Computers and Artificial Intelligence; Vol.3, No.4; 2026
E-ISSN: 3006-3728 P-ISSN: 3006-371X
DOI: https://doi.org/10.70267/cai.v3n4.186192
Published by: Zeus Press

A Review of General Information Encryption and Secure Network Transmission

Anran Huang*

School of Computer Science, Central China Normal University, Wuhan 430079, China

**Corresponding author: Anran Huang.*

Abstract

As learning, daily life, and work increasingly migrate online, general information transmitted over public channels faces increasingly severe network risks such as eavesdropping and disclosure, and data security has become a fundamental issue in the field of information security. In this context, this review focuses on the secure encryption and transmission of general information over networks, organizes the two technical routes of symmetric encryption [Data Encryption Standard (DES)/Advanced Encryption Standard (AES)] and asymmetric encryption [Rivest-Shamir-Adleman (RSA)/elliptic curve cryptography (ECC)] and their advantages and disadvantages, emphasizes the principles and measured performance of hybrid encryption (digital envelopes) that combines the two, supplements the Chinese commercial cryptographic system of SM2/SM3/SM4, then explains a layered transmission-security strategy that combines technology and management beyond algorithms, and finally discusses trends such as post-quantum cryptography, thereby forming a complete logical thread of distinctive strengths, hybrid complementarity, and system-level safeguards.

Keywords

symmetric encryption, AES, RSA, hybrid encryption, digital envelope, data transmission security, Chinese commercial cryptographic algorithms

1. Introduction

As office work, learning, social interaction, and other activities have almost entirely moved online, the risks of eavesdropping, tampering, and impersonation during information transmission have increased accordingly. Once data leave a personal computer, they must pass through network cables and other parties' servers, directly exposing the information to ordinary channels that others may inspect at will. Without encryption, information always faces many confidentiality problems; cryptography studies how to encrypt such information. In fact, cryptography concerns not only the resistance of an algorithm itself to attacks, but also algorithm strength, computation speed, key management, and practical limitations [1,2]. A defect in any link may reduce overall security. Therefore, this review does not discuss a single algorithm in isolation. Instead, it places the algorithms in a common application scenario and follows the question of how general information can be transmitted securely, connecting symmetric encryption, asymmetric encryption, hybrid systems, and management measures beyond algorithms, while also organizing recent research progress and development trends in these technologies.

© 2026 The Author(s). Authors retain copyright in their articles.

2. Symmetric and Asymmetric Cryptosystems

Modern encryption algorithms fall into many categories. The two most basic routes must first be distinguished according to whether encryption and decryption use the same key.

2.1 Symmetric Encryption

Symmetric encryption uses the same key for encryption and decryption, which requires the two parties to share the key in advance. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are the two most common representative algorithms. The mechanism resembles a lock that can be opened with the same key. Its structure is not complex, but its speed is high; therefore, symmetric encryption is generally preferred for encrypting large files. DES is introduced first. It has a 64-bit block size, but the actually effective key is only 56 bits, and its internal operation uses a 16-round Feistel structure. The fundamental defect of DES is its insufficient key length, with a search space of only 2^{56}. The Electronic Frontier Foundation (EFF) once used a dedicated device to crack it in only dozens of hours [1]. In the face of substantial computing power, an ingenious structure is of little use when the key length is insufficient, and DES was therefore gradually phased out.

AES later replaced DES; it is essentially the Rijndael algorithm [3]. Its block size is fixed at 128 bits, and it provides three key lengths of 128, 192, and 256 bits, corresponding to 10, 12, and 14 rounds, respectively. Its strength is far greater than that of DES, providing a higher level of security. Each round mainly performs four operations: byte substitution (SubBytes), row shifting (ShiftRows), column mixing (MixColumns), and round-key addition (AddRoundKey) [4-7]. The underlying operations are conducted over the Galois field GF (2^8), which corresponds precisely to Shannon's concepts of diffusion and confusion. One easily overlooked principle is Kerckhoffs's principle [2]: although the algorithm is public, its security depends only on the secrecy of the key. Consequently, these steps are publicly available while security can still be maintained. The problem with symmetric encryption appears elsewhere: when n people need pairwise communication, n(n-1)/2 keys must be maintained. Once the number of people increases, secure key distribution becomes another problem that must be solved. In addition, symmetric encryption cannot inherently provide digital signatures [1].

Analysis of existing studies shows that the evolution from DES to AES was not merely an increase in key length; it reflected a dynamic contest between the security of encryption algorithms and actual computing capability. Although DES could meet basic information-security needs in the early period of computing, its relatively small key space gradually became a fatal defect as computing capability increased. AES significantly improved security strength through a much larger key space and a design better suited to modern environments. Therefore, the core advantage of symmetric cryptosystems is their high efficiency in processing large-scale data, but their persistent defect is the inability to balance efficient big-data processing with secure key distribution. This also means that increasing only the encryption strength of the algorithm cannot successfully solve security problems in network transmission.

2.2 Asymmetric Encryption

Asymmetric encryption is also called public-key cryptography [8]. It assigns each person a pair of mathematically linked keys: the public key may be disclosed, whereas the private key must be properly protected. Taking Rivest-Shamir-Adleman (RSA) encryption as an example, two large prime numbers p and q are first selected, and n is set equal to their product. The encryption operation is $C = m^e \bmod n$, and the decryption operation is $m = C^d \bmod n$ [9]. Its security arises from the computational difficulty of factoring n into p and q. Because there is no need to worry about others seeing the public key, the distribution problem is alleviated: n users need to manage only 2n keys, and digital signatures can also be produced.

However, public-key cryptography is not without shortcomings. RSA relies on modular exponentiation with large integers and is much slower than AES [10], so it can encrypt only relatively short data. Many restrictions also exist in practical implementations: p and q must not be too close, the private exponent d must not be too small, and several users must not share the same modulus n [11]. Otherwise, specific attacks may occur. The security of the algorithm itself does not mean that an implementation written from it is necessarily secure. Elliptic curve cryptography (ECC) is also often compared with RSA. At the same security strength,

© 2026 The Author(s). Authors retain copyright in their articles.

160-bit ECC is approximately equivalent to 1024-bit RSA, and 256-bit ECC is approximately equivalent to 3072-bit RSA. ECC requires less storage and bandwidth [12,13].

Overall, the main value of asymmetric cryptosystems relative to symmetric cryptosystems does not lie in handling large-scale data-encryption tasks, but in solving problems such as key distribution, identity authentication, and digital signatures. RSA has a mature system and is widely used, but its high computational overhead limits its direct application in scenarios involving large amounts of data. ECC reduces storage and communication overhead through shorter key lengths and is therefore more suitable for resource-constrained application environments. Thus, asymmetric and symmetric algorithms are not simply substitutes for each other; instead, their functions are complementary, which directly supports the subsequent formation of hybrid cryptosystems.

3. Hybrid Encryption and Digital Envelopes

AES encrypts quickly but cannot ensure secure key transmission; RSA facilitates key transmission but is itself slow at encryption. To address this contradiction, engineering practice combines the two in a scheme called hybrid encryption, also known as a digital envelope [14]. The specific process is as follows. The sender temporarily generates a random symmetric session key and uses AES to encrypt the actual file content rapidly. The sender then uses the recipient's RSA public key to encrypt this short session key and finally packages and sends the ciphertext together with the encrypted session key. The recipient performs the reverse operation, first using the private key to recover the session key and then using that key to decrypt the file content. The process can be explained using a safe as an example: the file content is locked in a strong safe, while the key to the safe is placed separately in a small key box that is convenient to mail. A new session key is generated each time and discarded after use. Even if one session key is disclosed, only that file is affected; this mechanism can reduce the scope of the impact caused by a single key disclosure.

The slowness of RSA can be illustrated with measured data. In 2016, Chang Xu [15] conducted a set of comparisons on the Qt platform, and the figures are relatively intuitive. Two test files were used, with sizes of 1,923 KB and 21,840 KB. For the large file of approximately 21 MB, AES encryption took only 2.32 s and decryption only 2.83 s, whereas RSA encryption took 58.33 s and decryption took 1,185.45 s. Decryption was an order of magnitude slower than encryption because of modular exponentiation with large integers. These experimental data not only demonstrate that AES is faster than RSA, but also show that the two types of algorithms have entirely different functional roles in network transmission. If RSA is used directly to encrypt large files, the computational cost is very high. If RSA is limited to protecting the session key and AES is responsible for encrypting the file content, a relatively reasonable division of labor can be established between security and transmission efficiency. Hybrid encryption is therefore not a simple superposition of two algorithms; its value lies in using the advantages of different cryptosystems to complete a task collaboratively. In specific practical applications, a common approach is to place the RSA-encrypted session key in the file header and the AES ciphertext after it. The recipient first reads the header to recover the key and then decrypts the following file content. This system has also been widely used in engineering practice. In work conducted in 2025, Mengmeng Yang et al. [16] selected sensitive personal information such as names and identity-card numbers as the objects, used DES-RSA hybrid encryption, and combined it with measures such as graded permissions and periodic session-key replacement, so that unauthorized personnel could not view sensitive fields. The RSA private key was protected by a password through a hash algorithm. In similar studies, Zaifeng Tan et al. [17] applied DES-RSA hybrid encryption to secure data transmission over wireless networks, and Xiaohua Li [18] also discussed the application of hybrid encryption in computer-network data transmission. It is noteworthy that some application-oriented studies from 2025 still used DES-RSA combinations. This indicates that some studies placed greater emphasis on implementing established technical frameworks in specific scenarios, while their algorithm selection remained at some distance from current mainstream practice. This actually shows that the hybrid-encryption framework has long been established and that current additions mainly concern scenario adaptation and engineering details rather than the invention of an entirely new algorithm.

Therefore, judging from the development of the existing literature, the basic idea of hybrid encryption is already relatively mature, and repeatedly verifying that symmetric encryption is fast while asymmetric encryption is suitable for key protection produces relatively limited additional academic value. The issues that

© 2026 The Author(s). Authors retain copyright in their articles.

now deserve more attention are how to adjust the key-update cycle, algorithm combination, identity-authentication mechanism, and resource consumption according to different application environments. In other words, the focus of hybrid-encryption research is gradually shifting from proposing a combination method to making that method more secure, stable, and easy to deploy in specific scenarios.

4. Chinese Commercial Cryptographic Algorithms

While attention is paid to internationally mainstream algorithms such as AES and RSA, China's independently developed commercial cryptographic system is also an important component of data-encryption systems. It mainly includes three parts: the SM4 symmetric block cipher (SM4), whose block and key lengths are both 128 bits and which performs 32 rounds of iterative operations under standard GB/T 32907; the SM2 elliptic-curve public-key cryptographic algorithm (SM2), specified in GB/T 32918; and the SM3 cryptographic hash algorithm (SM3), specified in GB/T 32905, which outputs a 256-bit digest. Their functions broadly correspond to those of AES, ECC, and the Secure Hash Algorithm (SHA), respectively, and they can also form a Chinese digital envelope: SM4 encrypts the data, SM2 protects the key, and SM3 generates the data digest and can be combined with mechanisms such as digital signatures to provide integrity and source authentication. After the United States PRISM incident, China accelerated the process of using domestic algorithms to replace foreign algorithms; this is the most practical background of Chinese commercial cryptography.

From the perspective of algorithm structure, the plaintext, key, and ciphertext of SM4 are all 128 bits. The key-expansion step first calculates 32 round keys, and the round function combines linear and nonlinear transformations over 32 iterations. The decryption structure is the same as the encryption structure, except that the round keys are used in the reverse order. In 2020, Jiongwei Jiang et al. [19] tested SM4 on an STM32 embedded board with a clock frequency of 168 MHz. Two data points are worth mentioning. When plaintext was encrypted into ciphertext, the difference coefficient was approximately 0.531. When only one input bit was changed, the difference coefficient between the two ciphertext versions still reached 0.453 (the ideal value is approximately 0.5). This indicates a favorable avalanche effect: a slight input change makes the ciphertext almost unrecognizable, making reverse inference difficult for an attacker. The experiment also confirmed that SM4 could perform real-time encryption and decryption on computing-constrained small devices such as an Internet of Vehicles telematics box (T-BOX); once back-end verification failed after decryption, the data packet was discarded directly. In recent years, the financial, government, and critical-information-infrastructure sectors have continuously advanced migration to Chinese commercial cryptography. Chinese and international algorithms operate in parallel, with gradual replacement, which is an unavoidable aspect of China's data-encryption process. Corresponding SM2, SM3, and SM4 with ECC, SHA, and AES, respectively, reveals clear functional similarities between the Chinese cryptographic system and the internationally mainstream algorithms discussed above. However, the research significance is not limited to simply replacing existing algorithms. For actual network transmission, the more important task is to form an integrated cryptographic system covering data encryption, identity authentication, and integrity protection. Therefore, evaluation of a Chinese commercial cryptographic scheme must not compare only the operating speed or security parameters of a single algorithm; it should also examine standards adaptation, system-migration costs, application scenarios, and overall deployment conditions. In other words, research on Chinese commercial cryptography concerns not only whether an algorithm can be used, but also whether it can be used stably in an actual system.

5. Technical and Management System for Transmission Security

It should be noted that data encryption is not a sufficient condition for transmission security. Information faces many threats during transmission, including eavesdropping, impersonation, content tampering, and message replay [20,21]. If the three requirements of confidentiality, integrity, and availability - commonly called the confidentiality, integrity, and availability (CIA) triad - are to be met, a single encryption algorithm cannot satisfy these needs. Technically, a layered model is required. The core layer consists of algorithms such as AES, RSA, and the SM series, together with hybrid cryptosystems formed by their combination. The supporting layer includes firewalls, intrusion detection, virtual private networks (VPNs), message digests, digital certificates, and digital signatures. In addition, new technologies such as blockchain, artificial intelligence, and edge computing play supplementary roles [22]. A digital certificate can determine whether

© 2026 The Author(s). Authors retain copyright in their articles.

the current public key actually belongs to the other party, while a digital signature can simultaneously ensure that the source is authentic and that the content has not been tampered with. In coordination with encryption, these two mechanisms can effectively prevent man-in-the-middle attacks [23].

Management is also indispensable. Some literature summarizes it as a closed-loop model of prevention, monitoring, and traceability [22]. Data are first classified as general, important, or sensitive; graded warning measures are implemented during transmission; and logs are retained after transmission to facilitate investigation. These steps are accompanied by security training, access control, least-privilege settings, emergency backups, and other measures [21]. Specifically, encryption addresses confidentiality, while the complete model must further achieve the goals that an intruder cannot enter, cannot make changes, cannot deny an action, and can be traced. This system already has a mature real-world application: the small lock in a browser's address bar [2], namely Hypertext Transfer Protocol Secure/Transport Layer Security (HTTPS/TLS). Behind it is the same combination of asymmetric key negotiation, symmetric content encryption, and certificate-based identity verification, although the process is encapsulated and therefore almost imperceptible.

Accordingly, secure network transmission is not a single-point problem of selecting a sufficiently strong encryption algorithm. It is a system problem jointly composed of confidentiality, integrity, identity authentication, and operations management. Algorithms provide the cryptographic security foundation; protocols and certificates address trust between communicating parties; and permission control, logs, and emergency mechanisms determine whether security measures can continue to function in an actual environment. Therefore, from the perspective of network-transmission scenarios, establishing a layered protection system has greater practical significance than simply comparing the performance of one algorithm.

6. Research Trends and Conclusion

The preceding studies show that a relatively clear technical division of labor has formed in the field of secure transmission of general information. Symmetric cryptography mainly undertakes efficient data-encryption tasks; asymmetric cryptography undertakes key protection and identity-related functions; hybrid encryption organizes the two into a deployable transmission scheme; and certificates, signatures, and management mechanisms further address security needs that cannot be covered by a single algorithm. The core question in current research has therefore gradually shifted from whether encryption can be implemented to how security, efficiency, and deployability can be balanced in different application environments. AES, RSA, and hybrid envelopes have already reached a high level of maturity. Judging from the recent literature retrieved in this review, related research remains concentrated on application implementation, scenario adaptation, and engineering optimization. On the one hand, this shows that these technologies retain vitality; on the other hand, it reflects substantial homogeneity and a lack of novelty in their principles. Genuine development is concentrated mainly on lightweight implementation, adaptation to specific scenarios, and deployment of Chinese commercial cryptography. At the same time, the challenges posed by future quantum computing are becoming increasingly prominent. Once quantum computing becomes sufficiently powerful, Shor's algorithm [2] will be able to break efficiently the number-theoretic problems on which RSA and ECC depend, creating the potential risk of harvesting encrypted data now and decrypting them after a future quantum computer becomes available. The National Institute of Standards and Technology (NIST) has begun to advance post-quantum standards such as the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) [24], while researchers are also actively studying areas such as chaos-based cryptography and neural-network cryptography. Integrating encryption, authentication, and management so that ordinary people without cryptographic training can use them correctly is gradually becoming as important as algorithm strength.

In retrospect, the secure transmission of general information cannot be accomplished by any single algorithm. Symmetric encryption provides speed, asymmetric encryption emphasizes convenient key distribution, hybrid encryption combines the two into a usable digital envelope, Chinese commercial cryptography provides an independently developed solution, and certificates, signatures, and graded management establish another layer of protection beyond algorithms. Once the thread of distinctive strengths, hybrid complementarity, and system-level safeguards is organized, the internal logic of this body of literature becomes clear. For beginners, it is better to understand this main thread thoroughly before pursuing new terminology and then choose one direction among algorithm optimization, protocol design, and security

© 2026 The Author(s). Authors retain copyright in their articles.

management for in-depth study. This can establish a solid foundation for either studying post-quantum migration in the future or developing a genuinely practical encryption tool.

References

[1] Qin, Z. (2004). Cryptography algorithm: Survey and trends. *Journal of Computer Applications, 24*(2), 1-4.

[2] Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

[3] Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES - The Advanced Encryption Standard*. Springer.

[4] He, M., & Lin, H. (2002). Principles and implementation of the Advanced Encryption Standard (AES). *Application Research of Computers, 19*(12), 61-63.

[5] Zhang, J., Guo, X., & Fu, X. (2011). Analysis of the AES encryption algorithm and its application in information security. *Netinfo Security*, (5), 31-33.

[6] Zhao, X. (2010). Implementation and application of the AES encryption algorithm. *Journal of Changshu Institute of Technology, 24*(2), 105-110.

[7] National Institute of Standards and Technology. (2001). *Advanced Encryption Standard (AES)* (FIPS PUB 197). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.197

[8] Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644-654. https://doi.org/10.1109/TIT.1976.1055638

[9] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120-126. https://doi.org/10.1145/359340.359342

[10] Li, Y., Liu, Q., Hao, L., & Zhou, B. (2010). Efficient variant of the RSA cryptosystem. *Journal of Computer Applications, 30*(9), 2393-2397.

[11] Chen, C., & Zhu, Z. (2006). Applications and implementation details of the RSA algorithm. *Computer Engineering & Science, 28*(9), 13-14, 87.

[12] Wang, X., Sun, T., & Ma, J. (2023). Research progress of the RSA algorithm in network data transmission. *Computer Science, 50*(S1), 703-709.

[13] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5

[14] Wu, M. (2013). *Research on DES and RSA hybrid encryption algorithms* [Master's thesis, Harbin Institute of Technology].

[15] Xu, C. (2016). Application of AES and RSA hybrid encryption technology in network data transmission. *Wireless Internet Technology*, (13), 142-144.

[16] Yang, M., Sun, T., Yang, Z., & Sha, S. (2025). Secure transmission method for sensitive communication-network data based on DES-RSA hybrid encryption. *Changjiang Information & Communications, 38*(8), 175-177, 186.https://doi.org/10.20153/j.issn.2096-9759.2025.08.052.

[17] Tan, Z., & Gao, Z. (2025). A secure data-transmission method for wireless networks based on DES-RSA hybrid encryption. *Automation & Instrumentation*, (12), 42-46.

[18] Li, X. (2025). Application of hybrid encryption algorithms in computer-network data-transmission security technology. *Encyclopedic Knowledge*, (18), 14-16.

[19] Jiang, J., Hong, Z., & Chen, Z. (2020). Application of the SM4 encryption algorithm in the Internet of Vehicles. *China Computer & Network, 46*(3), 58-60.

[20] Wu, X., Zhong, F., & Liu, L. (2012). Data-encryption technology in secure network transmission. *Journal of Guizhou Meteorology, 36*(1), 56-57.

© 2026 The Author(s). Authors retain copyright in their articles.

[21] Wang, Z. (2025). The importance of network security in data transmission and corresponding countermeasures. *China Broadband, 21*(2), 58-60.

[22] Liu, D. (2026). Exploration of data-transmission security strategies in an information environment. *Digital Communication World*, (6), 12-14.

[23] Huang, L. (2025). Analysis of data-transmission security strategies in computer networks. *Applications of IC, 42*(11), 598-599.

[24] National Institute of Standards and Technology. (2024). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). https://doi.org/10.6028/NIST.FIPS.203.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Copyrights

Copyright for this article is retained by the author (s), with first publication rights granted to the journal. This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).

© 2026 The Author(s). Authors retain copyright in their articles.