

# Opportunities and challenges for commercial encryption applications in the Internet of Vehicles

Yuning Li<sup>1, 2</sup>, Kaitian Li<sup>1, 3</sup>, Xiuli Zhang<sup>1, 2</sup>

<sup>1</sup> China Automotive Technology and Research Center Co., Ltd. Tian Jin, China

<sup>2</sup> CATARC Software Testing (Tianjin) Co., Ltd, China

<sup>3</sup> China Auto Information Technology (Tianjin) Co., Ltd. Tian Jin, China

## ABSTRACT

The rapid development of vehicle networking technology has brought broad opportunities for commercial encryption applications, but it is also accompanied by many challenges. As an important guarantee for the information security of the Internet of vehicles, commercial encryption applications have obtained significant development opportunities in terms of technological innovation, market demand and policy support. However, the commercial encryption applications of connected vehicles are also facing challenges such as technical difficulties, lack of standardization, and increasing security threats. This paper aims to deeply analyze the opportunities and challenges of the commercial encryption application of the Internet of vehicles, and put forward corresponding development suggestions, in order to provide reference for the security development of the Internet of vehicles industry.

## KEYWORDS

Vehicle networking; Commercial encryption applications; Opportunity; Challenge; Technological innovation; Market demand; Policy support; Technical difficulties; Standardization; Security threat

## 1. INTRODUCTION

As an important part of intelligent transportation system, vehicle networking realizes the goal of intelligent transportation through the information interaction between vehicles and vehicles, vehicles and infrastructure, vehicles and pedestrians. However, with the wide application of vehicle networking technology, the problem of information security has become increasingly prominent. As a key technology to ensure the security of vehicle networking information, commercial encryption applications are facing huge opportunities and challenges [1].

With the rapid development of information technology and the continuous evolution of intelligent transportation systems, vehicle networking, as a key link connecting vehicles, infrastructure and pedestrians and other transportation elements, is gradually becoming an important engine to promote the development of intelligent transportation. Vehicle networking greatly improves the safety, efficiency and comfort of the traffic system by realizing the information interaction and sharing between vehicles. However, at the same time, the Internet of vehicles is also facing increasingly severe information security challenges. As the core technology to ensure the information security of the Internet of vehicles, the importance of commercial encryption application is self-evident [2].

At present, the commercial encryption application of the Internet of vehicles is ushering in unprecedented development opportunities. On the one hand, with the continuous expansion of the car networking market and the continuous progress of technology, the demand for commercial encryption

applications is increasingly strong, providing a broad space for the development of related industries. On the other hand, government departments attach great importance to the information security of the Internet of vehicles and have introduced a series of policies and regulations to promote the development of commercial encryption applications [3], providing a strong policy guarantee for them.

However, the commercial encryption application of the Internet of vehicles also faces many challenges. First of all, the complexity of the vehicle networking system makes the design and implementation of commercial encryption applications more difficult, and the security of multiple links and equipment needs to be considered comprehensively. Secondly, with the continuous upgrading and complexity of hacker attack methods, commercial encryption applications need to be constantly updated and improved to cope with increasingly severe security threats [4]. In addition, the lack of standardization and standardization also restricts the promotion and application effect of commercial encryption applications.

Therefore, an in-depth discussion of the opportunities and challenges of commercial encryption applications in the Internet of vehicles is of great significance for promoting the security development of the Internet of vehicles industry. This paper will analyze the status quo, development trend and problems of the commercial encryption application of the Internet of vehicles from multiple perspectives, and put forward corresponding suggestions and countermeasures, in order to provide useful references for the further development of the commercial encryption application of the Internet of vehicles.

## **2. OPPORTUNITIES FOR COMMERCIAL ENCRYPTION APPLICATIONS IN CONNECTED VEHICLES**

First of all, with the wide application of vehicle networking technology and the continuous expansion of the market, the demand for commercial encryption applications has shown an explosive growth trend. The functions of information interaction, data transmission and remote control between vehicles require strong encryption technology to ensure information security. This provides a broad market space and development opportunities for commercial crypto applications [5].

Secondly, the promotion of policies and regulations has also brought opportunities for commercial encryption applications in the Internet of vehicles. Government departments attach great importance to the information security of the Internet of vehicles, and have introduced a series of policies and regulations to promote the development of commercial encryption applications. These policies not only provide legal protection for commercial encryption applications, but also provide strong support for its wide application in the field of vehicle networking.

In addition, technological innovation has also brought new opportunities for commercial encryption applications in the Internet of vehicles. With the rapid development of cryptography, artificial intelligence and other technologies, the technical level of commercial encryption applications continues to improve, which can better meet the needs of information security in the Internet of vehicles [6]. The emergence of new encryption algorithms, authentication mechanisms and security protocols has provided more options and possibilities for commercial encryption applications in the Internet of vehicles.

Finally, the user's demand for information security also brings opportunities for commercial encryption applications in the Internet of vehicles. With the frequent occurrence of network security incidents, users are increasingly aware of the security protection of personal information and vehicle data. Commercial encryption applications can provide efficient and reliable information security protection, meet users' needs for information security, and thus improve the overall security of vehicle networking systems [7].

Technological innovation promotes the development of commercial encryption applications: With the continuous innovation of cryptography, artificial intelligence and other technologies, the application of commercial encryption applications in the field of vehicle networking has also been continuously expanded. The emergence of new encryption algorithms, authentication mechanisms and other technologies provides more secure and reliable information protection for vehicle networking. Market demand to promote the popularity of commercial encryption applications: With the continuous expansion of the Internet of vehicles market, users' demand for information security is also increasing. Commercial encryption applications can meet users' needs for information protection, improve the security of vehicle networking systems, and further promote the popularity of commercial encryption applications [8]. Policy support to help the development of commercial encryption applications: Government departments attach great importance to the information security of the Internet of vehicles, and have introduced a series of policies and regulations to promote the development of commercial encryption applications. The implementation of these policies provides a good development environment for commercial encryption applications and promotes its wide application in the field of vehicle networking.



**Figure 1.** Three aspects of opportunities for commercial crypto applications

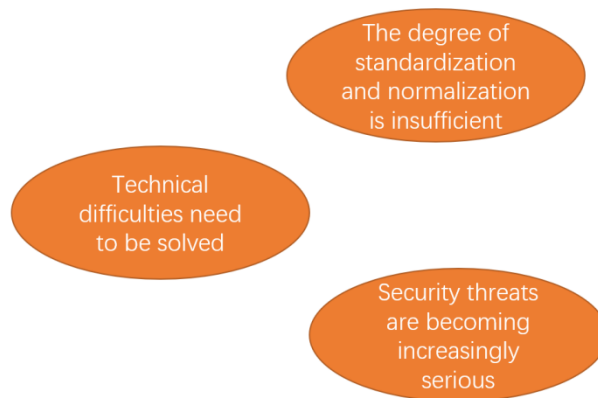
### **3. CHALLENGES IN BUSINESS ENCRYPTION APPLICATIONS FOR CONNECTED VEHICLES**

The technical challenges cannot be ignored. The complexity of vehicle networking system requires that commercial encryption applications can meet multiple requirements such as real-time, high efficiency and stability while ensuring security. However, it is often difficult for existing encryption technologies to take into account the performance cost of the system while ensuring security [9]. Therefore, how to design a secure and efficient encryption scheme is a major technical problem facing the commercial encryption applications of the Internet of vehicles. Automobiles are products with a high degree of internationalization, and some key components come from abroad. Due to the lack of mandatory standards for code application, foreign cryptographic algorithms are mainly used at present. Codes are widely used in communication scenarios such as vehicle internal data encryption storage, data transmission, vehicle and roadside facilities, and cloud platforms, but there are problems. For example, if the broken MD5 and SHA1 algorithms are used, the security cannot be guaranteed because the key length of the RAS algorithm is insufficient.

The issue of standardization and normalization is also one of the challenges facing the commercial encryption applications of the Internet of vehicles. At present, the field of car networking has not yet formed a unified encryption standard and specification, and there are differences in encryption technology between different manufacturers, which may lead to security risks when information interaction and sharing. Therefore, it is an urgent problem to promote the standardization and standardization of commercial encryption applications in the Internet of vehicles and achieve interoperability between different systems.

The increasingly severe security threats are also challenges that the commercial encryption applications of the Internet of vehicles must deal with. With the continuous upgrading and complexity of hacker attack methods, vehicle networking systems are facing more and more security threats. Commercial encryption applications need to be constantly updated and improved to cope with a variety of new attack methods to ensure the security of networked vehicle systems.

Finally, user privacy protection is also an important aspect of Internet of vehicles commercial encryption applications. In the vehicle networking system, vehicle and user information data needs to be properly protected to avoid illegal access and abuse. Therefore, how to achieve effective protection of user privacy while ensuring information security is an important issue that needs to be solved for commercial encryption applications of the Internet of vehicles. Technical problems need to be solved: The complexity of vehicle networking systems makes commercial encryption applications face many technical problems. How to improve encryption efficiency and reduce system overhead while ensuring security is an urgent problem to be solved. Insufficient degree of standardization and standardization: At present, the standardization and standardization of commercial encryption applications in the Internet of vehicles still need to be improved. Technical differences and interoperability issues among different vendors restrict the promotion and application effect of commercial encryption applications [10]. Increasingly serious security threats: With the wide application of vehicle networking technology, security threats such as hacker attacks and data leaks are also increasing. Commercial encryption applications need to be constantly updated and improved to cope with increasing security threats.



**Figure 2.** Challenges for commercial encryption applications

## 4. SUGGESTION AND PROSPECT

In view of the opportunities and challenges faced by the commercial encryption applications of the Internet of vehicles, this paper puts forward the following suggestions, as shown in Table 1:

### 4.1. Seize The Opportunity To Promote The Innovative Development Of Commercial Encryption Applications

Strengthen technology research and development and investment: In view of the complexity and real-time needs of vehicle networking systems, enterprises and research institutions are encouraged to increase investment in encryption technology research and development, and develop more efficient and secure encryption algorithms and protocols. Deepen market application and expansion: Seize the rapid development opportunity of the car networking market, promote the wide application of commercial encryption applications in key links such as vehicle communication, data transmission, and remote control, and explore new application scenarios and business models.

With the rapid development of information technology, the application of commercial encryption has become the core issue in the field of information security. In the current digital and networked era, grasping the opportunity to promote the innovative development of commercial encryption applications is of great significance for ensuring information security and promoting economic development.

First, the innovative development of commercial encryption applications is a necessary means to address information security challenges. In the information society, data leakage, network attacks and other information security incidents occur frequently, bringing huge economic losses and privacy risks to enterprises and individuals. By adopting advanced encryption algorithms and technical means, commercial encryption applications can effectively protect the confidentiality, integrity and availability of data and reduce information security risks. Therefore, promoting the innovation and development of commercial encryption applications is an urgent need to meet the challenges of information security and ensure information security.

Secondly, the innovative development of commercial crypto applications is also an important driver of economic development. With the rise of the digital economy, commercial encryption applications have been widely used in finance, e-commerce, cloud computing and other fields, providing safe and reliable information protection for these industries [8]. By promoting the innovative development of commercial crypto applications, it can further expand its application field, enhance the security and credibility of the digital economy, and thus promote the sustainable and healthy development of the economy.

In order to seize the opportunity and drive innovation in commercial crypto applications, we need to start from the following areas:

First, we will strengthen technological research and development and innovation. Enterprises, universities and research institutions are encouraged to strengthen cooperation and jointly carry out research and development and innovation of commercial encryption technology. Through the introduction of new algorithms, protocols and technical means, continuously improve the security and performance of commercial encryption applications to meet the changing information security needs [8].

The second is to promote standardization and standardization. Develop and improve standards and specifications for commercial encryption applications to promote interoperability and compatibility between different systems. Through standardization and standardization construction, the implementation cost and maintenance difficulty of commercial encryption applications are reduced, and the popularity rate and application effect are improved.

Third, strengthen personnel training and introduction. Increase the training and introduction of talents in the field of commercial encryption, and establish a high-quality and professional team of encryption technology talents. Through talent support, it provides a steady stream of intellectual support and innovation impetus for the innovative development of commercial encryption applications [9].

Fourth, we will strengthen policy guidance and support. The government should introduce relevant policies to increase support for the innovative development of commercial crypto applications. Through financial support, tax incentives and other measures, enterprises are encouraged to increase investment and promote the research and development and application of commercial encryption applications.

In short, seizing the opportunity to promote the innovative development of commercial encryption applications is an important measure to respond to information security challenges and promote economic development. We need to start from many aspects such as technology research and development, standardization construction, personnel training and policy guidance to jointly promote the innovative development of commercial encryption applications, and provide a strong guarantee for information security and economic development.

## 4.2. Address Challenges And Improve The Security Performance Of Commercial Encryption Applications

Strengthen standardization and standardization construction: Promote the standardization process of commercial encryption applications in the Internet of vehicles, formulate unified encryption standards and specifications, promote technical interoperability between different manufacturers, and reduce information security risks. Improve security protection capabilities: In view of increasingly serious security threats [10], strengthen the security protection capabilities of commercial encryption applications, including regularly updating encryption algorithms, improving authentication mechanisms, and strengthening data protection, etc., to ensure the security of vehicle networking systems.

Addressing the challenges and improving the security performance of commercial encryption applications is a critical and urgent task. With the rapid development of information technology, commercial encryption applications are facing increasingly complex and diversified security threats. In order to effectively address these challenges, we need to comprehensively improve the security performance of commercial encryption applications from multiple aspects.

First of all, strengthening the research and development and update of encryption algorithm is the key to improve security performance. With the continuous progress of code cracking technology, existing encryption algorithms may [7] face the risk of being cracked. Therefore, we need to continuously develop new encryption algorithms, improve encryption strength and security, and timely update existing encryption algorithms to cope with potential threats.

Secondly, establishing a sound key management mechanism is an important measure to ensure the security of commercial encryption applications. Key is the core element in the process of encryption and decryption, and its security is directly related to the security of the whole encryption system. Therefore, we need to establish a sound management mechanism for key generation, storage, transmission and use to ensure the security and confidentiality of the key and prevent the key from being leaked or abused.

In addition, strengthening network security protection is also an important aspect of improving the security performance of commercial encryption applications. Commercial encryption applications usually run in the network environment, so the strength of network security protection directly affects the security of encryption applications [9]. We need to take a variety of network security protection measures, such as firewalls, intrusion detection systems, etc., to prevent network attacks and malicious code intrusion, to ensure the transmission and storage of encrypted data security.

At the same time, improving the user's security awareness and operational norms is also a part that cannot be ignored. Users are the main users of commercial encryption applications, and their operational behavior directly affects the security of encryption applications. Therefore, we need to strengthen the security education and training of users, improve their security awareness and operational norms, and avoid security vulnerabilities caused by improper user operations.

Finally, strengthening cooperation and sharing is also an important way to improve the security performance of commercial encryption applications. To improve the security performance of commercial encryption applications requires the joint efforts and cooperation of all parties. We can strengthen exchanges and cooperation with international counterparts, share security technology and experience, and jointly deal with global security threats [9]. In addition, we can also establish close cooperation with upstream and downstream enterprises in the industrial chain to jointly promote the security performance of commercial encryption applications.

### **4.3. Balance Security And Privacy, Enhance User Trust**

Strengthen user privacy protection: When designing and implementing commercial encryption applications, the needs of user privacy protection should be fully considered, and technical means such as anonymization and de-identification should be adopted to ensure the safe and compliant use of user information. Strengthen user education and training: enhance users' awareness and attention to the information security of the Internet of vehicles, and enhance users' safety awareness and prevention ability by holding training courses and issuing safety guidelines [9].

### **4.4. Strengthen Policy Guidance And Supervision To Create A Good Development Environment**

Improve the policy and regulatory system: The government should introduce more policies and regulations to support the development of commercial encryption applications in the Internet of vehicles, clarify the main body of responsibility, regulatory requirements and penalties, and provide legal protection for the development of the industry. Strengthen supervision and law enforcement: Establish and improve the information security supervision mechanism of the Internet of vehicles [10], strengthen the supervision and law enforcement of commercial encryption applications, and ensure the compliance of enterprises and information security.

In order to strengthen policy guidance and supervision, and create a good development environment for commercial encryption applications, we can start from the following aspects: Clear policy orientation, strengthen the top-level design: The government should formulate a clear policy orientation, emphasize the importance and strategic position of commercial encryption applications, and clarify development goals and key tasks [8]. Through the introduction of relevant policy documents, it provides a strong policy guarantee for the development of commercial encryption applications. At the same time, strengthen the top-level design, overall consideration of the technology research and development, industrial application, marketing and other aspects of commercial encryption applications, to ensure the coherence and coordination of policies. Strengthen policy publicity and improve awareness: The government should increase the publicity of commercial encryption applications, and improve the public's awareness and understanding of commercial encryption applications by holding forums [11], exhibitions and other activities. At the same time, strengthen cooperation with the media, timely release the latest developments and results of commercial encryption applications, and create an atmosphere of public opinion conducive to its development. Optimize the regulatory mechanism [9] to ensure compliance development: establish a sound regulatory mechanism for commercial crypto applications, formulate sound regulatory rules and standards, and clarify regulatory responsibilities and authority. Strengthen daily supervision and risk assessment of commercial crypto applications to identify and deal with potential security risks in a timely manner. At the same time, strengthen coordination and cooperation with relevant departments, form a joint force [12], and jointly promote the compliance development of commercial encryption applications. Establish an incentive mechanism to promote innovation and development: The government should establish an incentive mechanism for commercial encryption applications, and encourage enterprises to increase investment and promote research and development and innovation of commercial encryption applications through financial support, tax incentives and other measures. At the same time, support enterprises to participate in international competition and cooperation, introduce foreign advanced technology [9] and management experience, and enhance the international competitiveness of China's commercial encryption applications. Strengthen talent training and introduction: The government should increase the training and introduction of talents in the field of commercial encryption, establish a sound talent training system [10], and provide sufficient talent support for the development of commercial encryption applications. At the same time, strengthen cooperation and exchanges with the international talent market, and attract more

outstanding talents to contribute to the development of commercial encryption applications in China[13].

**Table 1.** Recommendations and prospects for the future

1	Seize the opportunity to drive innovation in commercial crypto applications
2	Address challenges to improve the security of commercial encryption applications
3	Balance security and privacy to enhance user trust
4	We will strengthen policy guidance and supervision to create a favorable environment for development

Looking to the future, with the continuous development of vehicle networking technology and the continuous improvement of commercial encryption applications, the security of vehicle networking systems will be further improved. At the same time, with the continuous emergence of new technologies and the expansion of application scenarios, the application of commercial encryption applications in the field of vehicle networking will also be more extensive and in-depth.

## 5. CONCLUSION

The commercial encryption application of the Internet of vehicles is faced with great opportunities and challenges. By strengthening technology research and development, standardization and standardization work, as well as improving user security awareness and other measures, we can promote the wide application and development of commercial encryption applications in the field of vehicle networking. In the future, with the continuous progress of technology and the continuous expansion of application scenarios, the commercial encryption application of the Internet of vehicles will provide strong support for the security development of the Internet of vehicles industry.

## REFERENCES

- [1] Yang Yang, Yan Hongmei, Pan Shouhua. The application of the commercial passwords in the smart snatched commercial vehicle practice [J]. Journal of automotive electronics, 2021, (9): 9-12 + 15. DOI: 10.13273 / j.carol carroll nki QCDQ. 2021.09.008.
- [2] Wang Haitao. Application of commercial cryptography in the protection of trade secrets of central enterprises [J]. Journal of Beijing Institute of Electronic Science and Technology, 2016, 24(02): 93-96.
- [3] YAO Hailong, Yan Qiao. Cryptanalysis and design of Anonymous Authentication Protocol for value-added Services of Vehicle Networking [J]. Journal of Computer Research and Development, 202, 59(02): 440-451. (in Chinese)
- [4] WANG Rui, Li Zhiqiang, Yao Yingyi. Security Identity Authentication technology for vehicle networking based on domestic commercial password [J]. Information and Computer (Theoretical Edition), 2021, 33(08): 221-223. (in Chinese).
- [5] Chen Hong, Zhao Hongrui. Construction of legal system of commercial code information security with Chinese characteristics from the perspective of national security [J]. Information Security and Communication Security, 2020, (06):29-35.
- [6] Dong Tian, Li Guang, Yang Zhenyu, et al. Power grid enterprise File secret point annotation System Based on Transformer [J]. Journal of jilin university (information science edition), 2021, 33 (6): 6, 720-725. The DOI: 10.19292 / j.carol carroll nki JDXXP. 2021.06.016.
- [7] Application of commercial cryptographic technology in Vehicle networking [J]. Intelligent Connected Vehicle, 2022, (03):28-30.
- [8] LIU Yuan. Application of commercial cryptographic technology in Vehicle networking information security [J]. Network Security and Informatization, 2023, (03):131-134.
- [9] ZHANG Yuegong. Business secret industry ushered in the historical development opportunity [J]. China Information Security, 2019, (11):76-78.

- [10] Wang Yunhao. Performance research and implementation of lightweight cryptographic algorithm in Vehicle networking environment [D]. Beijing university of posts and telecommunications, 2023. DOI: 10.26969 /, dc nki. Gbydu. 2023.002929.
- [11] Him. Car networking communication oriented public key cipher algorithm applied research [D]. University of science and technology of China, 2023. The DOI: 10.27517 /, dc nki. Gzkju. 2023.002056.
- [12] Li Wenhan China. Car networking communication oriented dynamic encryption method research [D]. Lightweight xiking institute, 2023. The DOI: 10.27831 /, dc nki. Gxjxy. 2023.000151.
- [13] WANG Xinming, Cao Yuhan, Du Ke. Network identity authentication key agreement protocol based on SM2 car [J]. Journal of Internet technology, 2024, 14 (3) : 62-65 + 71. DOI: 10.16667 / j.i SSN. 2095-1302.2024.03.015.