Proceedings of the 3rd International Conference on Mechatronics and Smart Systems
DOI: 10.54254/2755-2721/117/2025.20951

Application of Digital Signatures in the Field of E-commerce

Jian Mu[1,a,*]

[1]*International School of Information Science & Engineering, Dalian University of Technology, Linggong Road, Dalian, China*
a. jianmuv@gmail.com
**corresponding author*

Abstract: As a critical mechanism to ensure e-commerce information security, digital signatures have been widely used in core scenarios such as identity authentication, data integrity verification, and non-repudiation assurance. This paper systematically reviews the technical principles of digital signatures and their practical applications in the field of e-commerce. It further investigates application processes and security characteristics of digital signatures for different application scenarios in centralized and decentralized trust models, such as business-to-customer (B2C) transactions, business-to-business (B2B) transactions, and Bitcoin peer-to-peer (P2P) transactions. At the same time, signature schemes based on classical algorithms such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), as well as cutting-edge signature technologies based on post-quantum cryptography, are discussed. Finally, combined with future technology trends, this paper looks forward to the innovative directions of digital signatures in lightweight design, privacy protection, and quantization, providing theoretical support and practical reference for the development of digital signatures in the field of e-commerce.

Keywords: Digital signature, e-commerce security, asymmetric encryption, blockchain and privacy protection, lightweight and quantum security.

1. Introduction

With the rapid development of information technology, e-commerce has become an important part of the global economy. However, the booming development of e-commerce is also accompanied by a significant increase in information security risks. Problems such as data tampering, identity fraud and transaction denial are becoming increasingly prominent. In this context, how to ensure the security, integrity and non-repudiation of data transmission has become a critical challenge of concern to the industry. As a security mechanism based on asymmetric encryption technology, digital signatures provide an effective solution to the above problems. More and more countries have enacted laws related to electronic signatures, clarifying that the legal effect of reliable electronic signatures is equivalent to that of handwritten signatures or seals, laying a solid legal foundation for the application and promotion of digital signatures.

The core mechanisms of digital signature are to sign information with a private key and verify it with a public key to ensure the authenticity and integrity of the data and the non-repudiation of the signer's identity. Since the advent of algorithms such as Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC), digital signature technology has gradually matured and has been widely

DOI: 10.54254/2755-2721/117/2025.20951

used in the field of e-commerce, especially in business-to-customer (B2C), business-to-business (B2B) and peer-to-peer (P2P) transactions.

In recent years, the global e-commerce market has experienced rapid expansion, and the demand for applications such as cross-border transactions and mobile payments has continued to grow. However, with the expansion of transaction scale, security threats and privacy breaches have become more serious. For example, in a centralized trust model, the single point failure risk of certificate authority (CA) nodes is significant; while in a decentralized model, the direct trust relationship of transactions requires a more efficient and secure verification mechanism. In this case, digital signature technology not only ensures data security for e-commerce, but also promotes the development of emerging technologies such as electronic payment and blockchain.

In addition, with the widespread adoption of smart devices and the Internet of Things (IoT), the efficiency of signature calculations on resource-constrained devices has become a major challenge. The traditional RSA algorithm is cumbersome and inefficient in these scenarios. In response, lightweight ECC and signature algorithms based on post-quantum cryptography have brought new solutions to resource-constrained devices. Furthermore, privacy protection, edge computing, and quantum security have also become important areas of current digital signature research.

In the field of digital signatures, numerous studies have demonstrated their critical role in e-commerce:

In terms of the implementation principle of digital signatures, Li et al. investigated the core role of public key infrastructure (PKI) in identity authentication and proposed a solution to transfer trust through certificate chains [1]. Yu et al. explored the secure e-commerce transaction process constructed by combining PKI with digital signatures in a centralized trust model [2]. Shaikh et al. conducted a detailed study on the lightweight design of ECC [3]. Liu et al. and Li et al. respectively studied lattice-based and hash-based digital signature algorithms in post-quantum cryptography [4,5]. Luo et al. and Li et al. proposed the vulnerabilities of existing blind signature schemes and explored the core properties of blind signatures [6,7]. Yin et al. pioneered a scenario demonstration of quantum e-commerce applications [8].

This paper aims to review the application and development of digital signatures in the field of e-commerce. It analyzes the technical principles and application processes of digital signatures, explores the application scenarios of digital signatures in centralized and decentralized trust models; compare the advantages and applicability of signature technologies based on classical algorithms such as RSA and ECC and post-quantum cryptography. Furthermore, this paper explores the innovative potential of digital signatures in future development directions such as lightweight design, privacy protection and quantum security.

2. The Implementation Principles of Digital Signatures

2.1. Digital Signatures

The core principle is asymmetric encryption technology. The signer uses a private key to encrypt the message digest to generate a signature. In order mitigate the computational cost of asymmetric encryption, it is usually chosen to encrypt the message digest content instead of processing the complete information. The receiver decrypts the signature through the signer's public key and compares the decrypted message digest with the original message digest to complete the verification.

Asymmetric encryption systems rely on a pair of keys, namely a public and a private, to perform encrypt and decrypt operations. The public key is available to anyone and can be used to encrypt information, whereas the private key is strictly confidential and can be decrypted solely by its owner. Digital signature protocols leverage this mechanism to ensure the authenticity and integrity of messages.

DOI: 10.54254/2755-2721/117/2025.20951

Take Alice as an example: her public key is publicly available and her private key is securely held by herself. When she wants to sign a document, she first selects a hash function to convert the document into a unique digest. Then, she encrypts the summary with her private key to generate a digital signature for the document and publishes the original document and the signature together.

As shown in Figure 1, when verifying the signature, the recipient Bob decrypts the signature using the public key published by Alice and generates a summary of the document using the same hash function. He then compares the two summary values. A match indicates, it means that the document was indeed signed by Alice and has not been tampered with; otherwise, the signature is invalid.

The core of this mechanism is that only those who hold the private key can generate a valid signature, while the public nature of the public key allows anyone to verify the signature. Currently, the commonly used implementations of digital signatures include RSA-based schemes and schemes using elliptic curve technology, both of which are widely used in the fields of secure communication and electronic authentication [9].

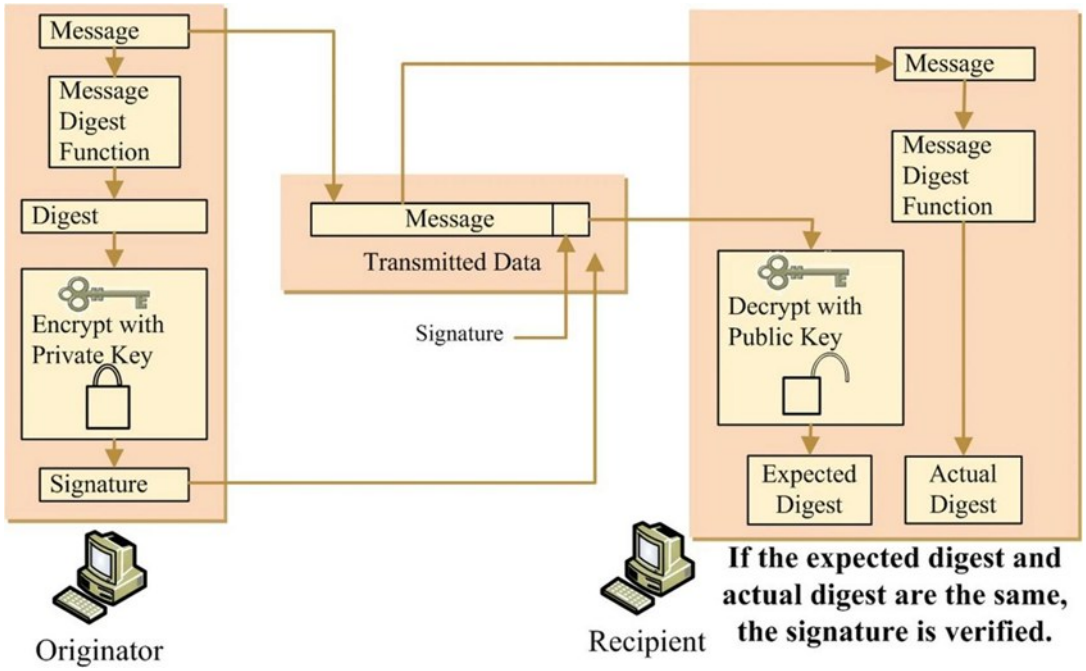

Figure 1: Data security digital signature process basic on RSA[10].

2.2. PKI

The implementation of digital signatures relies on the PKI. PKI is a security system based on asymmetric cryptographic algorithms and digital certificates. Its core purpose is to pass trust along the trust path, commonly referred to as a certificate chain, through a trust anchor-typically the root certificate of a CA, to achieve identity authentication and encrypted communication.

2.2.1. Fundamental Components

The PKI authentication model includes: root CA server, database server, registration authority(RA), security server and directory server (LDAP). This model facilitates trust propagation by issuing certificates and building a certificate chain through the collaboration of between the root CA, subordinate secondary CAs, and system server CAs. This hierarchical structure ensures the security and credibility of the authentication process. The detailed structure of the certificate chain is illustrated in Figure 2.

DOI: 10.54254/2755-2721/117/2025.20951

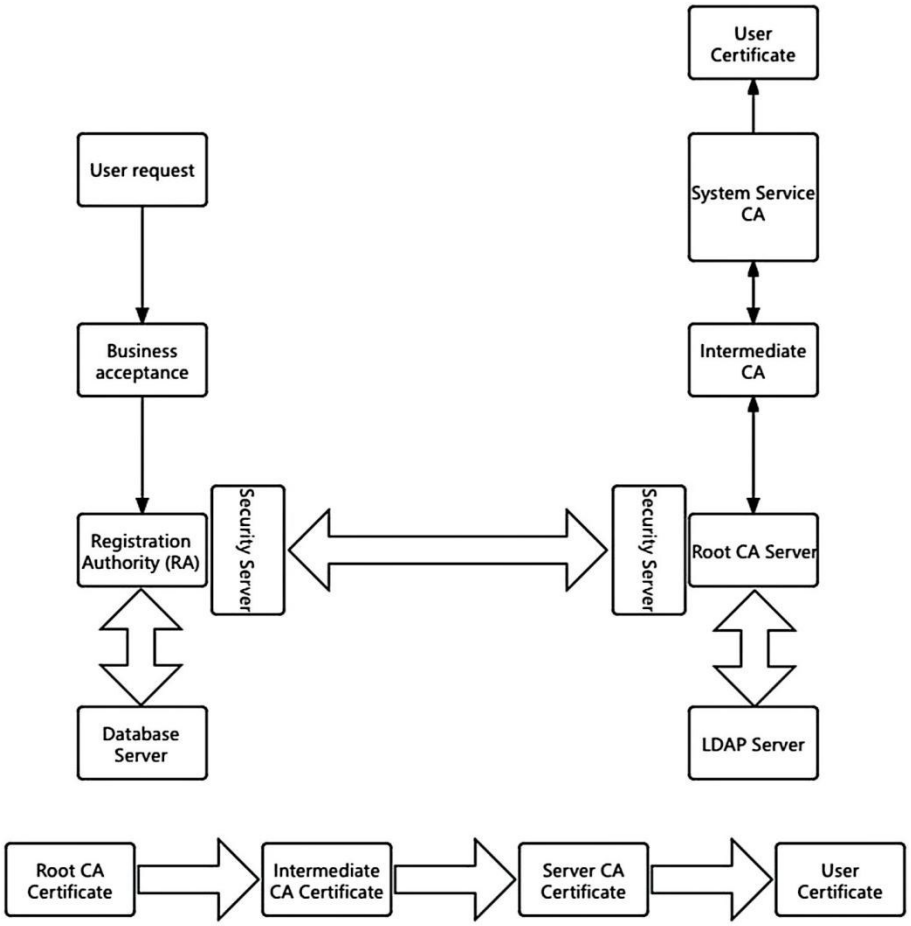

Figure 2: Traditional PKI Authentication Model and Certificate Chain Diagram[1].

2.2.2. Challenges of PKI Centralization

Traditional PKI systems rely heavily on CA nodes for identity authentication and certificate management. This reliance introduces a risk of Single Point of Failure(SPoF), which is primarily manifested in CA downtime, attacks, and key loss or leakage.

When the CA center experiences hardware failures, software crashes or power outages, the entire system's operations, including certificate application, verification, and revocation are disrupted. This disruption breaks the trust chain, paralyzes system functions, prevents new users from obtaining certificates and existing users from completing identity authentication normally. In addition, CA nodes are easily targeted by attackers. Common attack methods include denial of service attacks (DoS/DDoS), where attackers overload CA servers with a large number of malicious requests and fail to respond to normal requests; malicious intrusions may cause attackers to forge or issue illegal certificates, undermining the security and credibility of the system. If the CA database is attacked and the key or certificate is stolen, the trust system will be completely invalidated.

A particularly critical issue arises because the CA's private key, which is the trust foundation of the PKI system and is used to issue certificates, is vulnerable to compromise. Once the private key is leaked, attackers can forge legitimate certificates, deceive users, and undermine the security of communications, resulting in the inability to ensure data confidentiality and integrity, and the trust foundation of the entire PKI system will collapse. Therefore, the failure or security issues of the CA

DOI: 10.54254/2755-2721/117/2025.20951

node will directly affect the normal operation of the entire PKI system. How to prevent and solve this SPoF problem is the core challenge facing the PKI system.

2.2.3. PKI Authentication Procedure

The PKI identity authentication process can be categorized into two scenarios: intra-domain authentication and cross-domain authentication [1]:

Intra-domain authentication refers to the authentication between users and servers within the same PKI domain. As shown in Figure 3, the process includes the following steps: First, the user initiates an authentication request to the server through the client. After receiving the request, the server generates a true random number and returns it to the user. The user then signs the random number with his or her private key to generate a signature value, and sends the signature value together with the user certificate to the server.

After receiving the data sent by the user, the server first parses the user certificate, extracts the public key from it, and uses the public key to verify the validity of the signature value. Next, the server will also perform a series of validity verifications on the certificate, including checking whether the certificate is within the validity period, confirming whether it is included in the certificate revocation list (CRL), and parsing and verifying the entire certificate chain to ensure that the signature value of the root certificate is valid and credible.

After completing all verification operations, the server returns the conclusion of whether the authentication is successful to the user based on the verification results. If the verification is successful, it means that the user's identity is credible and the authentication process is successfully completed; otherwise, the authentication fails and the user is considered untrustworthy.

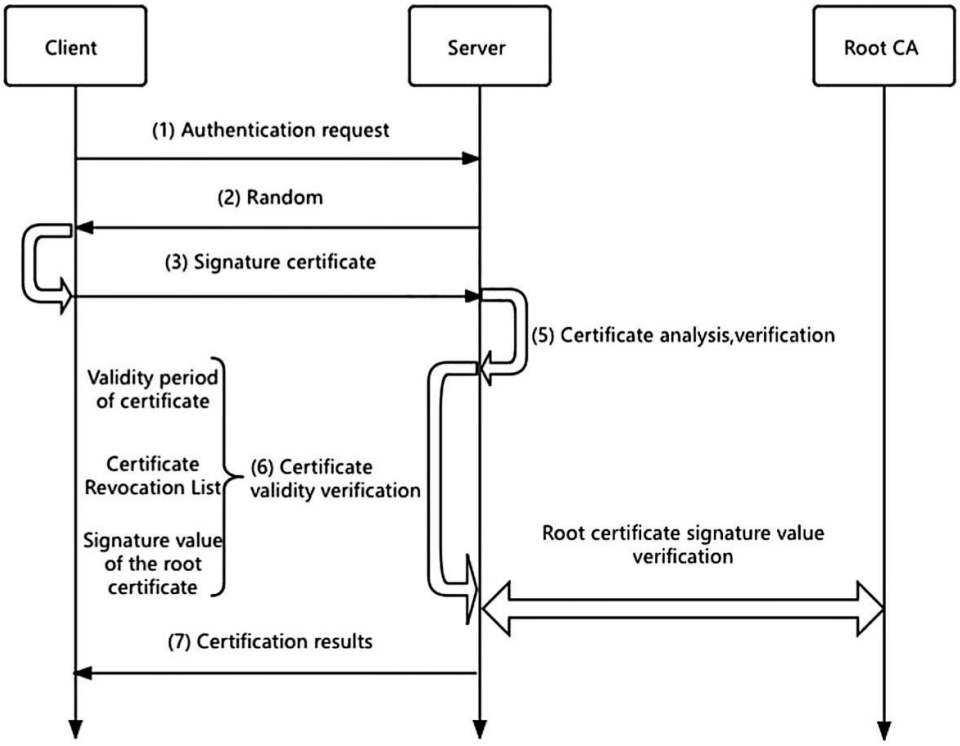

Figure 3: Intra-Domain PKI Identity Authentication Process[1].

DOI: 10.54254/2755-2721/117/2025.20951

Cross-domain identity authentication refers to the process for identity authentication when the user and the server belong to different PKI domains. As shown in Figure 4, the specific process is as follows: The user in domain A submits a certificate to the server in domain B and requests authentication. After identifies that the certificate originates from domain A, the server in domain B initiates a cross-certification request to the root CA of this domain. Subsequently, the root CA of domain B cross-certifies with the root CA of domain A, generates a cross-certificate, and establishes a trust relationship between the two domains.

Once the trust relationship is established, the server in domain B generates a random number and returns it to the user. The user signs the random number with the private key, and then submits the signature value and certificate to the server in domain B again. After receiving the data, the server in domain B parses the user certificate, verifies the validity of the signature value, and constructs the certificate path in reverse, including the relevant certificate chains of domain A and domain B, to ensure the integrity and validity of the certificate chain.

Finally, the server in domain B returns the authentication result to the user based on all the verification results. If all links are successfully verified, the user's identity is recognized and the authentication is successfully completed; otherwise, the authentication fails and the user cannot pass the verification.

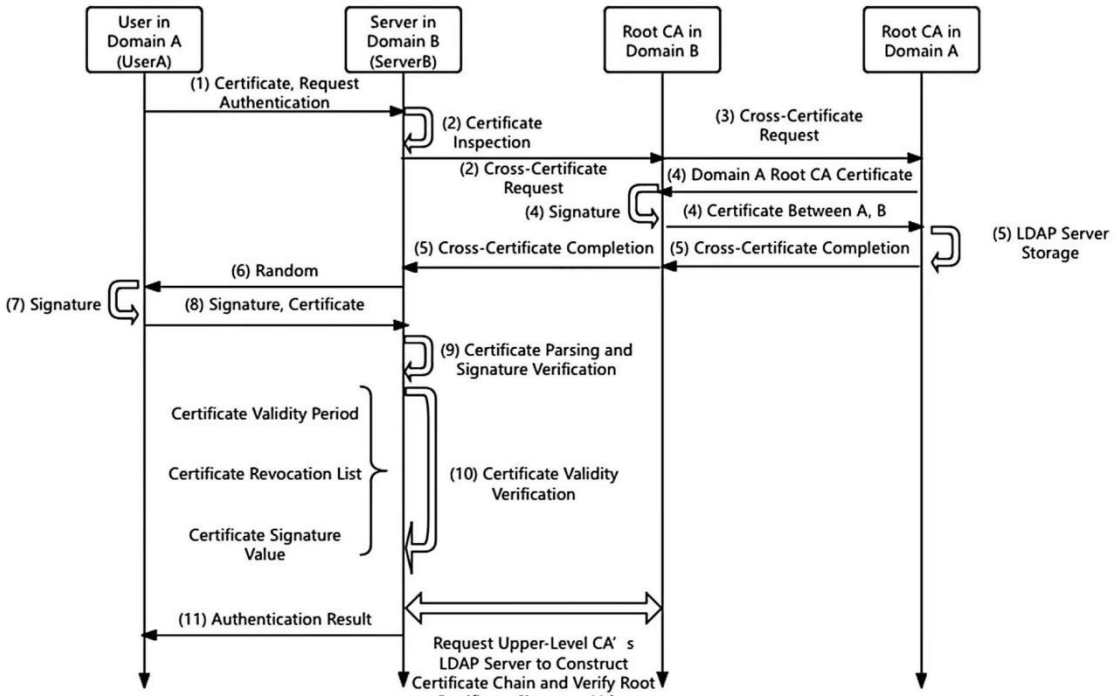

Figure 4: Cross-Domain PKI Identity Authentication Process[1].

3. Applications of Digital Signatures in Different E-Commerce Scenarios

3.1. Centralized Trust Model

In the B2C scenario, Electronic Data Interchange (EDI) security solutions usually include the following core steps:

First, the two transaction parties (sender and receiver) need to show each other digital certificates issued by the CA to verify the legitimacy and validity of the other party's certificate. This can be done

DOI: 10.54254/2755-2721/117/2025.20951

by checking the certificate library and revocation list, and obtaining the other party's RSA public key through the certificate.

Next, the sender encrypts the EDI message. The sender first computes a message digest of the EDI message using the MD5 algorithm, and then digitally signs the summary using its own RSA private key to generate a signature summary. Then, the signature summary is attached to the message, and the entire message and signature are encrypted using the DES algorithm. After that, the sender encrypts the DES key using the receiver's RSA public key, and finally sends the encrypted message and encrypted DES key to the receiver.

After receiving the data, the receiver needs to verify the integrity of the data. The receiver uses its own RSA private key to decrypt and obtain the DES key, and then uses the decrypted DES key to decrypt the message and signature digest. Subsequently, the receiver uses the sender's RSA public key to decrypt the signature digest, obtain the sender's summary value, and calculate the digest of the decrypted message independently. By comparing the two summary values, the receiver can confirm whether the message has not been tampered with and whether the sender is an entity that legally possesses the CA certificate.

Finally, in order to achieve the receiver's identity authentication and non-repudiation, the receiver processes the returned message according to the same steps. The receiver calculates the message digest and signs it with its own RSA private key, encrypts the signature and message, and sends them to the sender. The sender decrypts and verifies the signature to confirm the receiver's identity, thereby completing the other party's authentication. This process guarantees the security of communication, data integrity, and non-repudiation of identity[2].

3.2. Decentralized Trust Model

3.2.1. B2B Scenario

In the B2B process, as both parties of the EDI transaction are familiar with each other and have pre-established a dedicated encryption and authentication algorithm, the other party's RSA public key is known and the first step can be omitted. The remaining steps of the process are essentially identical to those described above.

3.2.2. P2P Transactions in Bitcoin Trading Scenarios

Digital signatures play a key role in ensuring address generation and fund security in the Bitcoin system. Bitcoin holders can maintain multiple Bitcoin addresses. Bitcoin addresses are generated by hashing and encoding public keys and are public identifiers, and private keys serve to prove ownership of these addresses and their associated funds.

In Bitcoin's P2P transactions, digital signature verification is peer-to-peer, reflecting a decentralized direct trust mechanism. Specifically, during a transaction, the sender uses the private key to generate a digital signature for the transaction information, including the hash value of the sender's address, the receiver's address, the amount, and other relevant details. The signature serves as proof that the sender does have the private key corresponding to the Bitcoin address, thereby verifying its legal ownership of the funds. Bitcoin uses the secp256k1 curve of the elliptic curve digital signature algorithm(ECDSA), which provides security based on a 256-bit key, while combining efficiency and small storage requirements [9].

During verification, the network node decrypts the signature with the sender's public key and compares the hash value of the transaction information to ensure that the transaction is authorized by the legitimate owner of the address and that the transaction data has not been tampered with. The transaction information is then broadcast to the entire network and ultimately verified by miners and recorded in the blockchain.

DOI: 10.54254/2755-2721/117/2025.20951

4. Practical Applications of Digital Signature Algorithms in the Field of E-Commerce

4.1. RSA

The RSA signature algorithm is one of the most mature digital signature algorithms, but RSA-based encryption and authentication mechanisms are usually used when resources constraints are not a critical concern. Since RSA requires a large key length, such as 2048 bits or higher, to meet modern security standards, its computational overhead is large, especially key generation, encryption, and decryption operations, which require strong processing power and storage resources.

4.2. ECC

Compared with the traditional RSA algorithm, ECC significantly shortens the key length while providing the same security level, thereby reducing computing, storage and bandwidth requirements, and is suitable for resource-constrained devices. The National Institute of Standards and Technology (NIST) has detailed the security of ECC and RSA in its "FIPS 186-4: Digital Signature Standard (DSS)". Under the premise of achieving the same security level, the key length of ECC is much shorter than that of RSA, 224-bit ECC ≈ 2048-bit RSA, 256-bit ECC ≈ 3072-bit RSA.

In the fields of mobile payment systems, smart POS terminals, wearable device payments, and cross-border e-commerce payments, due to the small size and limited computing power of hardware devices, the RSA algorithm is difficult to implement efficiently or cannot meet the needs of fast transaction processing. The lightweight ECC algorithm has a wide range of applications in these fields due to its high efficiency and low resource consumption [3].

4.3. Post-Quantum Cryptographic Algorithms

With the development of quantum computing, post-quantum encryption algorithms have emerged. Up to now, in NIST's post-quantum cryptography standardization project, the selected signature algorithms are mainly several lattice-based and hash-based digital signature algorithms.

4.3.1. Lattice-based Digital Signature Algorithms

The core foundation of the lattice-based digital signature algorithm is the mathematical properties of the lattice. The lattice is a discrete additive subgroup generated by linearly independent basis vectors. Its essence is a discrete point set and has the structure of a vector space.

Short Integer Solution (SIS) problem and Learning with Errors (LWE) problem are two constructive problems used in the design of cryptographic systems. SIS is to find a short integer vector that satisfies a specific modular linear equation. LWE is to infer the secret vector through a linear equation perturbed by noise.

These problems have been proven to be highly computationally difficult on both classical and quantum computers, providing a solid theoretical foundation for post-quantum cryptography [4].

4.3.2. Hash-based digital signature algorithms

Hash-based digital signatures utilize the core properties of hash functions, including one-way, collision resistance, and second preimage resistance. Its implementation mechanisms include one-time signature (OTS) and multiple signature (FTS). Classic schemes include Lamport OTS: using a key and public key that are twice the length of the message to implement the most basic one-time signature. Merkle OTS: adding a checksum to Lamport OTS to improve efficiency. Winternitz OTS: reducing the length of keys and signatures by iterating hash functions, but increasing computational overhead[5].

DOI: 10.54254/2755-2721/117/2025.20951

5. Specialized Signature Algorithms and Their Applications in E-Commerce

Group signatures, ring signatures, blind signatures, and proxy signatures have diverse and significant applications in e-commerce scenarios. These signature schemes enable functionalities such as privacy protection, authority delegation, and other effects.

5.1. Blind Signatures

During the signature generation process, the message content is invisible to the signer, thereby safeguarding the privacy of the message provider. The typical application of blind signatures in e-commerce is electronic payment, especially electronic cash (e-cash), which ensures that the identity privacy of the payer is not compromised.

The core characteristics of blind signatures include: Unforgeability, that is, only the legitimate signer can generate a valid signature; Non-repudiation, ensuring that the signer cannot deny the signature he generated; Blindness, that is, the signer cannot know the specific content of the signed message; Traceability, allowing the signature to be associated with the specific owner of the message; and Unlinkability, ensuring that no direct association can be established between the signer and the signed message. These characteristics make blind signatures play an important role in ensuring privacy and preventing identity leakage, especially in electronic payment applications such as e-cash, helping to protect the identity privacy of the payer[6,7].

However, blind signatures also face certain challenges: the signatory is entirely unaware of the signature content, which may lead to illegal use. In electronic cash systems, it may also cause the problem of infinite database growth[7].

During the transaction process, blind signatures help hide transaction data, ensuring privacy, security and anti-tracking.

5.2. Proxy Signatures

Proxy signature is an extended form of digital signature, first proposed by Mambo, Usuda and Okamoto in 1996. Its core idea is to allow the original signer to partially or completely authorize the proxy signer to generate a legally binding signature on behalf of the original signer. Proxy signature has important practical significance, especially in scenarios such as electronic voting and electronic auctions, which can effectively solve the efficiency problem caused by the original signer's inability to sign directly.

The proxy signature protocol must meet the following characteristics: Unforgeability, that is, only authorized proxy signers can generate valid signatures, Verifiability, the verifier can confirm that the signature is authorized by the original signer, Non-repudiation, the proxy signer cannot deny the signature he generated, Distinguishability, the proxy signature can be clearly distinguished from the original signature, Identifiability, the identity of the proxy signer can be determined and Anti-abuse, the proxy key can only be used within a specific authorization scope[11].

According to the authorization method, proxy signature can be categorized into full proxy signature, partial proxy signature and proxy signature based on authorization certificate. Among them, partial proxy signature is considered to be a more secure and practical solution because it can effectively limit the authority of the proxy signer. In recent years, in order to meet the needs of practical applications, the proxy signature scheme has been further developed, and variants such as threshold proxy signature, multi-proxy signature and time-sensitive signature have been derived. For example, threshold proxy signature allows multiple parties to jointly manage proxy keys to enhance security and responsibility allocation capabilities.

Although proxy signature has achieved certain results, it still faces the following challenges and research directions: improving the security of the scheme to resist forgery attacks and public key

DOI: 10.54254/2755-2721/117/2025.20951

replacement attacks; simplifying the algorithm to improve execution efficiency; solving the problem of signature right transfer and revocation; and exploring the integration of blind signature, zero-knowledge proof and other technologies into proxy signature to enhance its function. In addition, with the increasing demand for proxy signature in e-commerce scenarios, how to design an efficient, secure and practical proxy signature scheme has become an important direction for future research.

Due to its flexibility and security, proxy signature has become an important technology in e-commerce scenarios, and it has broad application prospects in authorization management, contract signing, and authority transfer.

6. Future Directions

With the rapid development of e-commerce and technological advancement, the role of digital signatures in ensuring transaction security, data integrity and user trust will be further expanded. The following are possible future development directions of digital signatures in the field of e-commerce:

6.1. Popularization of Digital Signature Algorithms

Globally, electronic payments are rapidly becoming popular, especially in many developing countries. Although mobile payments are developing rapidly, the processor performance of smart devices is still a major obstacle to their popularization. In order to enable mobile payments to be widely used on various devices, especially on devices with limited resources, it is necessary to make lightweight improvements to existing digital signature algorithms.

Optimizing computing efficiency is the key to lightweight improvements. With the popularity of smart homes and wearable devices, lightweight signature algorithms have become important. The improved ECDSA or lattice-based signatures can significantly reduce the consumption of computing resources while maintaining the same level of security.

6.2. Protection of Transaction Privacy

Transaction privacy is a core concern in the field of e-commerce, and digital signature technology will play an important role in privacy protection. In order to ensure the security and privacy of user transactions, the technical solutions mainly include zero-knowledge proof, multi-party privacy protection, distributed storage and dynamic signature mechanism.

The integration of zero-knowledge proof technology enables users to complete transaction verification without exposing sensitive data. For example, in electronic payment scenarios, users only need to prove that the account balance is sufficient without disclosing the specific amount, thereby effectively protecting personal financial privacy.

In multi-party transactions, such as auctions and cross-border payments, ring signatures and group signature technologies become effective solutions. These technologies ensure the legitimacy of transactions while hiding the specific identity information of the transaction parties to avoid privacy leakage.

Combined with blockchain technology, distributed privacy storage can be realized, and transaction data can be distributedly stored on the blockchain. All data is authenticated by signature, which not only ensures the integrity of the data, but also avoids the risk of privacy leakage caused by single-point storage.

After the introduction of dynamic signature and one-time signature mechanism, a unique digital signature will be generated for each transaction. This method effectively prevents transaction information from being reused or tampered with, ensures data security and transaction uniqueness, and further improves the level of privacy protection.

DOI: 10.54254/2755-2721/117/2025.20951

6.3. Quantum digital signature

Yin Hualei and others have proposed the first quantum e-commerce solution and have achieved the first international demonstration of a five-user quantum e-commerce application scenario, including the interaction between merchants, customers and third-party platforms [8]. The quantum e-commerce solution they proposed is a quantum e-commerce protocol based on a one-time global hash quantum digital signature. This solution can meet the requirements of data authenticity, integrity and non-repudiation in an e-commerce environment, while taking into account privacy protection and efficiency.

The future development direction of quantum digital signatures will be to support quantum signature protocols for multiple concurrent users. Realize quantum signature technology at longer distances and higher speeds. Expand the application of quantum digital signatures in blockchain, such as quantum Byzantine consensus protocol. Develop quantum network protocols with more complex functions.

7. Conclusion

This paper systematically sorts out the application and development direction of digital signature technology in the field of e-commerce, analyzes the applicable scenarios and limitations of classic algorithms such as RSA and ECC, and explores the potential applications of cutting-edge technologies such as post-quantum cryptography, privacy protection and lightweight design in this field. Research shows that ECC has become the mainstream choice in mobile payments and resource-constrained devices due to its high efficiency and low resource consumption, while the lattice-based post-quantum signature algorithm provides an important foundation for future anti-quantum attacks.

At the same time, this paper analyzes the application of digital signatures in decentralized and centralized trust models in combination with specific scenarios, such as B2C, B2B and P2P transactions, and proposes optimization strategies and privacy protection solutions for resource-constrained devices. Especially in terms of privacy protection, technologies such as zero-knowledge proof, ring signature and blind signature show broad application prospects.

Looking to the future, digital signature technology will make further breakthroughs in lightweight design, anti-quantum security and edge computing support. However, how to improve algorithm efficiency while ensuring high security and balance privacy protection and data availability will become the core topic of continuous exploration in this field. This study provides theoretical support for the application of digital signature technology in e-commerce, and the paper looks forward to more innovative solutions in the future to promote its practice and development in smart devices and blockchain.

References

[1] *Li, M., Ma, L., Wang, J., et al. (2024). Research on identity authentication technology based on blockchain and PKI. Information Security Research, 10(2), 148–155.*

[2] *Yu, S., Lan, Z., & Sun, Y. (2003). Secure e-commerce constructed by PKI. Microcomputer Development, 12, 65–67, 121.*

[3] *Shaikh, J. R., Nenova, M., Iliev, G., & Valkova-Jarvis, Z. (2017). Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained e-commerce applications. In 2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) (pp. 1–4). Tel-Aviv, Israel. https://doi.org/10.1109/COMCAS.2017.8244805*

[4] *Liu, F., Zheng, Z., Gong, Z., et al. (2024). A survey on lattice-based digital signature. Cybersecurity, 7(7). https://doi.org/10.1186/s42400-023-00198-1*

[5] *Li, L., Lu, X., & Wang, K. (2022). Hash-based signature revisited. Cybersecurity, 5(13). https://doi.org/10.1186/s42400-022-00117-w*

[6] Luo, Y. P., Tsai, S. L., Hwang, T., et al. (2017). On "A new quantum blind signature with unlinkability". Quantum Information Processing, 16(87). https://doi.org/10.1007/s11128-017-1536-8

[7] Li, M., Wang, T., & Luo, X. (2011). Cryptographic analysis of two partially blind signature schemes based on bilinear pairings. Application Research of Computers, 28(2), 435–438.

[8] Yin, H., Cao, X., Li, B., et al. (2024). Quantum e-commerce: The practical path of quantum digital signature. Physics, 53(2), 110–113.

[9] Martínez, V. G., Hernández-Álvarez, L., & Encinas, L. H. (2020). Analysis of the cryptographic tools for blockchain and Bitcoin. Mathematics, 8, 131. https://doi.org/10.3390/math8010131

[10] Fang, W., Chen, W., & Zhang, W. (2020). Digital signature scheme for information non-repudiation in blockchain: A state of the art review. Journal of Wireless Communications and Networking, 2020(56). https://doi.org/10.1186/s13638-020-01665-w

[11] Li, J., Cao, Z., Li, J., et al. (2003). The status and progress of proxy signatures. Journal of Communications, 10, 114–124.