Research on Secure Transmission of Communication Data in Wireless Network Space: Encryption by an Improved AES Algorithm

Jiqing Cao[1] and Junkuan Gao[2]
(Corresponding author: Jiqing Cao)
Information Engineering School, SIP Institute of Service Outsourcing[1]
School of Society, Soochow University[2]
No. 208, Songtao Road., Suzhou Industrial Park, Suzhou, Jiangsu 215123, China
Email: cjq1975@hotmail.com
(Received Sept. 29, 2023; Revised and Accepted Nov. 16, 2024; First Online Dec. 24, 2024)

Abstract

This paper briefly introduces the advanced encryption standard (AES) algorithm. In order to improve its performance, the number of encryption rounds was reduced, and the S-box table look-up method was used to replace the column confusion operation in the process of round encryption. Moreover, simulation experiments were carried out in the laboratory server to test the impact of encryption rounds on ciphertext and compare the encryption efficiency and security of the traditional and improved AES algorithms. The results showed that when the number of encryption rounds was 7, the computational load could be reduced under the premise of ensuring security; the improved AES algorithm had higher encryption efficiency and security.

Keywords: Advanced Encryption Standard; Data Transmission; Encryption; Wireless Network

1 Introduction

With the rapid development of information technology, the wireless network infrastructure has become indispensable to modern society. The existence of wireless network has greatly promoted the free flow and sharing of information [8]. Communication data is easy to be intercepted, tampered with, or stolen in the process of wireless network transmission, which seriously threatens personal privacy, corporate secrets, and even national security [12].

The advanced encryption standard (AES) algorithm is one of the extensively utilized symmetric encryption algorithms at present. It plays an important role in the field of data encryption due to its characteristics of high efficiency, high security, and easy implementation [7]. However, with the improvement of computer computing power, the security of the traditional AES algorithm has been challenged. In order to improve the encryption security, optimization of encryption algorithms is necessary.

Guo *et al.* [4] utilized fractional order chaotic time series to design an image encryption scheme. Yang *et al.* [14] designed an improved AES algorithm using chaos theory for solving the security problem of the AES algorithm. The feasibility and security of the algorithm were verified by simulation. Gai *et al.* [3] proposed a dynamic data encryption strategy, which aims at employing selective encryption strategies within the required execution time requirements. In this paper, the AES algorithm is briefly introduced. In order to improve its performance, the number of encryption rounds was reduced, and the S-box table look-up method was used to replace the column confusion operation in the process of round encryption. Moreover, experimental tests were carried out.

2 Improved AES Algorithm

The AES algorithm adopts the substitution-permutation network structure, which mainly includes two parts: round function and key extension [5]. The main function of the round function is to perform substitution, permutation, key encryption, and other operations on plaintext, and the function of key extension is to use the main key to generate the extension key for the key encryption operation in the round function [9].

Because of the open structure of the wireless network space, the data transmitted in it is also open and easy to be intercepted by eavesdropping. Moreover, the protocol in the wireless network is complex, and there may be security loopholes that are maliciously exploited, which will also lead to data leakage [6]. Therefore, data encryption is needed. The AES algorithm only need to use the round function for multiple iterations to realize data encryption, and the plaintext can be obtained by performing the inverse operation using the round function,

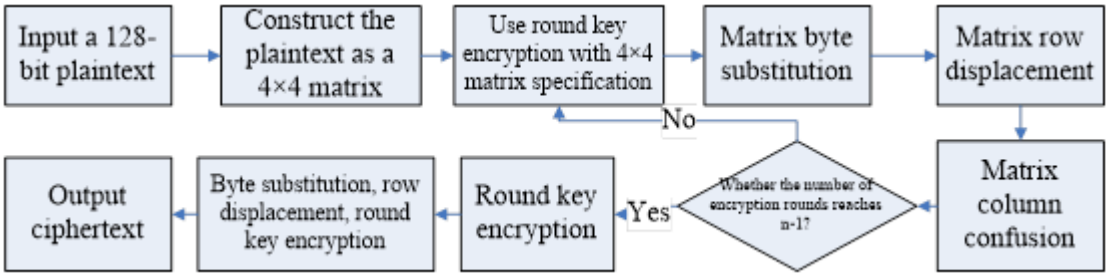

Figure 1: Encryption process of the traditional AES algorithm

which has high efficiency. However, in the face of the ever-developing wireless network space, the traditional AES algorithm is gradually difficult to cope with and needs to be improved [11].

As shown in Figure 1, the plaintext with a specified bit length is input. Taking a 128 bit length (16 bytes) as an example, if the plaintext exceeds 128 bits, the plaintext is grouped by 128 bits, and the group with a bit size below 128 bit is supplemented in the form of zero setting [1]. Each group can form a matrix of 4 × 4, and each element in the matrix is a 8-bit data. Then, addition operations are performed on the data using the round key (a matrix of 4 × 4) derived from the master key extension. Byte substitution is performed using the S box [2]. Displacement and column confusion operations are also performed. The above steps are repeated n-1 times as needed. At the n-th time, i.e., the last round of encryption, round key encryption, byte substitution, row displacement, and round key encryption operations are conducted [10]. Finally, the ciphertext is output.

When the traditional AES algorithm uses the round function to iteratively transform the data, most sub-operations require operations within a finite field, which will reduce the efficiency of the encryption algorithm. Therefore, the improvement of the AES algorithm is to use the S-box table look-up method in the "byte substitution" operation to deal with column confusion operations in the round transform. The formula of the round transform [13] is expressed as:

$$\begin{aligned} A_{i,j} &= I_{i,j} \oplus K_{i,j} \\ B_{i,j} &= S(A_{i,j}) \\ C_{i,j} &= B_{i,(i+j)\%4} \end{aligned}$$

$$\begin{aligned} \begin{bmatrix} O_{0,j} \\ O_{1,j} \\ O_{2,j} \\ O_{3,j} \end{bmatrix} &= \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} B_{0,j} \\ B_{1,j} \\ B_{2,j} \\ B_{3,j} \end{bmatrix} \\ &= \begin{bmatrix} 02 \times S(A_{0,j}) \\ 01 \times S(A_{0,j}) \\ 01 \times S(A_{0,j}) \\ 03 \times S(A_{0,j}) \end{bmatrix} \oplus \begin{bmatrix} 03 \times S(A_{1,j}) \\ 02 \times S(A_{1,j}) \\ 01 \times S(A_{1,j}) \\ 01 \times S(A_{1,j}) \end{bmatrix} \\ &\quad \oplus \begin{bmatrix} 01 \times S(A_{2,j}) \\ 03 \times S(A_{2,j}) \\ 02 \times S(A_{2,j}) \\ 01 \times S(A_{2,j}) \end{bmatrix} \oplus \begin{bmatrix} 01 \times S(A_{3,j}) \\ 01 \times S(A_{3,j}) \\ 03 \times S(A_{3,j}) \\ 02 \times S(A_{3,j}) \end{bmatrix} \end{aligned}$$

where $I_{i,j}$ is an element at the i-th row and j-th column of the input matrix, $K_{i,j}$ is an element at the i-th row and j-th column of the key matrix, $A_{i,j}$ is an element at the i-th row and j-th column after input matrix encryption, $S(\cdot)$ represents the S-box table look-up function, $B_{i,j}$ is an element at the i-th row and j-th column after byte substitution in $A_{i,j}$, $C_{i,j}$ is an element at the i-th row and j-th column after row displacement operation in $B_{i,j}$, and $O_{i,j}$ is the row and column element in the output matrix. It can be seen from the formula expression of the above round transformation that after the input data is encrypted by key, only table look-up replacement and addition operation are needed in the entire round transformation process as long as $S(\cdot)$, $02 \times S(\cdot)$, and $03 \times S(\cdot)$ are preset, which greatly reduces the computational complexity [15].

3 Simulation Experiment

3.1 Experimental Environment

Three laboratory servers were set up for experiments, Server 1 as the communication transmitter and Server 2 as the communication receiver.

3.2 Experimental Setup

First, Server 1 and Server 2 built a wireless communication network, and Server 1 sent files to Server 2. The

whole wireless communication process is as follows. First, Server 1 and Server 2 realized the "handshake" in the wireless network to unify the AES key used for encryption and then established the communication. Secondly, after Server 1 read the file to be sent, the AES key was used to encrypt the file. Then, the encrypted file was sent to Server 2 over the wireless network. After receiving the encrypted file, Server 2 used the AES key obtained during the handshake to decrypt the ciphertext.

3.3 Test Items

1) The impact of encryption rounds on the AES algorithm

   For the AES algorithm, the more iterations in encryption using the round function, the better the encryption effect of ciphertext, but the amount of computation will also increase. Therefore, it is necessary to choose the appropriate encryption rounds and minimize the encryption rounds on the premise of ensuring the encryption security. During the test, 20 groups of plaintext were randomly generated, and each group contained two 128-bit plaintexts. There was only one byte difference between the two plaintexts. The improved AES algorithm was used to encrypt the plaintext, and the number of encryption rounds was set from 1 to 10 respectively to compare the bit difference between the two ciphertexts in each group after encryption.

2) Efficiency of data encryption and decryption

   Files with a size of 15, 30, 45, 60, and 75 MB were set respectively to test the encryption and decryption time in the two algorithms. The t-test method was employed to compare the efficiency of encryption and decryption between the two algorithms. If the P value was less than 0.05, the difference between the two algorithms was considered significant.

3) Security test of the encryption algorithm

   First, 20, 40, 60, 80, 100 KB data were encrypted, and then the "0-1" balance and information entropy of the ciphertext were tested. The formulas are:

$$\delta = \frac{K_1 - K_2}{n}$$
$$H(S) = -\sum_{S} P(S_i)\log_2 P(S_i)$$

   where K_1 and K_2 are the number of 0 and 1 after the ciphertex is converted to a binary number, n represents the total number of 0 and 1 after the ciphertext is converted to a binary number, δ stands for the balance degree (the closer it is to 0, the better the "0-1" balance of the ciphertext and the stronger the randomness of the ciphertext), $H(S)$ is the information entropy of the ciphertext (when the American Standard Code for Information Interchange (ASCII) characters are randomly distributed, it means that the characters are distributed in an equal probability, and the information entropy at this moment is an ideal value, 8, i.e., the closer the ciphertext information entropy is to 8, the more stronger the randomness), and $P(S_i)$ is the probability of the i-th ASCII character in the ciphertext.

3.4 Test Results

The improved AES algorithm was employed to encrypt the plaintexts with only one byte difference, and then the average bit difference between the ciphertexts under different encryption rounds was compared, and the results are shown in Figure 2. The average bit difference between the ciphertexts after encryption increased with the increase of encryption rounds, and the average bit difference between the ciphertexts after six rounds was stable at about 120 bits. For a 128-bit ciphertext converted from 128-bit plaintext, an average bit difference of 120 bits indicated that the difference between the two ciphertexts was huge. Considering that the number of encryption rounds will prolong the encryption time, seven rounds of encryption was selected.

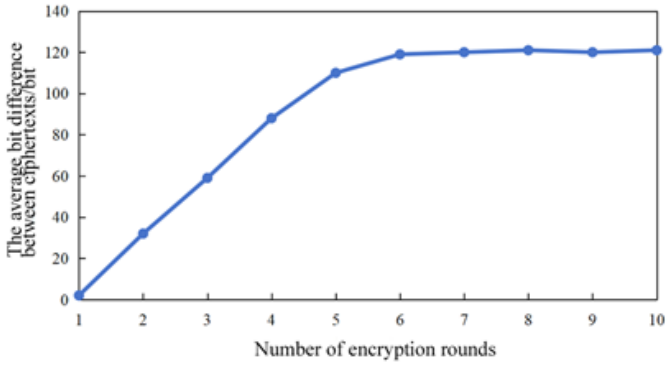

Figure 2: The effect of the number of encryption on the encryption effect

Moreover, the encryption and decryption efficiency of the traditional and improved AES algorithms was tested. The encryption and decryption time of the two encryption algorithms are shown in Table 1. The time spent on encryption and decryption increased as the size of the file became larger. For files of the same size, the improved AES algorithm had significantly higher encryption and decryption efficiency.

The "0-1" balance and information entropy of the ciphertext were used to measure its randomness. The higher the randomness of the ciphertext, the higher the security. The test results are shown in Table 2. It can be seen from the table that the randomness level of the ciphertexts obtained by the two encryption algorithms gradually rose with the increase of the file size. Under the same file size, the ciphertext obtained by the improved

Table 1: Encryption and decryption efficiency of the encryption algorithms

Encryption algorithm	**Traditional AES**		**Improved AES**	
File size	Encryption time /s	Decryption time /s	Encryption time /s	Decryption time /s
15 MB	1.35	1.42	1.12*	1.23*
30 MB	2.14	2.23	1.98*	2.10*
45 MB	3.25	3.38	3.04*	3.18*
60 MB	4.32	4.47	4.01*	4.21*
75 MB	5.47	5.59	5.11*	5.32*

Note: * indicates that the P value of the encryption or decryption time between the two algorithms is less than 0.05, i.e., the difference is significant.

Table 2: Ciphertext security

Data size	20 KB	40 KB	60 KB	80 KB	100 KB	
Traditional AES	Balance degree	0.02174	0.01249	0.00887	0.00423	0.00135
	Information entropy	7.784	7.789	7.836	7.869	7.887
Improved AES	Balance degree	0.00274	0.00178	0.00068	0.00053	0.00027
	Information entropy	7.965	7.987	7.987	7.996	7.998

AES algorithm had a smaller balance degree and an information entropy closer to 8, which meant that ciphertexts generated by the improved AES algorithm was more random and safer.

4 Conclusions

This paper reduced the number of encryption rounds in order to enhance the performance of the AES algorithm and used the S-box table look-up method to replace the column confusion operation in the process of round encryption. Moreover, simulation experiments were performed in the laboratory servers to test the impact of encryption rounds on ciphertexts and compare the efficiency and security of the traditional and improved AES algorithms. The results are as follows. The increase of encryption rounds increased the change in the ciphertext, but the change tended to be stable after six rounds, so the number of encryption rounds were set to 7. With the increase of the file size, the encryption and decryption time of the two encryption algorithms were prolonged. Under the same file size, the efficiency of the improved AES algorithm was significantly higher. With the increase of the file size, the balance degree of the ciphertext obtained by the two algorithms gradually decreased, and the information entropy gradually approached 8. Under the same file size, the ciphertext obtained by the improved AES algorithm had a smaller balance degree and an information entropy closer to 8.

References

[1] N. Attar, H. Deldari, M. Kalantari, "AES Encryption Algorithm Parallelization in Order to Use Big Data Cloud Naser Attar, Hossein Deldari, Marzie Kalantari," *Computer and Information Science*, vol. 10, no. 3, pp. 23-28, 2017.

[2] A. Banushri, R. A. Karthika, "A Survey on Data Security Using File Hierarchy Attribute-Based Encryption in Cloud Computing Environment," *Journal of Advanced Research in Dynamical & Control Systems*, vol. 2017, no. 4, pp. 144-149, 2017.

[3] K. Gai, M. Qiu, H. Zhao, J. Xiong, "Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing," in *IEEE International Conference on Cyber Security & Cloud Computing*, pp. 273-278, 2016.

[4] Z. Guo, J. Yang, Y. Zhao, "Double image multi-encryption algorithm based on fractional chaotic time series," *Open Mathematics*, vol. 13, no. 1, pp. 868-876, 2015.

[5] Y. M. Koukou, S. H. Othman, M. Nkiama, "Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithm," *IOSR Journal of Engineering*, vol. 06, no. 6, pp. 01-07, 2016.

[6] Z. L. Lan, L. Zhu, Y. C. Li, J. Liu, "A Color Image Encryption Algorithm Based on Improved DES," *Applied Mechanics & Materials*, vol. 743, pp. 379-384, 2015.

[7] C. C. Lee, H. C. Tseng, C. C. Liu, H. J. Chou, "Using AES Encryption Algorithm to Optimize High-tech Intelligent Platform," *WSEAS Transactions on Business and Economics*, vol. 18, pp. 1572-1579, 2021.

[8] A. Mersaid, T. Gulom, "The Encryption Algorithm AES-RFWKIDEA32-1 Based on Network RFWKIDEA32-1," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 1-11, 2016.

[9] Z. Mihret, M. W. Ahmad, "The Reverse Engineering of Reverse Encryption Algorithm and a Systematic Comparison to DES," *Procedia Computer Science*, vol. 85, pp. 558-570, 2016.

[10] P. R. More, S. Y. Gaikwad, "An Advanced Mechanism for Secure Data Sharing in Cloud Computing using Revocable Storage Identity Based Encryption," *International Journal of Engineering Business Management*, vol. 1, no. 1, pp. 12-14, 2017.

[11] A. B. Nasution, S. Efendi, S. Suwilo, "Image Steganography In Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB)," *Journal of Physics Conference*, vol. 1007, pp. 1-6, 2018.

[12] S. Oukili, S. Bri, "Hardware Implementation of AES Algorithm with Logic S-box," *Journal of Circuits Systems & Computers*, vol. 26, no. 9, pp. 1750141, 2017.

[13] T. Paka, S. Divya, "Data Storage Security and Privacy in Mobile Cloud Computing Using Hierarchical Attribute Based Encryption (HABE)," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 6, pp. 750-754, 2019.

[14] Z. H. Yang, A. H. Li, L. L. Yu, S. J. Kang, M. J. Han, Q. Ding, "An Improved AES Encryption Algorithm Based on Chaos Theory in Wireless Communication Networks," in *Third International Conference on Robot, Vision and Signal Processing*, pp. 159-162, 2015.

[15] H. Yue, X. Zheng, "Research on Encrypting Accounting Data Using Des Algorithm under the Background of Microprocessor System," *Microprocessors and Microsystems*, no. 1, pp. 104061, 2021.

Biography

Jiqing Cao, born in April 1975, graduated from Fudan University with a master's degree in June 2004. He is working at Suzhou SIP Institute of Service Outsourcing as an associate professor. He is interested in Cloud Computing, Big Data, and Intelligent Manufacturing.

Junkuan Gao, born in 1977, graduated with a Ph.D. in Management from Wuhan University in 2005, and currently works at the School of Sociology, Soochow University as an associate professor. His main research areas include privacy protection and Big Data.