Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 14, No. 3, 2024

Accelerate the Promotion and Application of Commercial Cryptography Technology in The Automotive Industry

Yuning Li[1, 2], Kaitian Li[1, 3], Xuebin Shao[1, 2]

[1]China Automotive Technology and Research Center Co., Ltd. Tianjin, China
[2]CATARC Software Testing (Tianjin) Co., Ltd, China
[3]China Auto Information Technology (Tianjin) Co., Ltd. Tianjin, China

Abstract: With the acceleration of the intelligent and networked process of the automobile industry, the problem of information security has become increasingly prominent. As the core guarantee means of information security, the promotion and application of commercial cryptography technology in the automobile industry is particularly important. In this paper, the application status and challenges of commercial cryptography technology in automobile industry are comprehensively analyzed, and the relevant strategies for promotion and application are put forward. By strengthening policy guidance, improving technological innovation capacity, promoting standardization construction and strengthening industry cooperation and exchanges, the aim is to accelerate the popularization and application of commercial cryptography technology in the automotive industry and improve the security protection capability of automotive information systems. The research of this paper is of great significance for promoting the construction of information security in automobile industry and promoting the rapid development of commercial cryptography technology.

Keywords: Commercial cryptography; The automotive industry; Information security; Promotion and application; Safety protection.

1. Introduction

The automobile industry as an important pillar of the national economy, its information level continues to improve, but at the same time, the problem of information security has become increasingly prominent. With its unique encryption, decryption and authentication functions, commercial cryptography provides a strong guarantee for automobile information security. However, at present, there are still some problems and challenges in the application of commercial cryptography technology in the automotive industry, which need to be studied deeply and solved by effective measures. With the rapid development of information technology, the automobile industry is ushering in a new era of intelligence and networking [1]. In this context, the security of automotive information system is particularly important, it is directly related to the normal operation of the vehicle, the user's data security and the reputation and interests of the enterprise. As the core guarantee means of information security, commercial cryptography has multiple functions such as encryption, decryption and authentication, which provides a strong support for the security protection of automotive information system.

However, while commercial cryptography technology has been widely used in other industries, its adoption in the automotive industry has lagged behind. This is mainly due to the lack of recognition of commercial cryptography technology in the automotive industry, the high cost of technology research and development and application, and the lack of standardization and standardization. Therefore, accelerating the promotion and application of commercial cryptography technology in the automotive industry [2] is of great significance for improving the security of automotive information systems and promoting the healthy development of the automotive industry.

This paper aims to deeply analyze the challenges and problems faced by the application of commercial cryptography technology in the automotive industry, and discuss the strategies and methods of its application. Through literature review, case analysis and other methods, this paper will sort out the application status of commercial cryptography technology in the automotive industry, analyze its role and value in the automotive information security, and put forward specific measures and suggestions to accelerate the promotion and application. It is hoped that the research of this paper can provide useful reference for the construction of information security in the automobile industry and promote the rapid development and wide application of commercial cryptography technology in the automobile industry.

Accelerating the promotion and application of commercial cryptography technology in the automotive industry is of great significance, mainly reflected in the following aspects: Improving the vehicle information security protection capability: As the core means to ensure information security, commercial cryptography technology can provide technical support for the terminal security access, secure communication between ECUs and firmware security. This helps prevent security risks such as malicious attacks, data leaks and illegal access, and improves the vehicle's information security protection capabilities. Promoting the digital transformation of the automotive industry: With the acceleration of the digital transformation of the automotive industry, there are increasingly more interaction scenarios between vehicles and external devices, such as vehicle information interaction systems and handheld mobile intelligent terminals, new energy vehicles and charging piles. The application of commercial[4] cryptography technology can achieve secure communication in these interactive scenarios, providing security for the digital transformation of

the automotive industry. Promote the integration of emerging technologies and the automotive industry: Commercial cryptography technology is not only deeply integrated with the Internet of vehicles technology, but also closely related to emerging technologies such as 5G, the Internet of Things, blockchain, and artificial intelligence. Accelerating the promotion and application of commercial cryptography technology in the automotive industry will help promote the integration of these emerging technologies and the automotive industry, achieve business service model innovation, reduce the potential risks of new technology application, and promote the new technology to better serve the automotive industry[5].

Increase consumer trust and satisfaction: The application of commercial cryptography technology can increase consumer trust in intelligent connected vehicles. By adopting cryptographic technologies such as digital certificates and digital signatures, vehicle identity authentication and data encryption are realized to protect the privacy and rights of consumers. This will help increase consumer satisfaction and acceptance of smart connected vehicles and promote their wider application.

Strengthening international competitiveness: In the context of increasingly fierce competition in the global automotive market, the promotion and application of commercial cryptography technology helps to enhance the international competitiveness of China's automotive industry. By mastering core technologies and formulating international standards, China's automobile industry can occupy a more favorable position in the global market and achieve sustainable development.

2. The Application Status of Commercial Cryptography Technology in The Automotive Industry

At present, the application of commercial cryptography technology in the automotive industry is mainly concentrated in vehicle communication, identity authentication, data transmission and other aspects. For example, in vehicle communication, commercial cryptography technology can achieve secure communication between vehicles and vehicles and between vehicles and infrastructure to prevent information from being tampered with or stolen [3]. In terms of identity authentication, commercial cryptography technology can ensure the authenticity of vehicle and user identity and prevent illegal access and operation; In terms of data transmission, commercial cryptography technology can ensure the confidentiality and integrity of data and prevent data leakage and tampering. The application status of commercial cryptography technology in the automotive industry is as follows. This is shown in Table 1, Data leakage may bring serious harm in various aspects, which are reflected in the following aspects:Financial loss: Attackers can use the leaked bank card information or personal account information to steal, so that the victim's funds are stolen, causing no small financial loss. Personal privacy exposure: The disclosure of personal privacy information, such as name, gender, birthday, home address, phone number, email address, etc., may lead to a variety of harassment and even identity theft, which has a serious impact on the victim's personal and family. Disclosure of the company's trade secrets: the company's confidential information, such as product design scheme, financial information, strategic planning, contact information of executives and employee information, once leaked, will seriously damage the company's business interests and reputation. Subject to blackmail and extortion: Attackers will often use coercion or blackmail to get the information they[6] want. Once they succeed in obtaining leakable data, they may intimidate victims into demanding payment or more data. The threat from these attackers is often so serious that victims are forced to pay a huge "ransom." Therefore, both individuals and enterprises need to be highly vigilant to the risk of data leakage and take effective security measures to prevent data leakage events. At the same time, it is necessary to respond and deal with the data leakage event in time to reduce the harm caused by it.

Table 1. Hazards associated with data breaches

Event type	Vulnerability name	Attack type	Coping measures
Data breach	Heartbleed	Man-in-the-middle attack	Update patches and strengthen authentication
Ransomware attack	WannaCry	ransomware	Back up data, update the system, and install antivirus software
DDoS attack	Reflex attack	Distributed denial of service	Deploy DDoS protection devices and optimize the network architecture

First, commercial cryptography technology is widely used in automobile identity authentication and data encryption. With the development of automobile intelligence and network connection, the communication and data transmission between automobile and external equipment are becoming more and more frequent, which makes the security threat of automobile increasingly increasing. Commercial cryptography ensures secure communication between the car and external devices by providing strong encryption and authentication capabilities, preventing data leaks and illegal access [3].

Secondly, commercial cryptography technology is also applied to the security protection of vehicle information systems. The vehicle information system contains various information and data of the vehicle, such as navigation information, vehicle status information and so on. Through commercial cryptography technology, such information can be encrypted and authenticated, ensuring the confidentiality and integrity of information during storage and transmission, and preventing illegal acquisition or tampering.

In addition, commercial cryptography technology is also applied to the security of remote service and management of automobiles. With the continuous expansion of vehicle remote service and management functions, such as remote fault diagnosis and remote software upgrade, these functions need to be transmitted and exchanged through the network. Commercial cryptography can ensure the security of these remote services and management operations, preventing

hackers from exploiting vulnerabilities to attack and disrupt.

At the same time, in the field of new energy vehicles, commercial cryptography technology also plays an important role. Key components such as battery management systems and charging facilities of new energy vehicles need to ensure the security and integrity of data, and commercial cryptography technology provides reliable security for these components [3].

However, although the application of commercial cryptography technology in the automotive industry has made some progress, there are still some problems. For example, some automobile manufacturers do not pay enough attention to commercial cryptography technology and lack sufficient security awareness; At the same time, the development and application cost of commercial cryptography technology is high, which is difficult for some smaller car manufacturers to bear. In addition, the degree of standardization and standardization of commercial cryptography technology needs to be improved, and there is a lack of uniform standards and norms to guide its application in the automotive industry.

Therefore, in order to accelerate the promotion and application of commercial cryptography technology in the automotive industry, it is necessary to increase the attention of automobile manufacturers to commercial cryptography technology, reduce the cost of research and development and application, strengthen standardization and standardization construction, and promote industry-universation-research cooperation to jointly promote the rapid development and wide application of commercial cryptography technology in the automotive industry. As shown in Table 2.

Table 2. Uses of commercial cryptography in several fields

Application field	Application status	Major technology	Typical case
Vehicle communication security	Widely used	Encrypted communication, digital signature	Vehicle-mounted V2X communication encryption solution
Vehicle system security	Gradual promotion	Identity authentication, access control	Vehicle-mounted infotainment system security hardening
Remote service security	Gradual popularization	Remote authentication and security upgrade	Remote vehicle diagnosis and upgrade services

3. Strategies to Accelerate the Application of Commercial Cryptography Technology in The Automotive Industry

1. Increase the attention of automobile manufacturers to commercial cryptography technology

Automobile manufacturers should fully realize the importance of information security to the development of enterprises, and take commercial cryptography technology as an important means to improve the level of information security. At the same time, the government and all sectors of society should also strengthen publicity and education to improve the awareness and attention of automobile manufacturers to commercial cryptography technology.

To improve the attention of automobile manufacturers to commercial cryptography technology, we can start from the following aspects:

Strengthen publicity and education: Through the organization of industry seminars, technical exchanges and other activities, to popularize the importance of commercial cryptography technology and its application value in the automotive industry to automobile manufacturers. At the same time, the media platform is used to publish successful cases and industry trends, and guide automobile manufacturers to pay attention to and understand the development trend of commercial cryptography technology. Formulate policy guidance: The government can issue relevant policies to clarify the importance of automotive information system security and the role of commercial cryptography technology in it, and encourage automobile manufacturers to adopt commercial cryptography technology to improve product security [4]. At the same time, for the use of commercial cryptographic technology for automobile manufacturers, you can give certain tax incentives or financial subsidies. Strengthen cooperation and exchange: Promote automobile manufacturers to establish close cooperative relationships with commercial cryptographic technology providers, scientific research institutions, etc., and jointly develop commercial cryptographic technology solutions suitable for the automotive industry. Through cooperation and exchange, automobile manufacturers can gain an in-depth understanding of the principles, applications and advantages of commercial cryptography technology, so as to increase their attention to it. Establish demonstration projects: Select some representative enterprises in the automotive industry to establish demonstration projects for the application of commercial cryptography technology to demonstrate its actual effect in improving automotive information security. Through the leading and driving role of the demonstration project, it can stimulate the interest and demand of other automobile manufacturers for commercial cryptography technology. Improve standards and norms: Develop and improve standards and norms for the application of commercial cryptography technology in the automotive industry [5] to provide clear guidance and basis for automobile manufacturers. Through standardization and standardization construction, it can promote the wide application and mutual recognition of commercial cryptography technology in the automobile industry, and improve the trust and attention of automobile manufacturers to commercial cryptography technology. As shown in Figure 1.

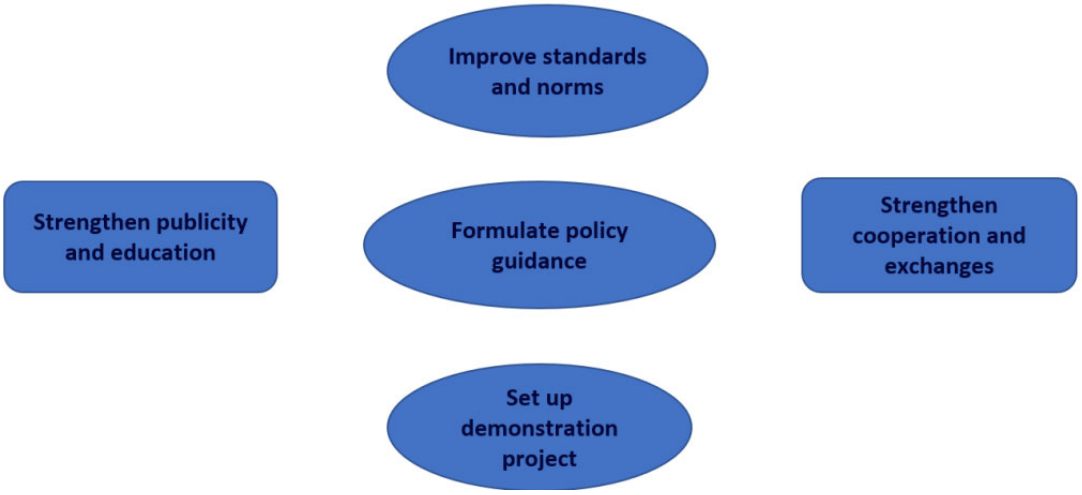

Figure 1. Emphasis strategies for commercial cryptography

2. Reduce the development and application costs of commercial cryptography technology

The government can encourage and support the development and application of commercial cryptography technology by formulating relevant policies. For example, special funds are set up to support research and development projects of commercial cryptography technology, and tax incentives or subsidies are given to automobile manufacturers that adopt commercial cryptography technology [6]. In addition, innovation and application of commercial cryptography technology can be promoted through industry-university-research cooperation. The main measures include: promoting technology sharing and reuse; Standardization and modular development; Policy support and financial subsidies; Industry-university-research cooperation; Cultivate professional talents; Optimize technology application process. As shown in Figure 2. To effectively reduce the development and application costs of commercial cryptography technology, we can start from the following aspects, Technology sharing and standardization: Establish unified technical standards and specifications, promote the versatility and compatibility of cryptography technology, and reduce research and development costs caused by technical differences. Strengthen technical exchanges and cooperation within the industry, share research and development results, and avoid duplication of investment and waste of resources[8]. Government support and policy guidance: The government can introduce relevant policies to provide financial support and tax incentives for the research and development and application of commercial cryptography technology to reduce the burden on enterprises. Establish demonstration areas or bases for research and development and application of cryptography technology, attract enterprises to settle in, form industrial agglomeration effect, and reduce costs. R&d innovation and technology optimization: Encourage and support innovative research and development of cryptography technology, improve the security and efficiency of cryptography algorithms, and reduce the cost of hardware and software due to high algorithm complexity.

Optimize the implementation of cryptography technology, such as the use of lightweight cryptography algorithm, hardware acceleration and other technical means to reduce the cost of hardware and software implementation. Personnel training and training: Strengthen the personnel training of cryptographic technology related majors, improve the professional quality and skill level of talents, and reduce the research and development costs caused by talent shortage[10].

Carry out training and popularization activities on cryptography technology, improve the cognition and application ability of enterprises and individuals on cryptography technology, and reduce the application cost. Marketing and industry cooperation: Strengthen the marketing and publicity of commercial cryptography technology, improve market awareness and acceptance, expand the scope of application, and reduce the cost of unit products. Strengthen cooperation with other related industries, such as chip manufacturing, network communication and other industries, and jointly promote the application and development of commercial cryptography technology to achieve cost sharing and benefit sharing. Intellectual property protection: Strengthen the protection of intellectual property rights of commercial cryptography technology, crack down on infringements, safeguard the legitimate rights and interests of developers, and stimulate innovation vitality. Through the comprehensive application of the above measures[8], it can effectively reduce the cost of research and development and application of commercial cryptography technology, and promote its wide application in more fields. At the same time, it is also necessary to focus on the security and reliability of commercial cryptography technology to ensure that the cost is reduced without compromising security performance.

3. Strengthen the Standardization and Standardization of Commercial Cryptography Technology

Establish a unified standard and specification system for commercial cryptography technology, and clarify the application requirements and standards for commercial cryptography technology in the automotive industry. At the same time, strengthen the docking and mutual recognition with international standards, and promote the wide application of commercial cryptography technology in the world.

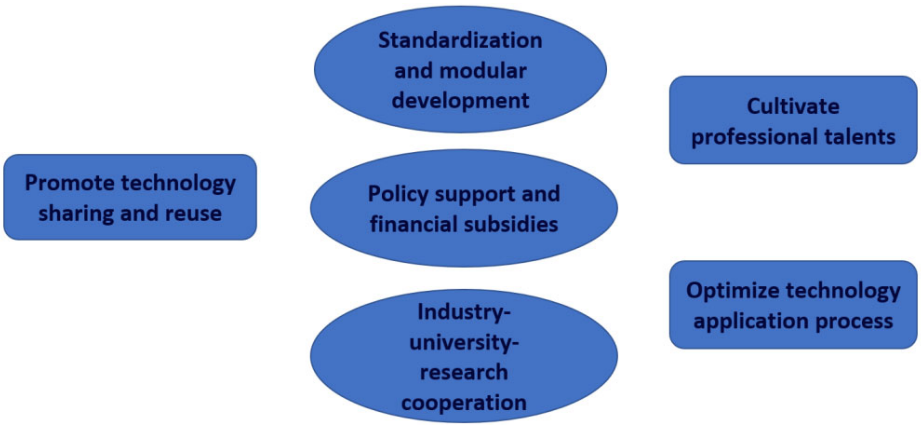

Figure 2. Steps to reduce commercial cryptography

Improve the standard formulation mechanism: First of all, it is necessary to establish and improve the standard formulation mechanism of commercial cryptography technology. This includes the establishment of a dedicated standard-setting body responsible for planning and organizing the development of commercial cryptographic technology standards. At the same time, it is necessary to strengthen the communication and cooperation with the national password management department and the standardization administrative department to ensure that the formulation of standards is consistent with the national password policy and development strategy [7].

Clarify the scope of standard formulation: The formulation of commercial cryptographic technology standards should cover commercial cryptographic algorithms, protocols, products, systems, services and other aspects. These standards should reflect the advanced nature, security and applicability of commercial cryptography technology, and provide unified technical requirements and test methods for the industry [8].

Promote the internationalization of standards: When developing commercial cryptography standards, it is necessary to fully consider the development trend and demand of international standardization, actively participate in international standardization activities [9], and promote the integration of Chinese commercial cryptography standards with international standards. This helps to enhance the international competitiveness and influence of China's commercial cryptography technology [10].

Strengthen the dissemination and implementation of standards: the formulation of standards is only the first step, and it is more important to ensure the widespread dissemination and effective implementation of standards. Training courses, seminars and other activities can be held to popularize the knowledge and application methods of commercial cryptographic technology standards to enterprises, scientific research institutions and the public. At the same time, it is necessary to establish a supervision mechanism for the implementation of standards, and investigate and correct behaviors that violate standards[11].

Establishment of standard update mechanism: With the continuous development of technology and the constant change of security threats, commercial cryptographic technology standards also need to be constantly updated and improved [7]. Therefore, it is necessary to establish a regular evaluation and update mechanism to revise and supplement existing standards to ensure that they remain up-to-date.

Promote collaboration between industry, university, research and application: Strengthen cooperation and exchanges between industry, university, research and application parties, and jointly promote the standardization and standardization of commercial cryptography technology. Enterprises can put forward the needs and problems in practical applications to provide practical basis for the formulation of standards; Scientific research institutions can provide technical support and innovation results to promote the updating and upgrading of standards; The user can feedback the effects and problems in the implementation of the standard, and provide valuable suggestions for the improvement of the standard.

4. Conclusion and Prospect

Accelerating the promotion and application of commercial cryptography technology in the automotive industry is of great significance to improve the level of automotive information security. By increasing the attention of automobile manufacturers to commercial cryptography technology, reducing the cost of research and development and application, and strengthening standardization and standardization construction, we can effectively promote the wide application of commercial cryptography technology in the automobile industry. In the future, with the continuous progress of technology and the expansion of application scenarios, commercial cryptography technology will play a more important role in the automotive industry, providing a more solid guarantee for automotive information security.

It is an important and urgent task to accelerate the application of commercial cryptography technology in the automotive industry. This initiative is not only about the information security of vehicles and drivers, but also has far-reaching implications for the sustainable development of the entire automotive industry.

First of all, the wide application of commercial cryptography technology can significantly improve the information security protection capability of automobiles. With the rapid development of vehicle networking technology, the interaction between vehicles and the external environment is increasing, and the information security risk is also increasing. Commercial cryptography technology can provide vehicles with reliable identity authentication, data encryption and access control functions, effectively prevent the occurrence of security events such as hacker attacks and data leaks, and ensure the safety of vehicles and drivers.

Secondly, the promotion and application of commercial cryptography technology helps to promote the digital transformation and intelligent upgrading of the automotive industry. With the continuous innovation and development of

the automotive industry, intelligence and networking have become an important trend in the development of the industry. As a core means to ensure information security, commercial cryptography technology can provide strong support for the digital transformation of the automotive industry, promote the secure interaction between vehicles and external devices, and achieve business model innovation and service quality improvement.

In addition, accelerating the promotion and application of commercial cryptography technology in the automotive industry also helps to enhance the international competitiveness of China's automotive industry. Under the background of increasingly fierce competition in the global automobile market, it is of great significance to master core technologies such as commercial cryptography technology to enhance the independent innovation ability and market competitiveness of China's automobile industry. By accelerating the promotion and application of commercial cryptography technology, China's automotive industry can better meet the security needs of the international market, enhance the added value of products and brand image, and further expand the international market.

References

[1] Li Fuqiang, Peng Haili. Application of dynamic encryption based on Private network in Automotive industry management [J]. Commercial Vehicles,2018,(12):105-107.

[2] Wei Cheng. Car network identity authentication and privacy in the aggregation scheme research [D]. Huazhong university of science and technology, 2022. The DOI: 10.27157 /, dc nki. Ghzku. 2022.003530.

[3] Wei Jumei, Zhang Liang, Ban Dingdong, et al. Based on new data security laws and regulations of automobile enterprise data security construction analysis [J]. Modern industrial economy and information technology, 2022, 12 (02) : 130-132. The DOI: 10.16525 / j.carol carroll nki. 14-1362 / n. 2022.02.049.

[4] XinRui S ,MuXi L ,XueZhu Y , et al.Research on C-V2X short-range communication security authentication technology based on domestic commercial cryptography algorithm [C]//[Publisher unknown],2023:

[5] Patsakis ,Constantinos,Solanas , et al.Privacy-Aware Event Data Recorders: Cryptography Meets the Automotive Industry Again [J]. IEEE Communications Magazine: Articles, News, and Events of Interest to Communications Engineers, 2013, 51(12): 122-128.

[6] Measures for Management of security evaluation of commercial cryptography applications [J]. Bulletin of The State Council of the People's Republic of China,2023,(33):29-32.

[7] Tian Minqiu. Review on research of cryptographic standard system in China [J]. Information Security and Communication Security,2018,(05):94-101.

[8] Gai Wenxuan, Xu Yu, Jin Junjie. Research on Commercial Password Application for Cloud scenario [C]// China Network Security Industry Alliance. Proceedings of 2023 Network Security Outstanding Innovation Achievement Competition. Hangzhou Anheng Information Technology Co., LTD.; 4, 2023: DOI: 10.26914 / Arthur c. nkihy. 2023.049934.

[9] Yao H Y, Chu R, Li H X, et al. Nuclear security system based on domestic commercial password solution study [J]. Automation instrument, 2023, 44 (S1) : 268-271 + 276. DOI: 10.16086 / j.carol carroll nki issn1000-0380.2023040038.

[10] Yang Nian. Research on the construction of public service platform for commercial cryptography application [J]. Communications and Information Technology, 2023, (05):126-129.

[11] GONG Qimin. Data encryption and standardization of data encryption technology [J]. Communications Security, 1987, (01): 1-12.