WEP Warwick Evans Publishing

International Journal of Global Economics and Management

ISSN: 3005-9690 (Print), ISSN: 3005-8090 (Online) | Volume 2, Number 3, Year 2024
DOI: https://doi.org/10.62051/IJGEM.v2n3.28
Journal homepage: https://wepub.org/index.php/IJGEM/index

Thinking about the application of commercial cryptography in intelligent connected vehicles

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

[1] China Automotive Technology and Research Center Co., Ltd. Tian Jin, China

[2] CATARC Software Testing (Tianjin) Co., Ltd, China

[3] China Auto Information Technology (Tianjin) Co., Ltd. Tian Jin, China

ABSTRACT

As an important part of intelligent transportation, the information security of connected vehicles has become increasingly prominent. As a key technology to ensure the information security of networked vehicles, commercial cryptography plays an important role in vehicle identity authentication, data encryption and secure communication. In this paper, the status quo, challenges and future development trend of commercial cryptography application in connected vehicles are discussed, and some suggestions are put forward to strengthen technology research and development, standardization and industry cooperation. By continuously optimizing the application strategy of commercial cryptography, the information security level of connected vehicles can be effectively improved, providing strong support for the security development of the industry.

KEYWORDS

Network-connected vehicle; Commercial cryptography; Information security; Identity authentication; Data encryption; Secure communication; Technology research and development; Standardization; Industry cooperation

1. INTRODUCTION

As an important development direction of future transportation, intelligent connected vehicles integrate technologies in many fields such as vehicles, communications, and the Internet. However, with the increasingly frequent data interaction between vehicles and the external environment, information security issues are becoming increasingly prominent. As the core technology to ensure information security [1], commercial cryptography is particularly important in the application of connected vehicles.

With the rapid development of information technology and the gradual advancement of intelligent transportation system, connected vehicles have become an important development direction of today's automobile industry. Connected cars not only have the basic functions of traditional cars, but also realize the all-round information interaction between vehicles and vehicles, vehicles and infrastructure, and vehicles and pedestrians through the deep integration of technologies such as the Internet and the Internet of Things. However, this highly connected nature also makes connected cars face unprecedented information security challenges.

As the core technology of information security, the application of commercial cryptography in connected vehicles is particularly important. Commercial cryptography can not only provide powerful identity authentication and data encryption functions for connected cars, ensure the security of information interaction between vehicles and the external environment, but also effectively prevent

malicious attacks and data leakage, and ensure the security and privacy of vehicles and passengers [2].

Therefore, in-depth thinking and discussion on the application of the commercial cryptography of the connected vehicles not only has important theoretical value, but also has practical guiding significance for promoting the security development of the connected vehicles industry. This paper will analyze the application status, challenges and future development trends of commercial cryptography in connected vehicles, and put forward corresponding suggestions in order to provide reference for the security development of connected automotive industry.

It can effectively ensure the safety of vehicle communication. In the connected vehicle, the communication between the vehicle and the external environment is indispensable, and these communications often involve vehicle control, navigation, vehicle information service and other aspects. By adopting advanced encryption technology and authentication mechanism, commercial cryptography applications ensure the confidentiality, integrity and authenticity of communication data, prevent malicious attacks and data tampering, so as to ensure the safety and reliability of vehicle communication.

Second, commercial cryptography applications help protect personal privacy and data security. Connected cars store a lot of personal information and vehicle data, such as owner identity information, driving habits, vehicle location and so on. Once this data is leaked or misused, it will pose a serious threat to personal privacy and vehicle safety [3]. Commercial cryptography applications store and transmit this data encrypted to ensure data security and prevent data leaks and misuse.

In addition, commercial cryptography applications can enhance the trust and reliability of connected vehicles. In intelligent transportation, autonomous driving and other scenarios, connected cars need to work with other vehicles, infrastructure and cloud platforms. By implementing functions such as identity authentication and access control, commercial cryptography applications ensure the trust relationship between participants and prevent unauthorized intrusion and malicious operations, thereby improving the reliability and stability of the entire system [4].

Finally, commercial cryptography applications are also of great significance in promoting the healthy development of the connected automotive industry. With the popularization and application of connected vehicles, information security has become one of the key factors restricting its development. As an effective means to solve the problem of information security, commercial cryptography application can provide solid technical support for the development of connected vehicles and promote its wide application and in-depth development.

2. CURRENT SITUATION OF COMMERCIAL CRYPTOGRAPHY APPLICATION OF CONNECTED VEHICLES

At present, the commercial cryptography application of connected vehicles is mainly concentrated in the following aspects: First, the vehicle identity authentication, through the cryptography technology to achieve the mutual authentication of vehicles and external devices, to ensure the legitimacy of data transmission; The second is data encryption, encrypting sensitive data [3] to prevent data leakage and tampering; The third is secure communication, using cryptographic technology to establish a secure communication channel to ensure the communication security between the vehicle and external equipment. The national cryptographic algorithm is shown in Table 1.

Table 1. Summary of national cryptographic algorithm

Serial number	Algorithm type	State cryptographic algorithm	International algorithm
1	Asymmetric encryption	SM2	RSA, RSA4096
2	Symmetric encryption	SM1	RSA, RSA4096

First, commercial cryptography are widely used in identity authentication and data encryption in connected cars. By using high-strength encryption algorithms and secure identity authentication mechanisms, commercial cryptography can effectively protect the security of information interaction between vehicles and the external environment, preventing malicious attacks and data leakage. This ensures that connected cars can safely and reliably communicate with other vehicles, infrastructure and pedestrians during driving, and achieve the goal of intelligent transportation [4].

Second, commercial cryptography are also used for secure communication in connected cars. By establishing a secure communication channel, commercial cryptography can ensure the security of communication between vehicles and external devices, preventing information from being stolen or tampered with. This ensures that when the connected car transmits important information, such as vehicle status and road condition information, it can maintain the authenticity and integrity of the information, and provide a reliable decision-making basis for intelligent driving.

In addition, with the continuous expansion of the connected car market and the continuous progress of technology, the application of commercial cryptography in connected cars is also constantly upgraded and improved. New encryption algorithms and authentication mechanisms continue to emerge, providing more comprehensive and efficient security protection for connected vehicles [5]. At the same time, the application of commercial cryptography is also gradually developing in the direction of intelligence and adaptability, which can automatically adjust security policies according to the changes of the running state of the vehicle and the external environment, and improve the security performance of connected vehicles.

Figure 1. Application status of business encryption

However, it should also be noted that there are still some challenges and problems facing the commercial cryptography application of connected vehicles. For example, with the continuous upgrading and complexity of attack methods, the security of commercial cryptography needs to be continuously improved and updated [6]. At the same time, cryptographic technology standards and interoperability between different vendors also need to be further strengthened and standardized.

In summary, the current situation of the application of the commercial cryptography of the connected vehicle shows a wide range of applications and a trend of continuous upgrading, which provides an important guarantee for the information security of the connected vehicle. In the future, with the continuous progress of technology and the expansion of application scenarios, the application of commercial cryptography in connected vehicles will be more extensive and in-depth, providing strong support for the development of intelligent transportation.

3. THE CHALLENGES OF COMMERCIAL CRYPTOGRAPHY APPLICATIONS IN CONNECTED VEHICLE

Although the application of commercial cryptography in connected vehicles has achieved some success, it still faces many challenges. First of all, the information system of the connected vehicle is complex, involving multiple links and equipment, and the application of cryptography technology needs to consider the security of each link. Secondly, with the continuous upgrading of attack methods, the security of commercial cryptography also needs to be continuously improved. In addition, the standardization and normalization of commercial cryptography need to be strengthened [7] to promote their widespread application in connected vehicles.

First of all, the information system of connected vehicles is extremely complex, involving multiple links and equipment, such as on-board terminals, sensors, communication networks, etc. This complexity makes the application of cryptography technology need to comprehensively consider the security of each link to ensure the security of the entire information system. However, at present, the application of commercial cryptography is still facing the problem of insufficient standardization, and there are differences in cryptography technical standards and interoperability among different manufacturers, which brings challenges to the overall security of connected vehicle information systems [8].

Secondly, with the continuous upgrading and complexity of attack methods, the security of commercial cryptography needs to be continuously improved and updated. Attackers may exploit vulnerabilities or weaknesses to steal sensitive information or tamper with data, posing a threat to the information security of connected vehicles. Therefore, commercial cryptography needs to be continuously innovated and improved to cope with increasingly severe security threats.

In addition, commercial cryptography applications need to consider performance and efficiency issues. The information system of the connected vehicle needs to process a large amount of data and information in real time, and the application of cryptography technology may increase the cost of calculation and communication, affecting the performance and real-time performance of the system. Therefore, how to improve the performance of cryptography application while ensuring the security is an important problem that needs to be solved in the commercial cryptography application of connected vehicles.

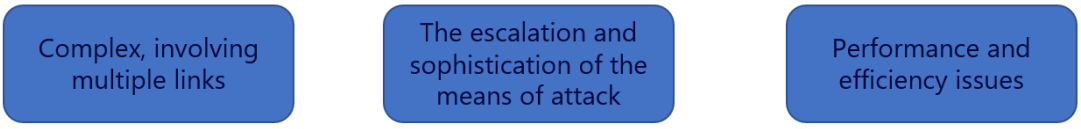

Figure 2. Challenges of business secrecy

Finally, the user's cognition and acceptance of commercial cryptography is also an important factor affecting its application effect. Some users may have doubts about the principles and security of cryptography, or may not be clear about the tradeoff between convenience and security brought about by using cryptography. Therefore, strengthening user education and publicity, and improving users' cognition and acceptance of commercial cryptography is also an important task to promote the application of commercial cryptography for connected vehicles.

To sum up, the application of connected vehicles commercial cryptography faces many challenges such as complexity, security, performance efficiency and user cognition. In order to overcome these challenges, it is necessary to continuously strengthen technology research and development and innovation, improve the standardization and standardization of cryptography technology, improve the performance and efficiency of cryptography applications, and strengthen user education and publicity to promote the widespread popularity and in-depth development of commercial cryptography applications for connected vehicles.

4. THE DEVELOPMENT TREND OF CONNECTED VEHICLE COMMERCIAL CRYPTOGRAPHY APPLICATIONS

In the future, the commercial cryptography application of connected vehicles will show the following development trends: First, the cryptography technology will be more intelligent and adaptive, and can automatically adjust the security policy according to the operating status of the vehicle and the change of the external environment; Second, cryptography technology will be more integrated and collaborative, and integrate with other security technologies of connected vehicles to form a more complete security protection system. Third, cryptography will be more open and standardized, promoting interoperability between different vendors and reducing security costs.

The important significance of the application of the connected vehicles commercial cryptography is that it promotes the development of the cryptography technology to the direction of intelligence and self-adaptation. With the popularization of connected vehicles and the improvement of intelligence, the traditional cryptography application has been difficult to meet the complex and changeable security needs. Therefore, commercial cryptography technology needs to be more intelligent and adaptive, able to automatically adjust security policies according to the operating state of the vehicle and changes in the external environment.

First, intelligent and adaptive cryptography enables real-time assessment of vehicle security risks. In the process of operation, connected vehicles may face various security threats such as network attacks, malware, and illegal intrusion. By adopting intelligent and adaptive cryptography technology, the security status of the vehicle can be monitored in real time, potential security risks can be found, and corresponding preventive measures can be taken to ensure the safe and stable operation of the vehicle.

Secondly, intelligent and adaptive cryptography technology can flexibly respond to changes in the external environment. Connected cars drive on different roads and environments, and may face different communication conditions and safety challenges. The intelligent and adaptive cryptography technology can automatically adjust the parameters of the encryption algorithm and the setting of the communication protocol according to the changes of the external environment, so as to adapt to different communication needs and security requirements, and ensure that the vehicle can maintain a safe communication state in various environments.

In addition, intelligent and adaptive cryptography technology can enhance the trust and reliability of connected vehicles. By enabling more precise identity authentication and access control, trust between vehicles and other participants is ensured. At the same time, intelligent and adaptive cryptography technology can also effectively prevent illegal intrusion and malicious operations, improve the reliability and stability of the entire system, and provide strong support for the wide application and in-depth development of connected vehicles.

The application of cryptography technology in connected vehicles will develop in the direction of more integration and collaboration, which is crucial to improve the security and reliability of connected vehicles.

Integration refers to the deep integration of cryptography technology with the various systems and components of the connected vehicle to achieve seamless connectivity and efficient collaboration. By embedding cryptography technology into the hardware and software of the vehicle, it is possible to ensure that the communication and data transfer between the various systems inside the vehicle are effectively protected. This integrated design not only simplifies the security management process, but also improves the efficiency and accuracy of security protection[8].

Synergy emphasizes cooperation and complementarity between cryptography and other security technologies. The security protection of connected vehicles requires a variety of technologies to work together, including but not limited to intrusion detection, firewall, access control and so on. Cryptographic technology can work together with these technologies to form a multi-level and all-

round security protection system. For example, cryptography can be used to encrypt communication data, while intrusion detection can be used to monitor potential attacks in real time. This collaborative way of working can maximize the safety performance of connected cars.

With the continuous progress of technology and the expansion of connected vehicle application scenarios, cryptography technology will continue to innovate and develop. In the future, we can expect to see the emergence of more intelligent, adaptive cryptography technology that can automatically adjust security policies according to the operating state of the vehicle and changes in the external environment. At the same time, with the integration and application of emerging technologies such as cloud computing, big data and artificial intelligence, cryptography technology will also be closely combined with these technologies to jointly escort the security of connected vehicles.

The application of cryptography technology in connected vehicles will tend to be more open and standardized, which is of great significance to promote the healthy development of the connected vehicles industry.

Openness means that cryptography technology will pay more attention to interworking with different systems and different platforms. With the continuous progress of connected vehicle technology and the increasingly rich application scenarios, cryptography technology needs to adapt to various complex communication environments and security requirements. Through open design, cryptography technology can be better integrated and coordinated with other technologies to form a unified security protection system. This will help break down technical barriers, promote cross-industry and cross-field cooperation and exchanges, and jointly promote the development of the connected vehicles industry.

Standardization is an important support for the opening of cryptography technology. Through the development of unified cryptographic standards and specifications, it can ensure that the cryptographic technology between different manufacturers and different models can be compatible and interworking, and reduce the cost and risk of technology conversion and integration. Standardization also helps to improve the reliability and stability of cryptography technology to ensure the security performance of connected vehicles. At the same time, standardization can also promote the innovation and development of cryptography technology, promote technical exchanges and cooperation within the industry, and enhance the competitiveness of the entire industry.

In the field of connected vehicles, the openness and standardization of cryptography technology will bring many benefits. First, it helps improve the safety of connected cars. By adopting a unified cryptography standard and specification, you can ensure that the communication between the vehicle and the external environment is more secure and reliable, and effectively prevent risks such as hacker attacks and data leaks. Second, openness and standardization will help reduce the manufacturing costs and operation and maintenance costs of connected vehicles. Standardized cryptography technology can achieve scale effects, reduce the cost of research and development and production; The open design helps to improve the maintainability and scalability of the system, and reduce the later operation and maintenance costs.

5. SUGGESTION AND PROSPECT

In view of the current situation and challenges of commercial cryptography application in connected vehicles, this paper puts forward the following suggestions: First, strengthen the research and development and innovation of cryptography technology to promote the continuous upgrading of the application of commercial cryptography in connected vehicles; The second is to strengthen the standardization and standardization of cryptography technology, and establish a unified cryptography application standard and test system; The third is to strengthen industry cooperation and information

sharing, promote technical exchanges and cooperation between different manufacturers, and jointly cope with information security challenges.

First of all, with the continuous progress of technology, commercial cryptography will pay more attention to intelligence and adaptive. The future connected vehicle commercial cryptography system will be able to intelligently adjust and optimize security policies according to the running state of the vehicle, the external environment and the actual needs of users to achieve more accurate and efficient security protection. At the same time, commercial cryptography technology will also pay more attention to adaptability, which can automatically adapt to different network environments, attack means and security threats, and provide continuous and stable security protection.

Secondly, the standardization and normalization of commercial cryptography will be further strengthened. With the continuous expansion of the connected vehicle market and the continuous maturity of technology, the standardization and standardization of commercial cryptography will become an important trend in the development of the industry. In the future, more complete commercial cryptography standards and specifications will be introduced to promote technical interoperability and compatibility between different manufacturers, and promote the widespread popularity and in-depth development of commercial cryptography applications for connected vehicles.

Third, commercial cryptography will be deeply integrated with other security technologies to form a more comprehensive and efficient security protection system. Connected vehicles are faced with security threats from many aspects, and it is necessary to use a variety of security technologies to ensure information security. Commercial cryptography will be deeply integrated with other security technologies such as intrusion detection, firewalls, data encryption, etc., to jointly build a multi-level security protection system and improve the overall security performance of connected vehicles.

In addition, with the rapid development of cloud computing, big data, artificial intelligence and other technologies, the application of commercial cryptography in connected vehicles will continue to innovate and expand. For example, cloud computing technology is used to achieve centralized management and dynamic update of commercial cryptography, big data technology is used to improve the security analysis and early warning capabilities of commercial cryptography, and artificial intelligence technology is used to achieve intelligent decision-making and self-learning of commercial cryptography.

Looking forward to the future, with the continuous expansion of the connected vehicle market and the continuous progress of technology, the role of commercial cryptography in ensuring the information security of connected vehicles will be more important. At the same time, with the continuous innovation of cryptography technology and the continuous expansion of application scenarios, the commercial cryptography application of connected vehicles will usher in a broader development prospect.

The future prospect of connected automotive commercial cryptography application is full of infinite possibilities and challenges. With the rapid development of connected vehicle technology, the importance of commercial cryptography as the core means to ensure its information security has become increasingly prominent. The following are some thoughts and prospects for the future of connected vehicle commercial cryptography application:

First, technology integration and collaboration. In the future, commercial cryptography will be more integrated into the various systems and components of connected vehicles, enabling seamless connectivity and efficient collaboration. Through deep integration with vehicle hardware and software, cryptography technology will be able to provide comprehensive security without affecting vehicle performance. At the same time, commercial cryptography will also work in concert with other security technologies to form a multi-level security protection system to jointly respond to increasingly complex cyber-attacks and threats [8].

With the development of artificial intelligence and big data technology, commercial cryptography technology will realize more intelligent and adaptive security policy adjustment. Through real-time analysis of data such as vehicle operating status, driving behavior and external environment, the cryptographic system can automatically adjust security parameters such as encryption strength and authentication mode to better adapt to security requirements in different scenarios. This will help improve the safety performance of connected cars and reduce safety risks.

The opening and standardization of commercial cryptography technology will be an important trend in the future. By developing a unified cryptography standard and specification to promote the interconnection between different vendors and different platforms, it will help reduce the cost of technology integration and improve the security level of the entire industry. At the same time, open cryptography technology can also attract more innovative forces to participate in promoting the continuous progress of connected vehicle security technology [6].

With the development of cloud computing, edge computing and vehicle-road collaboration technologies, commercial cryptography will play a more important role in these fields. Through cloud-edge collaboration, cryptography technology can realize the encrypted storage and secure transmission of massive data to ensure secure communication between vehicles and the cloud. Vehicle-road collaboration requires cryptographic technology to provide reliable identity authentication and data encryption services to ensure safe interaction between vehicles and road infrastructure.

Of course, the future of connected vehicle commercial cryptography applications also faces many challenges. For example, how to reduce the energy consumption and cost of cryptography while ensuring security; How to respond to the changing methods and threats of cyber-attacks; How to ensure the reliability and stability of cryptography technology. These questions need to be explored and solved in our future research.

6. CONCLUSION

The application of commercial cryptography for connected vehicles is an important means to ensure the information security of connected vehicles. Despite the challenges, by strengthening technology research and development, standardization efforts and industry cooperation, we can promote the widespread application of commercial cryptography in connected vehicles and provide strong support for the security development of the connected automotive industry.

In the future development, we should pay close attention to the new trends and new challenges of the information security of connected vehicles, and constantly adjust and optimize the application strategy of commercial cryptography to ensure that the information security of connected vehicles is effectively guaranteed. At the same time, we should also strengthen international exchanges and cooperation, learn from foreign advanced experience and technology, and promote China's connected automotive commercial cryptography application to reach the international advanced level.

REFERENCES

[1] ZHANG Manjun, Lu Xie, YAO Ge, et al. Research on the application of 5G network business security [J]. Post and Telecommunications Design Technology, 2023, (08):75-80.

[2] Qin Weiqiang, Ji Ruiqi, Ma Yujun, et al. Feasibility Analysis and Engineering Modeling of Simultaneous Promotion of Business Security Evaluation and isoassurance evaluation [J]. Wireless Internet Technology, 2023, 20(14):150-153. (in Chinese)

[3] Lai Jun, Gu Peng, Xing Xianghong, et al. Design of information Security PLC Control System based on business secret [J]. Communications Technology, 2023, 56(07):901-908.

[4] Huang Wenyin, Gao Xiujing, You Shuanghe, et al. A commercial cipher algorithm of commercial vehicle CAN secure communication scheme [J]. Journal of southern fujian normal university (natural science edition), 2023, 4 (01): 41-49. DOI: 10.16007 / j.carol carroll nki issn2095-7122.2023.01.016.

[5] Sun Shugang, Zuo Linlin, Yang Pengfei, et al. C bank a new generation of OA system and network security system research [J]. Journal of network security and data management, 2022, 9 (12): 3-9. DOI: 10.19358 / j.i SSN. 2097-1788.2022.06.001.

[6] Zhu Liufu, Li Jiguo, Lai Jianchang, et al. Attribute based Online/Offline Signature Scheme based on Shang Mi SM9 [J]. Journal of Computer Research and Development, 2023, 60(02):362-370. (in Chinese)

[7] Quan Bin, Wei Wei, Guo Lili. Commercial password techniques in the industry of the national key dealer net [J]. The application of digital technology and applications, 2022, 40 (02): 232-236. The DOI: 10.19695 / j.carol carroll nki cn12-1369.2022.02.75.

[8] Lai Jianchang, Huang Xinyi, He Debiao, et al. Based on commercial cipher SM9 efficient identification sign close [J]. Journal of password, 2021, 8 (02): 314-329. The DOI: 10.13868 / j.carol carroll nki JCR. 000440.