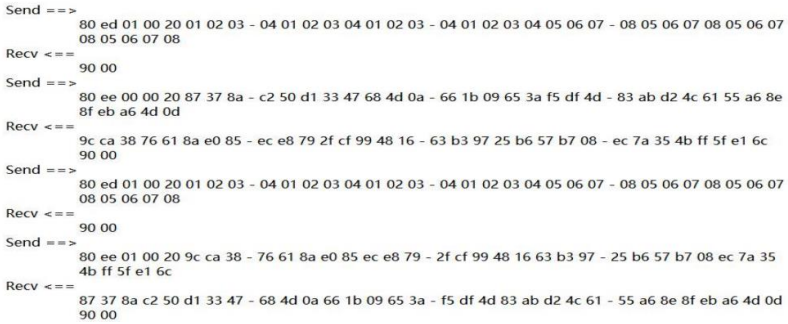

Figure 1: Test result by voltage of 3.19V and operation time of 0.5s.

The fault injection voltage remains unchanged and the operating time is raised to 1.5s, and the test results are presented in Figure 2. It can be noted that it is consistent with the results in Figure 1.

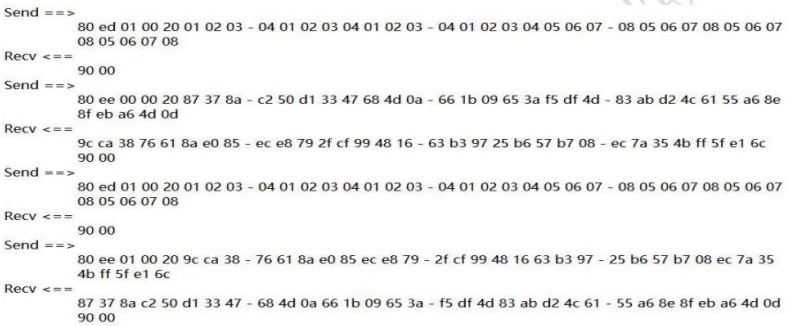

Figure 2: Test result by voltage of 3.19V and operation time of 1.5s.

When the operating time of fault injection is fixed at 0.5s, the voltage of fault injection is set to 3.2, 3.3, 3.4 and 3.5V respectively, and the same encryption and decryption procedure is performed, and the results are the same as those in the above figure.

After several tests, the cryptographic algorithms of the tested vehicle security chip can still function properly under voltage fault injection attacks.

5.2.2. Electromagnetic fault injection test

During the electromagnetic fault injection test, for the test of SM4 algorithm, the SM4 CBC encryption computation and decryption computation are carried out using the standard key, the plain-text data, and the cipher-text data under the normal condition and the electromagnetic injection condition, respectively.

Under normal conditions, the encryption and decryption test is conducted on the chip under test, and the Script Tool is opened to execute the programme. Figure 3 displays the test results.

In order to apply electromagnetic manipulation to the chip under test, the tester uses a precision adjustment frame to fix the circuit board of the tested chip and the magnetic field probe for

electromagnetic fault injection separately, then sets the magnetic field strength settings and adjusts the distance between the electromagnetic fault injection probe and the chip. The tests are carried out and the programme is executed. The test results are as follows (Figure 4). Through comparative analysis, it can be observed that the encryption and decryption operation of the tested chip does not have any abnormality.

```
Send =>
    80 ed 01 00 20 01 02 03 - 04 01 02 03 04 01 02 03 - 04 01 02 03 04 05 06 07 - 08 05 06 07 08 05 06 07
    08 05 06 07 08
Recv <=
    90 00
Send =>
    80 ee 00 00 20 87 37 8a - c2 50 d1 33 47 68 4d 0a - 66 1b 09 65 3a f5 df 4d - 83 ab d2 4c 61 55 a6 8e
    8f eb a6 4d 0d
Recv <=
    9c ca 38 76 61 8a e0 85 - ec e8 79 2f cf 99 48 16 - 63 b3 97 25 b6 57 b7 08 - ec 7a 35 4b ff 5f e1 6c
    90 00
Send =>
    80 ed 01 00 20 01 02 03 - 04 01 02 03 04 01 02 03 - 04 01 02 03 04 05 06 07 - 08 05 06 07 08 05 06 07
    08 05 06 07 08
Recv <=
    90 00
Send =>
    80 ee 01 00 20 9c ca 38 - 76 61 8a e0 85 ec e8 79 - 2f cf 99 48 16 63 b3 97 - 25 b6 57 b7 08 ec 7a 35
    4b ff 5f e1 6c
Recv <=
    87 37 8a c2 50 d1 33 47 - 68 4d 0a 66 1b 09 65 3a - f5 df 4d 83 ab d2 4c 61 - 55 a6 8e 8f eb a6 4d 0d
    90 00
```

Figure 3: Cryptographic operation result without electromagnetic fault injection.

```
Send =>
    80 ed 01 00 20 01 02 03 - 04 01 02 03 04 01 02 03 - 04 01 02 03 04 05 06 07 - 08 05 06 07 08 05 06 07
    08 05 06 07 08
Recv <=
    90 00
Send =>
    80 ee 00 00 20 87 37 8a - c2 50 d1 33 47 68 4d 0a - 66 1b 09 65 3a f5 df 4d - 83 ab d2 4c 61 55 a6 8e
    8f eb a6 4d 0d
Recv <=
    9c ca 38 76 61 8a e0 85 - ec e8 79 2f cf 99 48 16 - 63 b3 97 25 b6 57 b7 08 - ec 7a 35 4b ff 5f e1 6c
    90 00
Send =>
    80 ed 01 00 20 01 02 03 - 04 01 02 03 04 01 02 03 - 04 01 02 03 04 05 06 07 - 08 05 06 07 08 05 06 07
    08 05 06 07 08
Recv <=
    90 00
Send =>
    80 ee 01 00 20 9c ca 38 - 76 61 8a e0 85 ec e8 79 - 2f cf 99 48 16 63 b3 97 - 25 b6 57 b7 08 ec 7a 35
    4b ff 5f e1 6c
Recv <=
    87 37 8a c2 50 d1 33 47 - 68 4d 0a 66 1b 09 65 3a - f5 df 4d 83 ab d2 4c 61 - 55 a6 8e 8f eb a6 4d 0d
    90 00
```

Figure 4: Cryptographic operation result with electromagnetic fault injection.

6. Conclusions

This paper comprehends the regulations and standards related to vehicle security chips and analyses the main uses of security chips for TBOX, V2X OBU and OBD in vehicles, in order to provide the required cyber security functions such as identity authentication, trusted information transfer, and so on. The technical requirements for security chips for vehicle applications are based on three main aspects: environmental reliability, functional safety and performance. Aiming at the non-intrusive attack that is simpler to implement, this paper adopts the method of fault injection to carry out voltage attack tests and electromagnetic attack tests on the vehicle security chip. By comparing the cryptographic algorithm operation results under fault injection conditions and normal conditions, the corresponding anti-attack capability of the security chip is verified.

Acknowledgements

National Key R&D Program of China (2021YFB2501404).

References

[1] Secure cryptoprocessor, [online] Available: https://handwiki.org/wiki/Secure_cryptoprocessor.
[2] UN Regulation No. 155 - Cyber security and cyber security management system, 2021, [online] Available: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.
[3] Failure Mechanism Based Stress Test Qualification for Integrated Circuits, 2014, [online] Available: http://www.aecouncil.com/Documents/AEC_Q100_Rev_H_Base_Document.pdf.
[4] Zhang Y, Li X, Chen K,et al. Research of hardware Trojan design and differential analysis based on fault injection[J].Journal of Huazhong University of Science and Technology(Natural Science Edition), 2014.DOI:10.13245/j.hust.140415.
[5] Skorobogatov S P. Semi-invasive attacks: a new approach to hardware security analysis [D]. [S. l.]: Citeseer, 2005.
[6] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]//Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1996: 104-113.
[7] Trouchkine T, Bukasa, S ́banjila Kevin, Escouteloup M ,et al. Electromagnetic fault injection against a System-on-Chip, toward new micro-architectural fault models[J]. 2019.DOI:10.48550/arXiv.1910.11566.
[8] Yue C .Research on Vehicle Fault in Remote Diagnosis[J].Times Agricultural Machinery, 2017.
[9] Van Tilborg H C A. Encyclopedia of cryptography and security [M]. Boston, MA: Springer, 2005: 301–307.
[10] Handschuh H, Paillier P, Stern J. Probing attacks on tamper-resistant devices [C]. Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 1999: 303–315.
[11] Brekhov O , Klimenko A .Fault Tolerant ASIC/ULA-Based Computing Systems Testing via FPGA Prototyping with Fault Injection[C]//International Conference on Dependability of Computer Systems.2018.