E-commerce network security protection technology based on mixed data encryption strategy

Yuan He[1,*], Liqi Ou[1], Xiaofei Pu[2], Yunfei Li[1], Yuyuan Zhao[1]

***Abstract*—**Network security is required more by the development of e-commerce. Data encryption is an effective method to ensure network security. In this paper, Advanced Encryption Standard (AES) algorithm and Elliptic Curve Cryptography (ECC) algorithm were analyzed, and their advantages and disadvantages were found. Then a hybrid encryption strategy based on AES and ECC was proposed for the security protection of e-commerce networks. The performance of mixed encryption strategy was analyzed through different experiments, and it was found that AES algorithm and ECC algorithm had obvious advantages in symmetric and asymmetric algorithms. AES+ECC hybrid encryption strategy had lower space complexity and higher security. It took only 1000 ms to process 50 M packets. Experimental results demonstrated the reliability of AES+ECC hybrid algorithm. It provides some theoretical basis for its application in e-commerce network security protection.

***Keywords*—**e-commerce, mixed encryption, data encryption, advanced encryption standard, elliptic curve cryptography, network security.

I. Introduction

E-COMMERCE is a form of using computer network to carry out business activities, and an efficient and low-cost way of consumption. Network security is a key issue in the development of electronic commerce. A lot of important information and data are stored in the network. However, due to the openness of the network and the complexity of the network environment, e-commerce data are easy to be attacked by eavesdropping, tampering or malicious destruction [1], which seriously hinders the good development of e-commerce. Data encryption technology is a key technology to realize e-commerce network security protection [2]. However, due to the large scale and complexity of e-commerce data, the security of traditional single encryption algorithm cannot be guaranteed [3], while this deficiency can be made up by mixed encryption methods. Cheon et al. [4] proposed a hybrid homomorphic encryption algorithm. Public Key Encryption (PKE) and Slightly Homomorphic Encryption (SHE) are combined to reduce the storage requirements of the algorithm. Kuppuswamy et al. [7] combined public key encryption based on linear block ciphers with private key encryption based on simple symmetric algorithm to obtain a mixed encryption method. It effectively solves the problems of user privacy protection and authentication, and has high security. Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) algorithms are studied in this paper. An AES+ECC hybrid encryption strategy is designed and its performance is analyzed. It is proved that this method has high security and high speed, and can realize the security protection of e-commerce network.

Y. He is with Department of Trade and Technology, Xijing University, Xi'an, Shaanxi 710123, China (e-mail: yhyuan_h@yeah.net).

L. Q. Ou, Y. F. Li, and Y. Y. Zhao are with Department of Trade and Technology, Xijing University, Xi'an, Shaanxi 710123, China.

X F. Pu is with the China International Contractors Association, Beijing 100036, China.

II. Data Encryption Technology

Data encryption means that the plaintext of information is encrypted by some algorithm and transformed into unrecognizable code. The conversion of code to plaintext is only possible with the corresponding key. In this way, information and data can be guaranteed not to be stolen and tampered, so as to achieve network security protection [8]. Plaintext, ciphertext, key and algorithm are generally included in a data encryption technology. It is supposed that the encryption key is expressed as E_K, the decryption key is expressed as D_K, the clear text is expressed as M, and the ciphertext is expressed as C. The encryption process can be expressed as $E_K(M) = C$. The decryption process can be expressed as $D_K(C) = M$, and the relationship between encryption and decryption as $D_K(E_K(M)) = M$.

Data encryption technology needs to meet the following conditions: (1) the password system is uncrackable, or the cost of cracking is higher than the benefit of cracking; (2) it can be applied in different users and occasions, with a wide range of applications; (3) matching with the computer communication system and having no influence on the speed of system operation.

Current data encryption technologies can be mainly divided into two types: symmetric encryption such as data encryption standard (DES), International Data Encryption Algorithm (IDEA), AES, etc. and asymmetric encryption such as RSA, Rabin, McEliece, etc. Symmetric encryption technology has the advantages of fast encryption speed and short key length in big data encryption. However, there are some disadvantages such as difficulty in key management and transmission.

Asymmetric encryption technology has large key space and high security, but long key and slow encryption speed [9]. The hybrid data encryption policy can fully exploit the advantages of both encryption techniques. Therefore, in this paper, AES algorithm in symmetric encryption technology and ECC algorithm in asymmetric encryption technology are combined to form a hybrid encryption algorithm for the network security protection of e-commerce.

III. AES ENCRYPTION ALGORITHM

AES [10] is a symmetric encryption algorithm with higher security than DES, which has been widely used in many industries and fields. AES is an iterative block encryption algorithm with block and key lengths of 128 bits, 192 bits and 256 bits. The number of cycles for encryption and decryption of keys of different lengths is shown in Table I.

Table I Number of AES cycles

	Key block length	Data block length	The number of cycles
128	4	4	10
192	6	4	12
256	8	4	14

The AES algorithm mainly includes four steps: s-box change, row shift, column mixing and round key addition. The 128 bits grouping length and the 128 bits key length are taken as examples. The algorithm steps of AES are shown below.

(1) Exclusive OR (xor) operation is carried out with the extended key.

(2) s-box change: each byte is treated as an element in the finite domain k, and the multiplicative inverse is mapped and affine transformation is performed:

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

(3) Row shift: The principle of byte displacement in a 4 × 4 matrix is shown in Fig. 1. In Fig. 1, the first row remains the same. In the second line, A_1 byte moves. Then A_2 bytes in the second line moves. In the third line, A_3 byte moves. The values of A_1, A_2 and A_3 are taken according to different ciphertext lengths.

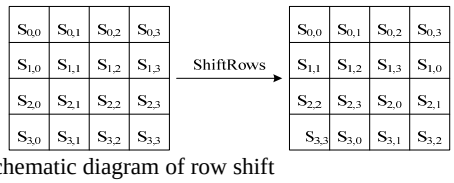

Fig. 1 Schematic diagram of row shift

(4) Column mixing: Each column in the matrix is regarded as the polynomial $a(x)$ in $GF(2^8)$ multiplied by the known polynomial $b(x)$. The result is processed by modular x^4+1 operation, and $c(x)=a(x)b(x)\bmod(x^4+1)$ is obtained. The principle is shown in Fig. 2.

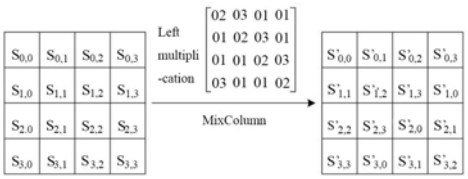

Fig. 2 Schematic diagram of column mixing

(5) Round key addition: the bytes in the corresponding matrix of round key is performed by xor and the key is mixed. The principle is shown in Fig. 3.

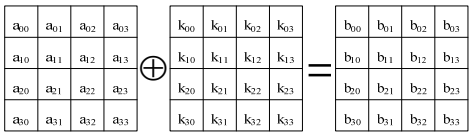

Fig.3 Schematic diagram of round key plus

The AES encryption algorithm supports different key lengths. It runs fast and has low memory requirements. However, in this algorithm, a large number of keys are needed to implement encryption and decryption, and the storage and management of keys are very difficult. Therefore, the use of AES alone cannot meet the needs of big data encryption and decryption in e-commerce networks.

IV. ECC ENCRYPTION ALGORITHM

In the asymmetric encryption algorithm, ECC has the advantages of high security, low storage space and low bandwidth requirements [11], which has been widely used. ECC algorithm is based on elliptic curve discrete logarithm problem. All the coefficients in the curve equation $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ are elements in the finite field $GF(p)$, where the elliptic curve $E(F_q)$ is defined as $E: y^2=x^3+ax+b(\bmod p)$, $a,b\in GF(p), 4a^3+27b^2(\bmod p)\neq 0$.

In E, point $P(x_1,y_1)$ and $Q(x_2,y_2)$ are selected randomly. Its operation is shown below:

(1) There is an infinite point O, $O+O=O$, $O+P=P$.

(2) The negative element of $P(x,y)$ is $(x,-y)$, $P+(-p)=O$.

(3) $P+Q=Q+P$.

In cryptography, it is supposed that the domain parameter of elliptic curve is $T=(p,a,b,G,n,h)$, where p,a,b is expressed to determine the elliptic curve, G is expressed as the base point, n is expressed as the order of G, and h is expressed as the integral part of the number of all points on the

curve divided by n. Any integer K_s is selected in $[1, n-1]$. $K_r = K_s G$ is calculated and the key pair (K_s, K_r) is determined, where K_s stands for the private key and K_r stands for the public key. Suppose that a wants to send message m to B. First of all, B's public key $(E(F_q), p, n, Q)$ should be looked up, and m is used to represent the domain element $m \in F_q$. A random number k is taken from $[1, n-1]$. B's public key is used to calculate $(x_1, y_1) : kP$, $(x_2, y_2) := kQ$, $C := mx_2$, and the encrypted data (x_1, y_1, C) is sent to B.

The decryption process of ECC is as follows: B uses the private key d to calculate $(x_2, y_2) := d(x_1, y_1)$ and $(x_2, y_2) := d(x_1, y_1)$ and then calculates $m := Cx_2^{-1}$ to obtain plaintext m.

ECC algorithm has short key length, low time complexity and small storage space. However, this algorithm is relatively complex and slow, and it cannot meet the needs of big data processing.

V. A Mixed Encryption Strategy Based on AES and ECC

To make up for the limitations of the two algorithms, a hybrid encryption strategy is obtained by combining AES with ECC. This encryption strategy is more secure, efficient and flexible. The advantages of the two excellent algorithms are combined.

The encryption and decryption process of the mixed encryption strategy is as follows:

(1) ECC algorithm is used to generate public and private keys: point $a, b,$ is selected on the elliptic curve; G is chosen according to $E_p(a, b)$; a random number K_s is take from $[1, n-1]$; point K_p is determined; let $K_p = K_s G$, and the key pair (K_s, K_p) is determined.

(2) AES algorithm is adopted to encrypt the plaintext: sender A takes K_A as AES key; random number $r, r \in \{1, 2, \cdots, n-1\}$ is taken; according to key pair (K_{Bs}, K_{Bp}) of receiver B $u = rK_{Bp}$, $R_1 = rG = (x_1, y_1)$, $v = x_1 K_A$ is obtained; binary group (u, v) is obtained and sent to A.

(3) AES decryption: x_1 is decrypted by $(x_1, y_1) = K_{BS}^{-1} u$, K_A is decrypted by $K_A = x_1^{-1} v$, and plaintext m is obtained.

VI. Performance Analysis

Compared with single encryption algorithm, hybrid encryption strategy can make full use of the advantages of the two algorithms. Firstly, the advantages of AES and ECC algorithms are analyzed.

E-commerce data packets of the same size are encrypted and decrypted by two symmetric encryption algorithms, DES and AES. The encryption and decryption speed of the algorithm is shown in Table II.

Table II Comparison of encryption and decryption speed between DES and AES

	DES	AES
Encryption speed	1.8Mb/s	5.1Mb/s
Decryption speed	1.9Mb/s	2.9Mb/s

It can be found from Table II that the encryption speed of DES is 1.8 Mb/s and the encrypted speed of AES is 5.1 Mb/s in encrypting data packet of the same size, indicating that AES is significantly faster. In terms of decryption speed, DES is 1.9 Mb/s and AES is 2.9 Mb/s, indicating that AES is significantly faster. The encryption speed of AES is about three times as fast as DES, and its decryption speed is about two times as fast as DES, indicating that the encryption and decryption efficiency of AES is significantly higher than DES.

The biggest problem with asymmetric encryption algorithms is encryption speed. The same e-commerce data packets are encrypted using ECC and another asymmetric encryption algorithm named RSA algorithm [12] to achieve the same level of security. The key lengths required for both algorithms are shown in Table III.

Table III Key length comparison between RSA and ECC

RSA	512	768	1024	2048
ECC	106	132	155	211

Table III shows that RSA requires a much larger key length than ECC in achieving the same security (2048 bits vs. 211 bits). Therefore, ECC requires significantly less computation than RSA in the encryption and decryption process.

AES and ECC have excellent performance in symmetric and asymmetric encryption algorithms respectively, so the hybrid algorithm based on AES and ECC is much better than other hybrid algorithms. In Fig. 4, RSA, ECC and hybrid encryption algorithms are used to decode the same file, and the relation between the decoding time and the size of key is shown.

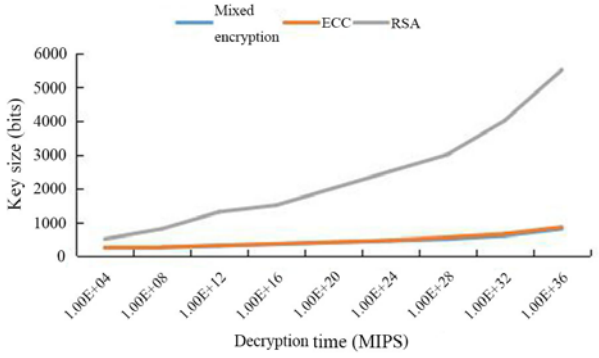

Fig. 4 Relationship between size of key and decryption time of different algorithms

As can be seen from Fig. 4, when the key size is less than 1000 bits, the key size required to decipher the file in the same

time varies little. However, as the decoding time increases, RSA algorithm needs a large key to ensure the same security. While the space complexity of ECC algorithm is small, the space complexity of mixed encryption strategy is smaller than that of ECC algorithm. It shows that mixed encryption has a good performance in big data encryption and has high security.

AES and ECC mixed encryption strategy is compared with AES and RSA mixed strategy. The encryption and decryption time of two encryption strategies for e-commerce data packets of different sizes is shown in Table IV.

Table IV Comparison of encryption and decryption time

Encryption and decryption time	10 M	20M	30M	40M	50M
AES+RSA (ms)	250	520	710	935	1200
AES+ECC (ms)	235	500	700	910	1000

Table IV shows that the time required by the two mixed encryption strategies for encryption and decryption increases with the increase of data packets. It can be found from the comparison of the two algorithms that the running time required by the mixed encryption strategy in this paper is significantly less than that of AES+RSA algorithm. It takes only 1000 ms to run 50 M packets. It shows that the encryption strategy in this paper has obvious advantages in the running time, and it can encrypt and decrypt the data in a shorter time. It has higher encryption and decryption efficiency.

VII. Discussion

With the development of social economy and information technology, people's consumption pattern and consumption concept have changed greatly. E-commerce has been developing better and better [13], occupying an increasingly important position in people's life and being favored by numerous consumers. In the complex and changeable network environment, the data security of e-commerce is greatly challenged [14]. E-commerce stores a lot of important asset information and financial information in an online database, which is of great significance to all parties involved in the transaction. It must be properly secured. Data encryption technology is a good method of security protection and has been well used in e-commerce.

Single encryption technology has both advantages and disadvantages. In order to achieve more efficient data encryption, mixed data encryption technology emerges. Mixed data encryption and can solve the key problem in symmetric encryption. It can also solve the problem that it is difficult to deal with big data work. In this paper, AES algorithm and ECC algorithm are selected for research. AES algorithm is fast, efficient and secure, but it also has the disadvantages of easy key leakage and difficult storage management in the process of encryption and decryption. ECC algorithm can save bandwidth and storage space, and has unique advantages in public and private key generation. However, there are also problems of slow operation speed and poor ability to process big data in public key encryption. Neither algorithm can meet the requirement of e-commerce security protection. Therefore, this paper designs a hybrid encryption strategy based on AES and ECC. The combination of the two algorithms can reduce computational overhead and improve encryption and decryption efficiency [15].

Public and private keys are generated by AES+ECC hybrid encryption strategy via ECC algorithm. Then encryption and decryption are performed by AES algorithm, which not only ensures the running speed of the algorithm, but also avoids AES key management difficulties and other problems. The performance analysis results show that AES and ECC are excellent algorithms in their own algorithm categories, and the performance of their mixed encryption strategies is obviously better than other mixed methods. When the same data packet is encrypted and decrypted, the key length required by the mixed encryption strategy is obviously less than that of other algorithms in the same decoding time, which ensures that the algorithm has faster computing speed and higher security. Table IV also shows that although the running time of the two mixed encryption strategies increases with the increase of data packets, it can be found from the comparison that the running time of AES+ECC algorithm is still smaller than that of AES+RSA algorithm. In the encryption and decryption of 50 M packets, the running time required by AES+RSA is 1200 ms, while the running time required by AES+ECC is 1000 ms, which proves the high running efficiency of the mixed encryption strategy in this paper and the advantages of the algorithm in processing the encryption and decryption of big data. The data in e-commerce network is very huge, and the common encryption strategy cannot effectively protect the data in the network, while the mixed encryption strategy can achieve this goal. Experimental results show that the hybrid strategy proposed in this paper has high running speed, high security and high efficiency, and can meet the requirements of e-commerce network security protection.

VIII. Conclusion

This study explored how to realize the security protection of e-commerce network. AES algorithm combined with ECC algorithm gives full play to the advantages of the two algorithms. AES+ECC hybrid encryption strategy is obtained, and the experiment shows that the algorithm has high security. The encryption and decryption of 50 M data packets can be realized in only 1200 ms using the mixed encryption strategy, which is fast enough to fully meet the needs of e-commerce network security protection. It has a high feasibility in the field of e-commerce.

References

[1] P. Prisha, H. F. Neo, T. S. Ong, et al., "E-commerce Security and Identity Integrity: The Future of Virtual Shopping," *J. Comput. Theor. Nanosci.*, vol. 23, no. 8, pp. 7849-7852, 2017.

[2] S. W. Guo, "e-commerce Information Management System Data Security Research," *Adv. Mater. Res.*, 971-973, pp. 4, 2014.

[3] E. S. Yang, L. You, Z. D. Wu, et al., "Massive Data Hybrid Encryption Algorithm Based on Cloud Computing," *Appl. Mech. Mater.*, 651-653, pp. 4, 2014.
[4] J. H. Cheon and J. Kim, "A Hybrid Scheme of public-key Encryption and A certain Homomorphic Encryption," *IEEE Trans. Inform. Forens. Secur.*, vol. 10, no. 5, pp. 1052-1063, 2015.
[5] L. Song, J. Qin, S. X. Liang, et al., "A Hybrid Encryption Scheme for Hadoop Based on Symmetric and Asymmetric Encryption," *Appl. Mech. Mater.*, vol. 598, pp. 691-694, 2014.
[6] A. Y. Nesterenko and A. V. Pugachev, "A new hybrid encryption scheme," *Moscow State Univ. Inform. Tech.*, pp. 56-71, 2015.
[7] P. Kuppuswamy and S. Q. Y. Al-khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm," *MIS REVIEW: Int. J.*, vol. 19, no. 2, pp. 13, 2014.
[8] C. M. Liu and Y. J. Sun, "The Application of Data Encryption in Network Security," *Appl. Mech. Mater.*, 513-517, pp. 3, 2014.
[9] S. C. Iyer, R. R. Sedamkar and S. Gupta, "A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach," *Proc. Comput. Sci.*, vol. 79, pp. 293-298, 2016.
[10] A. Sachdev and M. Bhansali, "important Cloud Computing Security using AES Algorithm," *Int. J. Comput. Appl.*, vol. 67, no. 9, pp. 19-23, 2014.
[11] R. D. O. Paulo, V. Delisandra Feltrim, A. F. M. Luciana, et al., "Energy Consumption Analysis of the Cryptographic Key Generation Process of RSA and ECC Algorithms in Embedded Systems," *IEEE Latin Am. Trans.*, vol. 12, no. 6, pp. 1141-114, 20148.
[12] S. Kuljanski, "RSA algorithm," *Military Tech. Courier*, vol. 58, no. 3, pp. 65-77, 2010.
[13] W. Y. Yu, Z. J. Ding, L. Liu, X. M. Wang and R. D. Crossley, "Petri net-based the methods for analyzing structural security in e-commerce business the processes," *J. Future Gener. Comput. Syst.*, pp. S0167739X17323671 -, 2018.
[14] A. H. Djumadi Barkatullah, "Does self-regulation provide legal protection and security to e-commerce consumers?," *Electr. Commerce Res. Appl.*, pp. S1567422318300565, 2018.
[15] N. Ashish, N. Priyadarsi, X. J. He, A. Jamdagni and D. Puthal, "A hybrid encryption technique for Secure-GLOR: Adaptive secure routing protocol for dynamic wireless mesh networks," *Future Gener. Comput. Syst.*, pp. S0167739X17322409, 2018.