INFORMATION SECURITY ENCRYPTION TECHNOLOGY FOR SPECIAL INTERNET OF VEHICLES-JOINT AES AND RSA ALGORITHMS

Yanling Bai
School of Artificial Intelligence, Zhengzhou Railway Vocational & Technical College, Zhengzhou, 450056, China

Abstract - While Internet of vehicles technology improves transportation efficiency, it also brings challenges in information security. That is, how to guarantee the confidentiality and integrity of data has become a key issue to be solved. To this end, the research is based on the advanced encryption standard algorithm and its parallel optimization. Meanwhile, the elliptic curve Diffie-Hellman algorithm is incorporated into the Rivest-Shamir-Adleman encryption algorithm for key exchange optimization. Finally, a new special vehicle Internet of vehicles information security encryption model is proposed. The experimental results indicated that the new model achieved the fastest encryption speed of 125 Mbit/s, the fastest decryption speed of 135 Mbit/s, the lowest resource consumption rate of 53.72%, and the lowest latency rate of 3.98%. In the six types of classical information tampering tests, the new model was especially effective in resisting encryption against man-in-the-middle attack and authorization bypass. Its encrypted data integrity rate was up to 99.93%, and its processing throughput was up to 19.32 Mbps. In conclusion, the proposed encryption model of the study outperforms the traditional algorithms in terms of encryption efficiency, computational resource consumption, and data transmission delay. This method can further enhance the data security of special vehicles Internet of vehicles to ensure the safe operation of special vehicles.

Keywords: Specialized vehicles; IoV; Message encryption; AES; RSA; ECC.

1. Introduction

With the rapid development of information technology, internet of vehicles (IoV), as an emerging intelligent transportation system, is capable of realizing intelligent data exchange and interaction between vehicle and vehicle, vehicle and road network, and vehicle and cloud through the integration of wireless communication and information technology [1]. However, while IoV technology brings convenience and efficiency, it also raises many information security issues. Especially in the application scenarios of special vehicles, such as public transportation and military vehicles, the information security problem is more prominent [2]. These vehicles usually need to deal with a large amount of sensitive data, such as positioning information, vehicle status data, traffic control data, and so on. Once these data are illegally tampered with or leaked, they will pose a great threat to social security, public services, and national security. Vishwakarma et al. found that modern software-defined networks still harbored unpredictable security vulnerabilities when dealing with IoV. For this reason, the study proposed an improved practical Byzantine fault-tolerant IoV security encryption algorithm. The results demonstrated that the algorithm reduced the computational cost by 85% compared to the advanced scheme [3]. According to Gong et al., frequent RFID authentication may raise the network's overall computational and communication overhead in situations including traffic congestion. Thus, this study proposed an IoV secure encryption method in combination with elliptic curve cryptography (ECC) algorithm. Experimental results indicated that this method reduced the communication overhead by 66.67% compared to traditional RFID in non-congested scenarios [4]. Bojjagani et al. found high potential danger posed by security vulnerabilities and cyber threats in existing IoV. To address the problem, the researchers proposed a novel protection strategy by performing a formal analysis of security through the Real-Random Predictor

© 2025 The Author(s). Published by Cefin Publishing House – Bucharest, https://ijomam.com/

https://doi.org/10.17683/ijomam/issue22.v1.18

model. The results demonstrated that the strategy was more confidentiality-stable and robust compared to advanced methods [5]. A secure and effective anonymous batch authentication technique with conditional privacy based on ECC was proposed by Maurya et al. after they discovered that the current IoV authentication schemes were ineffective and came with significant computational and communication overheads. The results demonstrated that the scheme supported batch signature verification, and it could efficiently verified multiple signatures at the same time with high effectiveness [6].

Advanced encryption standard (AES), a symmetric encryption algorithm, is widely used in data encryption scenarios due to its efficient encryption speed and low computational overhead [7]. Tang et al. found that IoV for hazardous chemical logistics vehicles had large privacy and data security issues. For this reason, the study analyzed AES and combined it with data encryption standard algorithms for optimization to propose a protocol algorithm. The experimental results demonstrated that the method could effectively improve the security and real-time performance of IoV data transmission [8]. To improve the security of cloud-side data in IoV, Wu et al. generated a pseudo-random key stream by fusing AES and bitwise-orthogonal operations for constraints. The results indicated that the key sequence generated by this method was not only highly randomized, but also robust to small disturbances in the initial value. The Rivest-Shamir-Adleman (RSA) algorithm, as a representative of asymmetric cryptography, realized secure and reliable key distribution and authentication through the pairing mechanism of public and private keys [9]. To prevent unauthorized vehicles, bystanders, or drivers from connecting and implanting or changing sensitive data, Lin et al. focused on how to secure information transfer through IoV in real time. The researchers proposed an elliptic curve digital signature algorithm in conjunction with RSA. The results indicated that the algorithm effectively reduced the system key reconstruction synchronization time and reduced the number of phases to resynchronize the system key [10]. Anusuya Devi et al. proposed a new security protocol which combines AES and RSA cryptography. AES was used for robust encryption in the first phase and RSA was used for efficient key management in the second phase. The experimental results indicated that the efficiency of encryption, decryption, and total execution time of this hybrid protocol was improved as compared to the existing algorithms [11].

In summary, existing IoV information security encryption methods have made some progress in improving encryption efficiency and data security, but still have problems such as higher encryption latency and higher computation and communication overhead. To address these shortcomings, the study proposes a hybrid encryption model that combines improved AES and RSA. The model not only improves the encryption and decryption speeds (DSs), but also optimizes the key management and security with lower computational cost and delay rate by introducing the AES parallelization optimization technique and the elliptic curve Diffie-Hellman (ECDH) key exchange mechanism of RSA. The innovation of the research lies in overcoming the limitations of a single algorithm by combining the advantages of two encryption algorithms. In particular, it provides a more efficient and secure solution in terms of adaptability and efficiency performance in the complex environment of IoV, aiming to further enhance the efficiency and security of data encryption for special vehicles in IoV.

2. Methods and Materials

2.1 Improved AES-based Secure Encryption for Special Vehicle IoV Information

The encrypted core data of IoV information security of hazardous chemical transportation vehicles include transportation paths, load information, vehicle status, and environmental monitoring data. Once maliciously attacked or tampered with, it may cause serious security accidents and even lead to large-scale casualties and environmental pollution [12-13]. In addition, since hazardous chemical transport vehicles involve high-value, flammable and explosive special cargoes, the IoV system puts forward higher requirements on data security, integrity and anti-attack capability. The structure of IoV information security encryption system for hazardous chemical transport vehicles is shown in Figure 1 [14-15].

In Figure 1, the encryption system is mainly composed of three parts: the vehicle-mounted terminal, the communication network system and the monitoring center. Specifically, the vehicle-mounted terminal includes vehicle gateway, encryption module, and data acquisition module, which is responsible for real-time collection of vehicle operation status, environmental parameters, cargo information, and encryption processing of data. The communication network system adopts a combination of cellular communication and Internet to ensure stable data transmission in a wide-area environment. The monitoring center is composed of decryption module and management terminal.

The decryption module decrypts the received data by using the private key. Moreover, the integrity and authenticity of the data are verified by matching algorithm [16]. For the IoV information security requirements of hazardous chemical transportation vehicles, the traditional symmetric encryption algorithm, although with low computational complexity, is suitable for vehicle terminals with limited resources, but there are some hidden dangers in terms of security. Therefore, the study adopts AES as the encryption core to ensure data confidentiality with its high security and efficient computational performance. The encryption process of AES is shown in Figure 2.

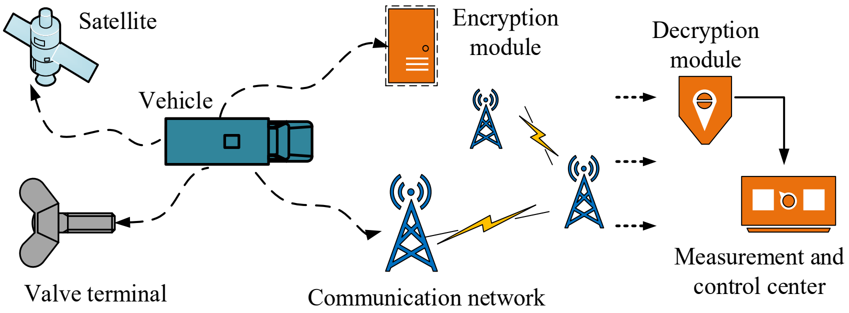

Figure 1: Structure of IoV information security encryption system for hazardous chemical transport vehicles

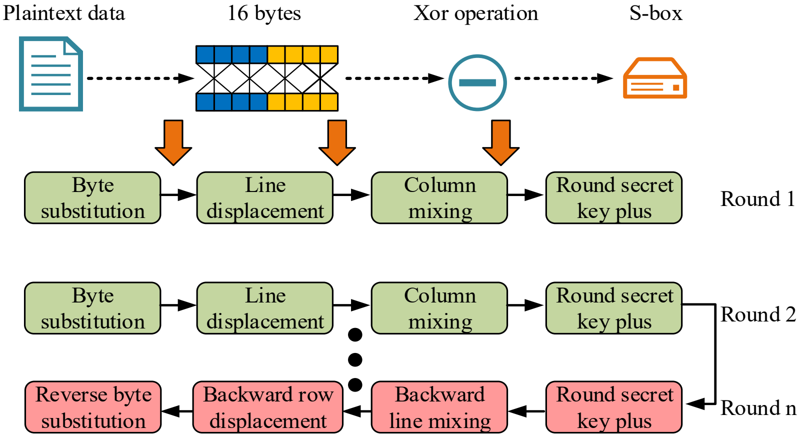

Figure 2: Encryption flow of the AES algorithm

In Figure 2, AES encryption consists of multiple rounds. Each round performs byte substitution (BS), row shifting (RS), column mixing (CM), and round key addition operations (RKAOs). First, the plaintext data is split into 16-byte groups and iso-orthogonal to the initial key. Subsequently, BS utilizes S-boxes for nonlinear transformation and RS adjusts the data position. CM uses finite domain matrix operations to enhance diffusivity. The RKAO processes the data by extended key dissimilarity [17-18]. The final round omits CM and performs only the first three steps to generate the ciphertext output. Hazardous chemical transportation vehicles in IoV the data stream D needs to be grouped before it is encrypted. It is assumed that the data stream D is of length L and the grouping size $b=16$ bytes. Then the initial key K is computed as shown in Equation (1) after key expansion to generate multiple rounds of key K_i.

$$K_i = F(K_{i-1}) \oplus K_{i-4}, \quad i = 4,5,\cdots,44 \tag{1}$$

In Equation (1), $F(\_)$ denotes the table S-box nonlinear transformation and wheel constant operation. $\oplus$ denotes the dissimilarity operation. During each round of AES encryption, the state matrix S performs the dissimilarity operation with the corresponding round key K_i as shown in Equation (2).

$$S_i = S_{i-1} \oplus K_i, \quad i = 1,2,\ldots,r \tag{2}$$

In Equation (2), r denotes the number of AES rounds. S_i denotes the state matrix after the i th round. The packet that the car sends is configured to guarantee the confidentiality and promptness of the encrypted data. After AES processing, the encrypted data is calculated as shown in Equation (3).

$$\begin{cases} C_j = AES_{Enc}(P_j, K_{dyn}) \\ K_{dyn} = H(K,T) \oplus R \end{cases} \tag{3}$$

In Equation (3), AES_{Enc} denotes AES encryption. V_j denotes the j th vehicle. P_j denotes the data packet sent by the j th vehicle. C_j indicates the encryption result of the data sent by the j th vehicle K_{dyn} denotes dynamic key. T denotes dynamic window. $H(\_)$ denotes the hash function. R denotes random perturbation factor. After the decryption end receives the ciphertext C_j, the computational formula for key decryption and hash check is shown in Equation (4).

$$\begin{cases} P_j^{'} = AES_{Dec}(C_j, K_{dyn}) \\ H(P_j^{'}) = H(P_j) \Rightarrow D_{Com} \end{cases} \quad (4)$$

In Equation (4), AES_{Dec} denotes AES decryption. $P_j^{'}$ denotes the intermediate state after the j th round of decryption. $H(P_j^{'})$ denotes hash checksum. $H(P_j)$ denotes the hash value of the data after the j round of decryption. To optimize the serial decryption process of AES algorithm, to reduce the data grouping waiting time and to improve the overall throughput, the study is to try the task grouping parallel computing, and to optimize the decryption computation by data flow mapping. The original serial AES decryption elapsed time is calculated in comparison with the total decryption time after parallel computing as shown in Equation (5).

$$\begin{cases} T_{serial} = T_{round} \times Q \times N \\ T_{parallel} = \dfrac{T_{serial}}{M} \end{cases} \quad (5)$$

In Equation (5), Q denotes the number of AES decryption rounds. N denotes the number of data groups. T_{round} denotes the single round decryption elapsed time. M denotes the number of parallel computing cores. Meanwhile, the study adds an enhanced hash checksum mechanism to the decryption process that combines cross-hashing and cryptographic hash mapping between data blocks to guarantee the integrity of the decrypted data and improve the anti-tampering capability. The improved hash checksum function calculation formula is shown in Equation (6).

$$H_{enhanced} = H(S_j^0) \oplus H(S_{j-1}^0) \oplus H(S_{j+1}^0) \oplus K_H \quad (6)$$

In Equation (6), $H(S_j^0)$ denotes the hash value of the current data block. $H(S_{j-1}^0)$ and $H(S_{j+1}^0)$ denote the hash values of the front and back neighboring data blocks, respectively. K_H denotes the encryption hash key dynamically generated by the system. At this point, the study further introduces timestamps combined with hash checksums for data verification, as shown in Equation (7).

$$H_{verify} = H\left(S_j^0 \| T_s\right) \oplus K_t \quad (7)$$

In Equation (7), K_t denotes the timestamp encryption key. If H_{verify} checksum fails, the system will reject the packet to prevent replay attack. At this time, the improved AES encryption process is shown in Figure 3.

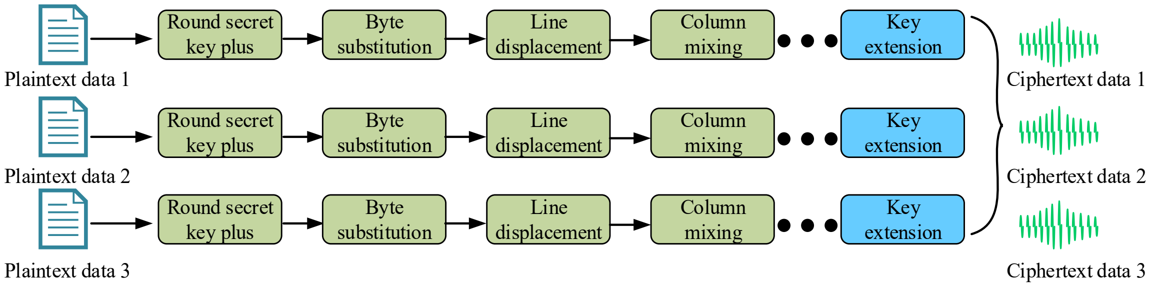

Figure 3: Improved AES operation flow

In Figure 3, each data block goes through BS, RS, CM, and RKAOs in turn. During the parallelization process, the input data is divided into multiple 16-byte groupings. Each grouping first goes through the BS step, a process that utilizes S-boxes for nonlinear substitution operations. Next, a row shift operation cyclically shifts the bytes in each row, changing the order of the data in the rows. Then, the CM step further extends the data changes by matrix multiplication over a finite domain. Finally, at the end of each round, a RKAO is performed using the expanded round key to complete the encryption for the current round. The improved AES algorithm introduces a parallel execution mechanism, which enables each data block to be encrypted independently at the same time, optimizing the efficiency of data processing.

2.2 Construction of a Secure Cryptographic Model for Special Vehicle IoV Messages Incorporating Improved AES and Improved RSA

After the parallelization and optimization of AES, the study reveals that despite the significant advantages of the method in enhancing encryption speed and improving data processing capacity, it still faces the problems of key management and data sharing security [19]. Therefore, the study introduces the RSA algorithm to enhance the security of encrypted data and key management by combining with public key cryptography. In Figure 4, the RSA algorithm flow is displayed [20].

In Figure 4, first, the RSA algorithm randomly generates two large primes p and q. Then, the modulus n as well as the Euler function $\varphi(n)$ are computed. Next, an encryption exponent e is chosen such that e is mutually prime with $\varphi(n)$, i.e., the conditions $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$ are satisfied. Subsequently, the decryption exponent d is solved by the extended Euclidean algorithm. This makes the inverse of $de = 1 \bmod \varphi(n)$, i.e., e and d are inverse elements under the modulus $\varphi(n)$.

Following the creation of the key, the sender uses the recipient's public key to encrypt the plaintext message m. In parallel, the recipient uses the private key to decrypt the encrypted ciphertext c. However, although the traditional RSA algorithm can provide a more secure data transmission method, its key exchange process has potential security risks, especially in an untrusted network environment.

For this reason, the study introduces ECDH and improves the key generation process of RSA by utilizing the secure key exchange mechanism provided by ECDH.

The ECDH-RSA authenticatable key negotiation process is shown in Figure 5.

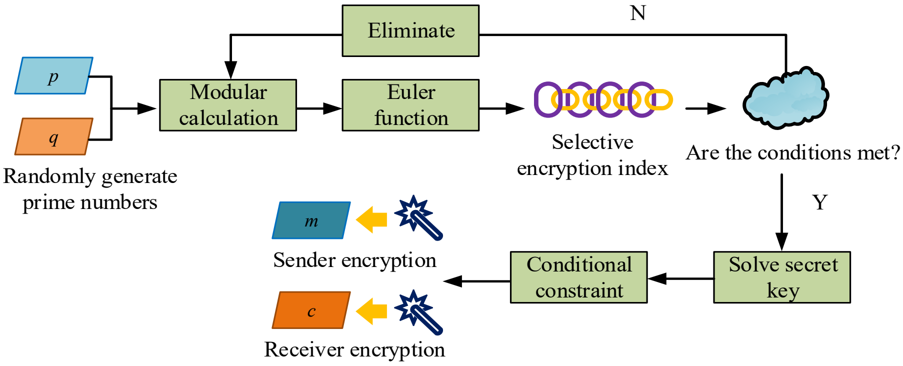

Figure 4: RSA algorithm flow

In Figure 5, the ECDH-RSA authenticatable key negotiation process begins with user A and user B obtaining identity information through their respective private and public key pairs, and subsequently exchanging public keys. User A generates a shared key based on the computation of its private key and user B's public key. Similarly, user B also generates the shared key by computing with the public key of user A through its private key. The shared key is used to verify whether the two parties have successfully reached a consensus. Moreover, the shared key is used for subsequent encrypted communication. The base point on the elliptic curve is set to be G, the private key of user A is d_A, and the private key of user B is d_B. Then the formula for calculating the shared key K_{AB} is shown in Equation (8).

$$K_{AB} = d_A \cdot P_B = d_B \cdot P_A \tag{8}$$

In Equation (8), $P_A = d_A \cdot G$ denotes the public key of user A. $P_B = d_B \cdot G$ represents the public key of user B. P_A and P_B represent points on the elliptic curve, respectively. ECDH optimizes the RSA encryption process with this shared key, counted as shown in Equation (9).

$$C = (m \cdot H(K_{AB}))^e \cdot \bmod n \tag{9}$$

In Equation (9), m denotes the plaintext message. $H(K_{AB})$ denotes the hash value of the shared key K_{AB}. e denotes the RSA public key index. n denotes RSA modulus. C denotes the encrypted ciphertext. In the decryption process, the receiver decrypts the message by the RSA private key together with the hash value of the shared key. The improved RSA decryption formula is shown in Equation (10).

$$m = (C \cdot H(K_{AB})^{-1})^d \cdot \bmod n \tag{10}$$

In Equation (10), $H(K_{AB})^{-1}$ denotes the inverse element of the shared key hash. d denotes the RSA private key. In addition, considering the complexity of key generation and exchange, the study quantifies the computational formula for the efficiency of ECDH for RSA encryption process as shown in Equation (11).

$$\eta = \frac{T_{RSA} - T_{ECDH-RSA}}{T_{RSA}} \tag{11}$$

In Equation (11), η denotes the improvement ratio of encryption efficiency. T_{RSA} denotes the computation time of traditional RSA encryption. $T_{ECDH-RSA}$ denotes the RSA encryption time after the introduction of ECDH. The computational equation of the key update mechanism is shown in Equation (12).

$$K_{AB}^{'} = H(K_{AB}) \cdot d_A \cdot P_B = H(K_{AB}) \cdot d_B \cdot P_A \qquad (12)$$

In Equation (12), $K_{AB}^{'}$ denotes the updated shared key. $H(K_{AB})$ denotes the hash value of the shared key generated in the previous cycle. Finally, the study combines the improved AES and improved RSA to propose a new special vehicle IoV information security encryption model. Its structure is shown in Figure 6.

In Figure 6, the whole new special vehicle IoV information security encryption model is divided into two main phases, i.e., encryption phase and decryption phase.

In the encryption phase, the sender first encrypts the AES key using the RSA public key to ensure the security of the AES key during transmission. Next, the sender uses the encrypted AES key to perform AES encryption on the plaintext data to generate encrypted data. The encrypted data is transmitted to the receiver via the Internet. In the receiving phase, the receiver first decrypts the transmitted encrypted AES key using the RSA private key to obtain the correct AES key. Then, the receiver uses the decrypted AES key to decrypt the encrypted data using AES decryption, and finally recovers the original plaintext data.

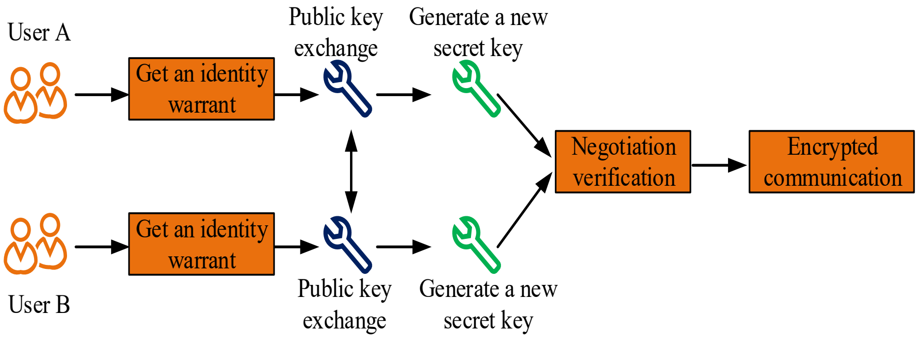

Figure 5: ECDH-RSA Authentication key negotiation process

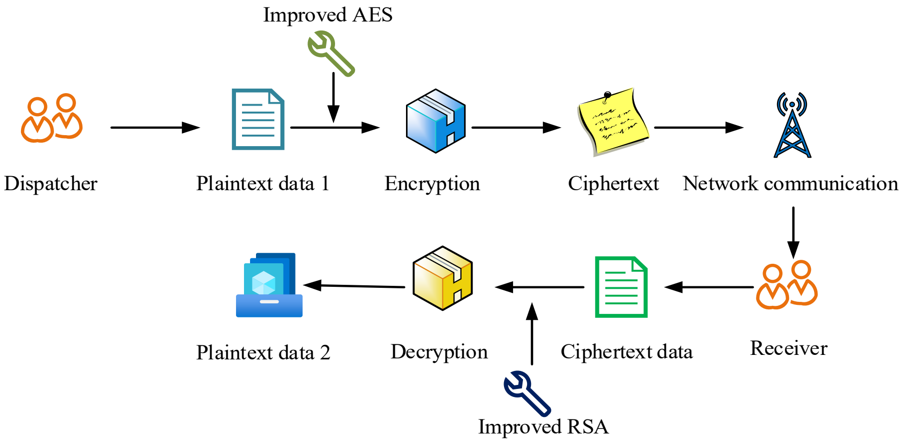

Figure 6: New special vehicle IoV information security encryption model

3. Results

3.1 Performance Testing of IoV Message Security Encryption Model for New Specialized Vehicles

The study setup CPU is Intel Core i9-13900K, GPU is NVIDIA RTX 4090, and 64GB RAM. The operating system is Windows 10 Pro and the programming language and tool is Python 3.8. Internet of Things Intrusion Detection System 2017 (IoT-IDS 2017) and Connected and Autonomous Vehicle Data Set 2020 (CAV 2020) are used as test data sources. Among them, IoT-IDS 2017 contains data traffic from multiple IoT devices, modeling the traffic characteristics under different attack types, such as DoS, DDoS, malicious code, data tampering, and so on. The CAV 2020 dataset includes a variety of information such as vehicle status, GPS information, real-time traffic flow data, inter-vehicle communication data, and so on.

The study first tests the selected values of two types of hyperparameters that affect the performance of the model the most, i.e., random perturbation factor R for AES and public key index e for RSA. The test results are shown in Figure 7.

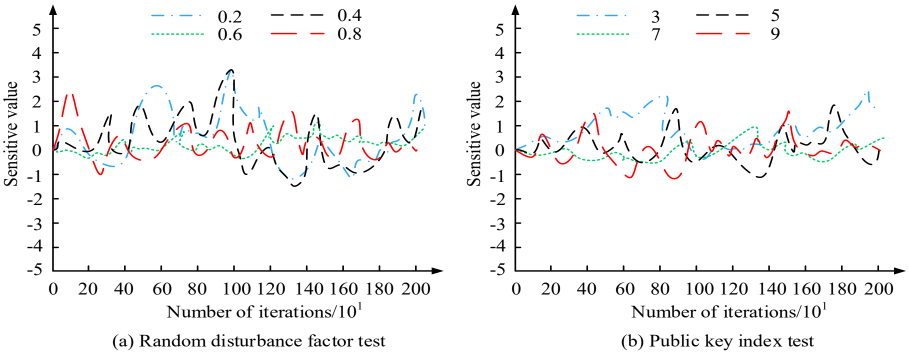

Figure 7: Hyperparameter selection test result

Figure 7(a) shows the results of the selected value test for the random perturbation factor. The model's sensitivity values exhibit an increasing trend of volatility as the perturbation factor rises. When the perturbation factor is 0.8 and 0.2, the sensitivity value fluctuates significantly and reaches the highest peaks of 4 and 3, respectively. In contrast, at moderate values, such as 0.6, the sensitivity value is smoother, and the maximum value is not more than 2. This suggests that higher or lower random perturbation factors lead to a significant increase in the model's sensitivity, which may bring about instability in the encryption effect.

Low public key indices (e.g., 3 and 5) make the sensitivity value fluctuate more, and the maximum fluctuation can reach 3. As the public key indices increase, e.g., 7 and 9, the sensitivity fluctuation tends to stabilize, and the maximum fluctuation decreases to between 1 and 2. In particular, the sensitivity value is relatively smoothest when the public key index is 7, indicating that a higher public key index helps to improve the stability of the encryption process. The study continues with an ablation test of the final model with the index mean square error (MSE). The test results are shown in Figure 8.

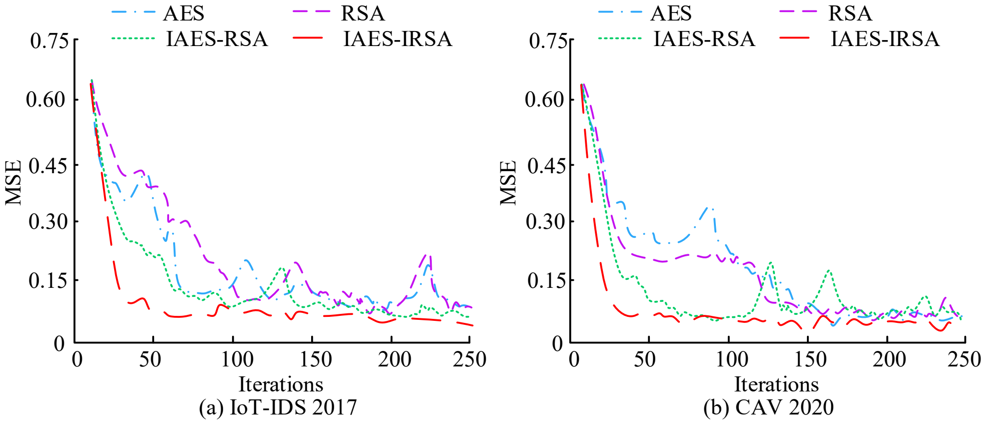

Figure 8: Ablation test results

Table 1. Index test results of different encryption methods

Data	Model	Encryption speed /Mbit/s	Decryption speed /Mbit/s	Resource consumption rate /%	Delay rate /%
IoT-IDS 2017	AES	100	110	65.32	5.21
	RSA	80	85	72.45	7.32
	ECC	85	90	69.12	6.15
	Our model	120	130	55.88	4.12
CAV 2020	AES	110	115	62.14	5.55
	RSA	90	95	74.21	7.16
	ECC	95	100	70.33	6.84
	Our model	125	135	53.72	3.98

Figure 8(a) shows the ablation test results in the IoT-IDS 2017 dataset. The AES-IRSA model consistently has the lowest MSE value, around 0.15, showing optimal encryption and data processing performance. The MSE values of the RSA and IAES-RSA models are close to each other, at around 0.2. The AES model has an initially high MSE value but eventually stabilizes at around 0.2. Figure 8(b) shows the ablation test results in the CAV 2020 dataset. The IAES-IRSA model continues to exhibit the lowest MSE at about 0.2. The RSA and IAES-RSA have slightly higher MSE values, close to 0.3, with little difference in performance. The AES has a consistently higher MSE, close to 0.3, which is significantly behind the other models. This indicates that the IAES-IRSA model performs optimally on both datasets with the lowest MSE, verifying its advantages in information security and data accuracy. For comparison, the study presents the same class of more sophisticated encryption techniques, including AES, RSA, and ECC. Table 1 displays the findings.

In Table 1, the proposed model is studied to perform best in encryption speed, DS, resource consumption rate, and latency rate. In particular, the suggested model outperforms AES, RSA, and ECC in terms of encryption speed, with values of 116.42 Mbit/s and 125 Mbit/s on the two kinds of datasets. The suggested model's DS speed of 135 Mbit/s is noticeably faster than that of previous algorithms.

In addition, the resource consumption rate of this new model is minimum 55.88%, which is much lower than other algorithms. Its delay rate is minimized to 3.98%, ensuring higher real-time performance. In conclusion, the proposed model of the study outperforms the traditional encryption algorithms in all performance metrics, performs more efficiently, has low latency, consumes less resources, and is suitable for complex IoV information security encryption tasks.

3.2 Simulation Test of a New Special Vehicle IoV Information Security Encryption Model

To verify the real application effect of the new special vehicle IoV information security encryption model, the study simulates 6 types of classical IoV information tampering attack types as examples, namely data tampering, man-in-the-middle attack (MMA), replay attack, identity spoofing, cryptographic key tampering, and authorization bypass. Comparative tests are conducted on the above six types of cryptographic models to verify their respective performance. The test results are shown in Figure 9.

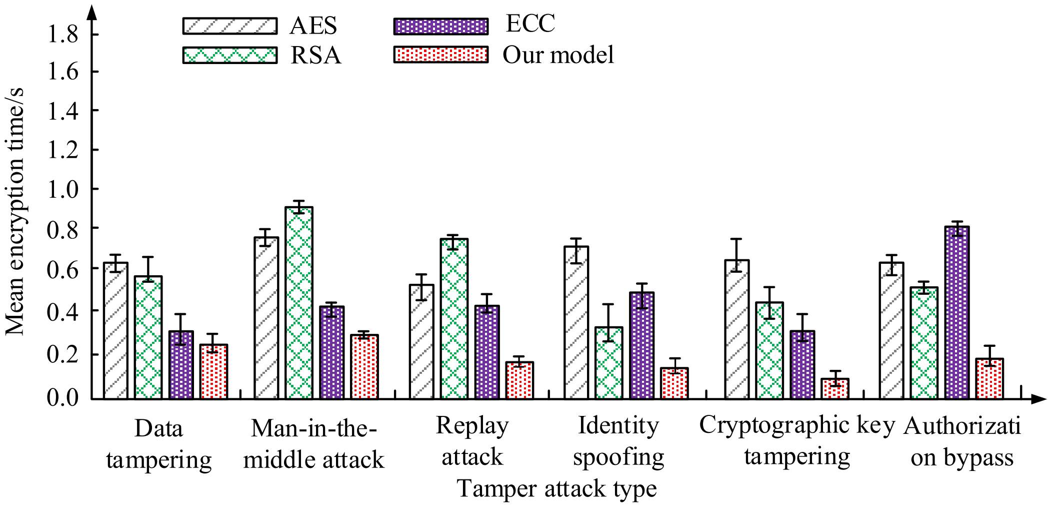

Figure 9: Comparison of average encryption time of different encryption methods

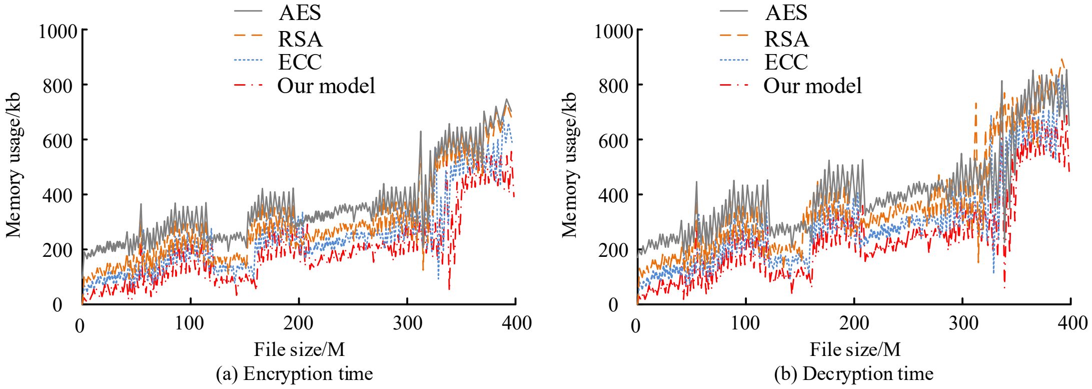

Figure 10: Comparison of memory consumption of encryption and decryption by different algorithms

Table 2. Each model deals with the test results of indicators of different attacks

Data	Model	Encryption delay /ms	Data integrity rate /%	Throughput /Mbps
Man-in-the-middle attack	AES	135.72	98.24	15.89
	RSA	213.58	96.45	12.33
	ECC	145.23	97.63	14.27
	Our model	120.56	99.87	18.65
Authorization bypass	AES	152.41	97.45	16.52
	RSA	220.32	95.32	11.68
	ECC	148.76	96.12	13.45
	Our model	125.18	99.93	19.32

In Figure 9, the proposed model of the study shows better encryption efficiency than AES, RSA, and ECC under all attack types. The encryption time of this new model is significantly lower than the other algorithms under common attacks such as data tampering and MMA, with a minimum encryption time of 0.15 s. In comparison, the encryption times for AES and RSA are 0.6 and 0.55 s, respectively, and 0.5 s for ECC. In addition, the proposed model is studied to maintain the lowest encryption time when dealing with replay attack, identity spoofing, cryptographic key tampering, and authorization bypass attack. It further proves its efficiency and stability in dealing with complex attacks. Overall, the proposed model of the study shows better performance in all test scenarios. The study tests the encryption memory consumption of different algorithms separately. The results are shown in Figure 10.

Figure 10(a) shows the comparison results of encryption memory consumption of different algorithms. The memory consumption of each encryption algorithm increases gradually as the file size increases. The model proposed in the study shows lower memory consumption compared to AES, RSA, ECC for encryption task and the memory usage is about 350KB for large file processing. Moreover, the memory consumption of AES, RSA, and ECC is close to 750KB, 650KB, and 600KB. Figure 10(ab) shows the comparative results of decryption memory consumption of different algorithms. The comparison of memory consumption during decryption is similar to that of encryption, but overall both show that the decryption memory consumption of the proposed model is also significantly lower than that of the other algorithms. Especially when the file size is large, the growth trend of memory consumption is slower, while the memory consumption of the other algorithms shows a steeper growth curve with the increase of file size. In particular, when the file size is 150M, the memory consumption of the proposed model is 100KB, while the other three types of algorithms all consume more than 200KB. Overall, the study proposes that the model's memory usage during both encryption and decryption is better than that of AES, RSA, and ECC, and is more suitable for existing IoV message encryption. Finally, the study continues with an in-depth test of two types of attack types that show large differences in efficiency, namely, MMA, and authorization bypass. The test uses throughput, encryption latency, and data completeness as measurements. Table 2 displays the findings.

In Table 2, the suggested model's delay performance is maximized with respect to encryption delay. Especially in the face of MMA and authorization bypass, its encryption delay is 120.56ms and 125.18ms respectively, which is significantly lower than that of AES, RSA, and ECC algorithms. In terms of data integrity rate, this new model is close to perfect in both MMA and authorization bypass attack, which are 99.87% and 99.93%, respectively. The throughput test results show that the proposed model reaches 18.65Mbps when dealing with MMA. The ride reaches 19.32Mbps when dealing with authorization bypass, which are both significantly higher than the throughput of other algorithms. In summary, this new model not only provides lower encryption delay when dealing with these two types of attacks. It also demonstrates the best performance in terms of data integrity and throughput, which fully proves its advantages in security and efficiency.

4. Conclusions

Aiming at the problem of special vehicle IoV information security, the study proposed a hybrid encryption model combining AES and RSA algorithms by optimizing the parallelization of AES algorithms and improving the ECDH key exchange mechanism of RSA algorithms, aiming to enhance the encryption efficiency and security of IoV data. The outcomes indicated that when the perturbation factor was 0.6 and the public key index took the value of 7, the maximum value of the sensitivity of the model was not more than 2, which demonstrated cryptographic stability. In addition, comparing with the pure AES and RSA modules, the MSE value of the encryption model incorporating improved AES and improved RSA could be as low as close to 0.1, which was significantly reduced numerically. The suggested model had the lowest resource consumption rate (53.72%) and the lowest latency rate (3.98%) when compared to other advanced encryption models. The fastest encryption speed was 125 Mbit/s, and the fastest DS was 135 Mbit/s. The shortest encryption time of 0.15 s for the proposed model was found in the classic information tampering test for six categories. The maximum reduction was 0.35 s compared to other methods. In addition, the memory usage of this new model was around 350KB during large file processing, while the memory consumption of AES was close to 750KB. In summary, the aforementioned results demonstrate that the suggested model's cryptographic efficiency and tamper resistance are enhanced across a range of attack scenarios. However, although the introduction of ECDH to optimize the RSA key exchange process improves the key management security, the frequency and efficiency of the key update mechanism still need to be further optimized for more complex application scenarios in the highly dynamic and frequently changing IoV environment. Future research can further explore the possibility of combining multiple cryptographic algorithms and validate them in more complex IoV environments to drive IoV technology toward higher security and efficiency.

Acknowledgments

The research is supported by: 2022 Henan Vocational Education Teaching Reform and Practice Project, Research and Practice on the Training Model of Higher Vocational Information Security Skills Talents Based on "Position-Course-Competition-Certification, Docking Education", (NO. Yu Jiao [2023] 03135); Henan Province Vocational Education Teaching Reform Research and Practice Project, Research and Practice on Empowering the "Three Teachings" (Teachers, Teaching Materials, Teaching Methods) Reform in Higher Vocational Education through Multi-form Digital Resource Construction, (NO. Yu Jiao [2024] 05751).

References

[1] Ning Y, Chen Y, Huang Z, Xue S. Research on Information Security of Key Systems for Intelligent Connected Vehicles. Advances in Engineering Technology Research, 2024, 12(1): 558-558. https://doi.org/10.56028/aetr.12.1.558.2024

[2] Bao Y, Qiu W, Cheng X, Sun J. Fine-grained data sharing with enhanced privacy protection and dynamic users group service for the IoV. IEEE Transactions on Intelligent Transportation Systems, 2022, 24(11): 13035-13049. https://doi.org/10.1109/TITS.2022.3187980

[3] Vishwakarma L, Nahar A, Das D. LBSV: Lightweight blockchain security protocol for secure storage and communication in SDN-enabled IoV. IEEE Transactions on Vehicular Technology, 2022, 71(6): 5983-5994. https://doi.org/10.1109/TVT.2022.3163960

[4] Gong Y, Li K, Xiao L,Cai J, Xiao J, Liang W, Khan M K. VASERP: An adaptive, lightweight, secure, and efficient RFID-based authentication scheme for IoV. Sensors, 2023, 23(11): 5198-5203. https://doi.org/10.3390/s23115198

[5] Bojjagani S, Reddy Y C A P, Anuradha T, Rao P V V, Reddy B R, Khan M K. Secure authentication and key management protocol for deployment of internet of vehicles (IoV) concerning intelligent transport systems. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(12): 24698-24713. https://doi.org/10.1109/TITS.2022.3207593

[6] Maurya C, Chaurasiya V K. Efficient anonymous batch authentication scheme with conditional privacy in the Internet of Vehicles (IoV) applications. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(9): 9670-9683. https://doi.org/10.1109/TITS.2023.3271355

[7] Zhang Y, Zhang L, Wu Q, Mu Y. Blockchain-enabled efficient distributed attribute-based access control framework with privacy-preserving in IoV. Journal of King Saud University-Computer and Information Sciences, 2022, 34(10): 9216-9227. https://doi.org/10.1016/j.jksuci.2022.09.004

[8] Tang Y, Chen Y, Jung H. Hazardous Chemicals Logistics Internet of Vehicles Based on Encryption Algorithm. Scalable Computing: Practice and Experience, 2024, 25(3): 1287-1300. https://doi.org/10.12694/scpe.v25i3.2064

[9] Wu Y, Wu L, Cai H. Cloud-edge data encryption in the internet of vehicles using Zeckendorf representation. Journal of Cloud Computing, 2023, 12(1): 39-44. https://doi.org/10.1186/s13677-023-00417-7

[10] Lin H Y, Hsieh M Y. A dynamic key management and secure data transfer based on m-tree structure with multi-level security framework for Internet of vehicles. Connection Science, 2022, 34(1): 1089-1118. https://doi.org/10.1080/09540091.2022.2045254

[11] Anusuya Devi V, Sampradeepraj T. End-to-End Self-organizing Intelligent Security Model for Wireless Sensor Network based on a Hybrid (AES–RSA) Cryptography. Wireless Personal Communications, 2024, 136(3): 1675-1703. https://doi.org/10.1007/s11277-024-11353-3

[12] Xie Z, Chen Y, Ali I. Efficient and secure certificateless signcryption without pairing for edge computing-based Internet of Vehicles. IEEE Transactions on Vehicular Technology, 2022,

72(5): 5642-5653. https://doi.org/10.1109/TVT.2022.3230442

[13] Hu X, Li R, Wang L, Ning Y. A data sharing scheme based on federated learning in iov. IEEE Transactions on Vehicular Technology, 2023, 72(9): 11644-11656. https://doi.org/10.1109/TVT.2023.3266100

[14] Ullah I, Khan M A, Kumar N, Abdullah A M, AlSanad A A, Noor F. A conditional privacy preserving heterogeneous signcryption scheme for internet of vehicles. IEEE Transactions on Vehicular Technology, 2022, 72(3): 3989-3998. https://doi.org/10.1109/TVT.2022.3220041

[15] Wu J, Jin Z, Li G, Xu Z, Fan C, Zheng Y. Design of vehicle certification schemes in IoV based on blockchain. World Wide Web, 2022, 25(5): 2241-2263. https://doi.org/10.1007/s11280-022-01078-3

[16] Zhang M, Zhou J, Cong P, Zhang G, Zhuo C, Hu S. LIAS: A lightweight incentive authentication scheme for forensic services in IoV. IEEE Transactions on Automation Science and Engineering, 2022, 20(2): 805-820. https://doi.org/10.1109/TASE.2022.3165174

[17] Sikarwar H, Das D. A novel MAC-based authentication scheme (NoMAS) for Internet of Vehicles (IoV). IEEE Transactions on Intelligent Transportation Systems, 2023, 24(5): 4904-4916. https://doi.org/10.1109/TITS.2023.3242291

[18] Mahmood A, Siddiqui S A, Sheng Q Z. Trust on wheels: Towards secure and resource efficient IoV networks. Computing, 2022, 104(6): 1337-1358. https://doi.org/10.1007/s00607-021-01040-7

[19] Cheng H, Yang J, Shojafar M, Cao J, Jiang N, Liu Y. VFAS: Reliable and privacy-preserving V2F authentication scheme for road condition monitoring system in IoV. IEEE transactions on vehicular technology, 2023, 72(6): 7958-7972. https://doi.org/10.1109/TVT.2023.3242309

[20] Salem R B, Aimeur E, Hage H. A Multi-Party Agent for Privacy Preference Elicitation. Artificial Intelligence and Applications. 2023, 1(2): 98-105. https://doi.org/10.47852/bonviewAIA2202514