ISSN: 2688-8645

Research on Security Mechanism and Testing Verification Method of Encryption Chips for Automotive Information Security Components

Ziyi Wang [a], Junjie Xu [b], Zongyao Ji [c], Xuesong Wu *

CATARC Intelligent Technology (Tianjin) Co., Ltd. Tianjin, China

* Corresponding author: Xuesong Wu (Email: wuxuesong@catarc.ac.cn),

[a] wangziyilucky@catarc.ac.cn, [b] xujunjie@catarc.ac.cn, [c] jizongyao@catarc.ac.cn

Abstract

Against the background of the rapid popularization of intelligent connected vehicles, the in-vehicle electronic and electrical architecture is continuously upgraded to domain control and centralization, putting forward higher requirements for information security in links such as in-vehicle data interaction, vehicle-cloud communication, firmware upgrade, and identity authentication. As the hardware root of trust in the in-vehicle information security system, encryption chips undertake key functions such as key storage, encryption and decryption operations, digital signature, secure boot, and communication authentication, and their security directly determines the entire vehicle network and data security capabilities. Starting from the actual application scenarios of in-vehicle encryption chips, this paper systematically sorts out their hardware security architecture, key management system, cryptographic algorithm implementation, physical anti-attack design, and secure communication mechanism, analyzes the typical risks faced by encryption chips in the current in-vehicle environment such as physical attacks, side-channel attacks, illegal interface access, and key leakage, and constructs a comprehensive testing verification method covering functional testing, cryptographic performance, physical security, interface security, and environmental reliability combined with ISO/SAE 21434, national cryptographic algorithm standards, and automotive-grade security requirements. Verified through bench testing and real-vehicle environment, the testing system proposed in this paper can comprehensively identify the security shortcomings of encryption chips and realize quantitative evaluation of security capabilities, providing a systematic technical reference for the selection, development, evaluation, and engineering implementation of in-vehicle security chips.

Keywords

Automotive Information Security; Encryption Chip; Security Mechanism; Key Management; Side-Channel Analysis; Testing Verification; Automotive-Grade Security.

1. Introduction

With the continuous improvement of vehicle intelligence and networking, the number of external interfaces of vehicles and internal network nodes continues to increase, and the information security threats faced by in-vehicle systems are becoming increasingly complex. In recent years, cyber attacks on key in-vehicle components such as ECUs, in-vehicle gateways, and T-BOXs have occurred frequently, and attack methods have gradually evolved from traditional protocol cracking to deep-level directions such as firmware tampering, key theft, identity counterfeiting, and communication hijacking. In this context, relying on software-level

ISSN: 2688-8645

encryption strategies can no longer meet automotive-grade high-security requirements, and hardware-level security protection has become an industry consensus.

Encryption chips, including independent security chips (SE), master chips integrated with HSM modules, and in-vehicle MCUs with built-in hardware encryption engines, are the core basic components of the in-vehicle information security system. They provide underlying trusted capabilities for in-vehicle systems through hardware isolation, non-exportable keys, physical anti-detection, and anti-side-channel attack mechanisms. Encryption chips have become indispensable security support units in scenarios such as in-vehicle Ethernet, CAN FD communication security, OTA secure upgrade, battery management systems, and V2X vehicle-road collaboration.

Although encryption chips are of great importance, systematic research on their security mechanisms in the industry is still relatively insufficient, and testing verification methods also lack unified specifications. Some encryption schemes adopted by in-vehicle components only implement basic algorithm functions, and have obvious shortcomings in key protection strength, physical protection capability, and anti-attack performance, making it difficult to cope with professional attack methods such as fault injection, power analysis, and electromagnetic monitoring. At the same time, existing testing mostly focuses on functional correctness, lacking in-depth mining of security vulnerabilities, and cannot fully reflect the security performance of chips in real in-vehicle environments.

Based on the above problems, this paper systematically sorts out the security mechanisms of in-vehicle encryption chips, analyzes their typical attack surfaces and risk levels, constructs a comprehensive testing verification system integrating function, security, environment, and attack, and verifies the effectiveness of the method through actual test data, providing a complete technical path for the secure development and evaluation of in-vehicle encryption chips. [1]

2. Analysis of Core Security Mechanisms of In-Vehicle Encryption Chips

The security capability of in-vehicle encryption chips is not realized by a single technology, but an in-depth defense system composed of hardware architecture, key management, cryptographic algorithms, physical protection, and secure communication. Various mechanisms cooperate with each other to form a closed-loop security capability from the underlying hardware to the upper application. The core security mechanisms are shown in Table 1.

Hardware security architecture is the foundation for encryption chips to achieve security capabilities. To avoid unauthorized access to sensitive information, the chip usually divides an independent secure execution environment inside, which is strictly isolated from the general computing area. All operations related to keys, signatures, and encryption/decryption are completed inside the security domain, and the external host can only call services through limited instruction interfaces and cannot directly read internal sensitive data. This isolation method fundamentally avoids the risk of information leakage caused by debug ports and bus hijacking. [2]

Key management is the core of the security capability of encryption chips. In in-vehicle systems, once the key is leaked, the entire vehicle security system will face a complete collapse. Therefore, in-vehicle encryption chips generally adopt a full life cycle key management strategy, with strict control starting from key generation. The root key is usually generated by a hardware true random number generator and stored in the secure storage area inside the chip, and is not allowed to be exported in plaintext under any circumstances. During key use, the chip restricts the key call scope through permission control, secure channels, and usage scenario binding. When abnormal access is detected, it will actively trigger the key erasure mechanism to minimize security risks.

ISSN: 2688-8645

Table 1. Core Security Mechanisms of In-Vehicle Encryption Chips

Security Dimension	Core Mechanism	Key Technology	Security Goal
Hardware Security Architecture	Hardware Isolation, Independent Security Domain	TrustZone, HSM Independent Kernel, MPU Memory Protection	Block unauthorized access and ensure secure environment isolation
Key Management Mechanism	Full Life Cycle Key Protection	True Random Number Generation, Key Hierarchy, Hardware Storage, Non-Exportable	Prevent key leakage, tampering, replacement and illegal reuse
Cryptographic Algorithm Mechanism	Hardware Implementation of National/International Algorithms	SM2/SM3/SM4, AES, RSA, ECC, SHA Series	Ensure data confidentiality, integrity, non-repudiation
Physical Anti-Attack Mechanism	Active Defense, Attack Detection and Response	Tamper-Proof Sensor, Voltage/Temperature/Clock Monitoring, Key Self-Destruction	Resist physical detection, fault injection, attack
Secure Communication Mechanism	Authenticated Encryption, Anti-Replay	SecOC, Secure Diagnosis, Encrypted Firmware Upgrade, Two-Way Authentication	Ensure trusted transmission of in-vehicle bus and vehicle-cloud communication

Cryptographic algorithms are the basis for data encryption, identity authentication, and integrity verification. To meet domestic and foreign compliance requirements, automotive-grade encryption chips usually support both national cryptographic algorithms and international general algorithms. Symmetric encryption algorithms are mainly used for efficient encryption and decryption of in-vehicle communication data, asymmetric algorithms are mostly used for identity authentication, key negotiation, and digital signatures, and hash algorithms provide guarantee for data integrity. To resist side-channel attacks, chips usually adopt strengthening methods such as masking, power randomization, and instruction out-of-order at the algorithm implementation level to improve the security of the operation process.

Physical anti-attack mechanism is an important feature that distinguishes in-vehicle encryption chips from ordinary consumer chips. Since in-vehicle components are deployed in an open environment, there is a risk of being disassembled, detected, and attacked, so encryption chips are built with multi-level active defense circuits. By monitoring changes in environmental parameters such as voltage, clock, temperature, and light, the chip can identify attack behaviors such as fault injection, detection, and burr interference in real time, and immediately trigger a security response, including cutting off sensitive circuits, clearing keys, locking chip operation permissions, etc.

Secure communication mechanism transforms encryption capabilities into system-level security capabilities for actual in-vehicle business scenarios. For example, secure boot ensures that firmware is not tampered with, SecOC provides authentication protection for CAN messages, and secure diagnosis and encrypted OTA improve the full life cycle security level of vehicles. These mechanisms together constitute the security service capability of in-vehicle encryption chips for the entire vehicle system.

ISSN: 2688-8645

3. Security Risks and Attack Surface Analysis of In-vehicle Encryption Chips

In practical applications, in-vehicle encryption chips face potential threats from multiple levels such as physical, hardware, interface, and algorithm, and the hazard degrees of different attack methods are significantly different. Combined with the deployment characteristics and attack costs of the in-vehicle environment, typical risks can be divided into different levels, as shown in Table 2.

Table 2. Security Risk Level Classification of In-Vehicle Encryption Chips

Risk Level	Attack Type	Typical Attack Methods	Hazard Consequence
Extremely High Risk	Physical Attack	Detection, Fault Injection, Key Theft, Chip Reverse Engineering	Complete key leakage, collapse of the entire vehicle security system
High Risk	Side-Channel Attack	Power Analysis (DPA), Electromagnetic Analysis (EMA), Timing Attack	Key cracking, failure of communication and data security
High Risk	Interface Attack	Debug Port Cracking, Unauthorized Access, Protocol Bypass	Illegal reading and writing of keys, implantation of malicious firmware
Medium Risk	Algorithm Attack	Weak Implementation Attack, Side-Channel Bypass, Mathematical Vulnerability Exploitation	Encryption failure, data decryption and tampering
Medium Risk	Key Management Risk	Key Export, Unauthorized Use, Update Hijacking, Weak Key	Sensitive data leakage, bypass of identity authentication
Low Risk	Environmental Adaptation Risk	Security Failure under Extreme Temperature, Humidity and Voltage, Insufficient Anti-Interference	Intermittent security abnormality, function degradation

Physical attack is the most threatening attack method to encryption chips. Attackers directly obtain internal chip signals through, microscopic detection, probe measurement, or induce the chip into an abnormal state through voltage burrs, clock disturbances, thereby bypassing security controls to read keys. Once such an attack succeeds, all security mechanisms of the encryption chip will fail, so extremely high requirements are placed on physical protection capabilities. [3]

Side-channel attack is a non-intrusive attack. By analyzing indirect information such as power consumption, electromagnetic radiation, and operation timing of the chip during operation, the internal key is deduced using a statistical model. Due to low attack cost, remote or near-field implementation, and difficult detection, side-channel attacks have become the main realistic threat to current in-vehicle encryption chips.

Interface attacks mainly target the debug ports and communication interfaces of the chip. Some chips do not completely close debug permissions after leaving the factory, or have protocol implementation vulnerabilities. Attackers can bypass security mechanisms through

ISSN: 2688-8645

unauthorized access to achieve malicious operations such as firmware tampering and key reading, causing serious security impacts on in-vehicle components.

In addition, algorithm implementation defects, key management strategy omissions, and reduced security capabilities in extreme environments may also become attack breakthroughs, making encryption chips unable to achieve expected security goals.

4. Security Testing Verification Method System of Encryption Chips

To comprehensively, objectively, and quantitatively evaluate the security capabilities of in-vehicle encryption chips, this paper constructs a comprehensive testing verification system covering five dimensions: function, performance, security, environment, and attack, realizing a complete evaluation from basic functions to in-depth security vulnerabilities.

The entire testing system is composed of an encryption chip bench, side-channel analysis equipment, fault injection platform, environmental test chamber, and data collection system, which can support non-intrusive, semi-intrusive, and intrusive multi-type testing items, with reproducible testing processes and quantifiable results.

Table 3. In-Vehicle Encryption Chip Security Testing Evaluation Index System

Testing Category	Core Indicator	Qualification Standard	Weight
Key Security	Key Non-Exportable Rate, Attack Self-Destruction Response Time, Storage Encryption Strength	100%, <10ms, ≥256 bits	25%
Algorithm Security	Algorithm Compliance, Random Number Pass Rate, Side-Channel Protection Capability	100% compliant, pass NIST, no key leakage	20%
Physical Security	Anti-Fault Injection Success Rate, Anti - Success Rate, Physical Attack Survival Rate	0% attack success, 100% protection	20%
Interface Security	Unauthorized Access Rejection Rate, Debug Port Lock Rate, Security Authentication Pass Rate	100%, 100%, 100%	15%
Performance and Environment	Algorithm Throughput, Delay, Security Function Integrity Rate after Environmental Test	≥100Mbps, <5ms, 100%	15%
Compliance	Compliance with National Cryptographic/ISO/Automotive-Grade Standards	All items compliant	5%

In functional security testing, it mainly verifies whether the basic security mechanisms of the chip are normally implemented. Including whether key generation, storage, call, update, and destruction comply with security strategies, whether secure boot can effectively block the startup process when firmware is tampered with, whether debug ports are completely locked, and whether SecOC secure communication can resist message replay and tampering attacks. [4]

Cryptographic algorithm and performance testing mainly verifies the correctness and efficiency of algorithm implementation. The testing content includes whether encryption/decryption, signature/verification functions of algorithms such as SM2, SM3, SM4, AES, and ECC are normal,

ISSN: 2688-8645

whether the random number generator meets NIST standards, and whether algorithm operation throughput, delay and other indicators meet in-vehicle real-time requirements.

Physical security and side-channel testing are the core content of in-vehicle encryption chip testing. Through DPA power analysis and EMA electromagnetic analysis, verify whether the chip has key leakage risk under a large number of operation traces; through fault injection methods such as voltage burrs and clock interference, test the chip's anomaly detection and response capabilities; at the same time, simulate scenarios and tamper prevention to verify the effectiveness of physical protection mechanisms.

Automotive-grade environmental reliability testing faces actual in-vehicle working conditions, verifying the stability of the chip's security functions under environments such as temperature cycling, damp heat, vibration, shock, and electromagnetic interference, ensuring that security mechanisms do not fail or keys are not abnormally leaked under extreme conditions.

To achieve a unified evaluation of test results, this paper establishes a quantitative index system, comprehensively scoring from key security, algorithm security, physical security, interface security, environmental reliability and other aspects, as shown in Table 3.

The overall testing is carried out according to the process of document review, baseline testing, functional testing, attack testing, environmental testing, and comprehensive scoring, and finally forms a complete test conclusion and security improvement suggestions. [5]

5. Testing Verification Results and Analysis

To verify the effectiveness of the proposed testing system, three typical automotive-grade encryption chips are selected for comparative testing, including domestic independent SE chips, chips integrated with HSM modules, and general integrated encryption engine MCUs, with a total of 420 testing use cases covering all dimensions of function, security, and environment. The test results are shown in Table 4.

Table 4. Comparison of In-Vehicle Encryption Chip Test Results

Testing Indicator	Chip A (Domestic SE)	Chip B (HSM)	Chip C (Integrated Encryption)
Key Security Score	98.5	92.3	81.6
Algorithm Compliance	100% (All National Cryptographic Items)	100% (International)	90% (Partial National Cryptographic)
Side-Channel Protection	No Key Leakage (Pass)	Slight Leakage (Warning)	Obvious Leakage (Fail)
Fault Injection Protection	100% Interception, Key Self-Destruction	90% Interception, Partial Self-Destruction	65% Interception, Protection Failure
Environmental Security Integrity Rate	100%	98%	92%
Comprehensive Security Score	96.8 (Excellent)	89.4 (Qualified)	78.2 (Unqualified)
Testing Coverage	94.6%	93.8%	91.5%

The test results show that independent security chips have the most prominent performance in key protection, physical protection, national cryptographic compliance, and anti-side-channel attack capabilities, and can meet the needs of in-vehicle high-security scenarios. Integrated

ISSN: 2688-8645

HSM chips have balanced overall performance but have certain shortcomings in side-channel protection. Although ordinary integrated encryption schemes can achieve basic encryption functions, they are obviously insufficient in physical security, key protection, and anti-attack capabilities, and are difficult to apply to key security components such as in-vehicle gateways, domain controllers, and T-BOXs.

The overall testing process shows that the testing system constructed in this paper can effectively distinguish the security levels of different chips, accurately identify security weaknesses, and has strong engineering practical value.

6. Conclusion and Prospect

Focusing on encryption chips for automotive information security components, this paper systematically analyzes five core security mechanisms: hardware security architecture, key management, cryptographic algorithms, physical anti-attack, and secure communication, sorts out typical threats such as physical attacks, side-channel attacks, and interface attacks, and constructs a comprehensive testing verification system covering function, performance, security, environment, and attack.

Actual testing verification shows that this testing system can comprehensively and quantitatively evaluate the security capabilities of in-vehicle encryption chips, accurately identify security vulnerabilities and shortcomings, and provide a scientific basis for chip selection, product development, and standard formulation. At the same time, the test results also show that independent SE chips and HSM modules are significantly better than general integrated encryption schemes in security strength, and are better choices for key in-vehicle components.

In the future, lightweight anti-side-channel algorithms can be further optimized for automotive-grade environments, multi-chip collaborative security testing can be carried out, research on security chip evaluation methods in vehicle-cloud integrated scenarios can be conducted, and the formation of a unified industry testing specification for in-vehicle encryption chips can be promoted to continuously improve the underlying hardware security capabilities of intelligent connected vehicles.

References

[1] ISO/SAE 21434. Road vehicles—Cybersecurity engineering. 2021.

[2] GM/T 0008-2012. Cryptographic Testing Criteria for Security Chips. 2012.

[3] GB/T 32960.2-2025. Technical Specifications for Remote Service and Management System of Electric Vehicles. 2025.

[4] State Cryptography Administration. Technical Requirements for Cryptographic Application of In-Vehicle Information Security. 2024.

[5] China Automotive Technology and Research Center Co., Ltd. White Paper on Automotive Security Chip Application Fields. 2025.