Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1221162, 6 pages
https://doi.org/10.1155/2022/1221162

Research Article

Auxiliary System for Contract Signing Based on Electronic Signature Technology

Yu Jia[1,2,3] **and Zhen Li**[4]

[1]*Fujian Police College, Fuzhou, Fujian 350000, China*
[2]*The Key Laboratory of Document Examination of the Ministry of Public Security, Shenyang, Liaoning 110000, China*
[3]*Shenzhou Judicial Appraisal Center, Nanchang, Jiangxi 330000, China*
[4]*Department of Documents Examination, Criminal Investigation Police University of China, Shenyang, Liaoning 110000, China*

Correspondence should be addressed to Zhen Li; lizhen_wjjyjsx@cipuc.edu.cn

Received 14 June 2022; Revised 20 July 2022; Accepted 27 July 2022; Published 22 September 2022

Academic Editor: Kuruva Lakshmanna

With the rapid development of the Internet, a large part of people's work and life has been transferred to the computer. Now, the processes of file transfer and data storage in people's work are all completed by computers. In the process of working with computers, how to ensure the legality, traceability, antitampering, and uniqueness of documents is an important part of the development of computers. In order to ensure the security in the process of electronic contract authentication, this study has carried out a detailed analysis and design of electronic signature technology. In this study, PKI technology and USB Key technology are combined, which effectively prevents the tampering of electronic signatures and electronic seals in electronic contracts. This study uses PKI technology to strengthen the application and distribution of electronic seals and achieve the purpose of copyright protection of digital media. The improved electronic signature technology in this study can improve the security of signing electronic contracts at work and make users' electronic signatures indestructible and noncopyable.

1. Introduction

The scope of electronic signatures is very wide. Any electronic technical means that can prove the identity of the parties in electronic communication and prove the recognition of the content of the documents by the parties can be called electronic signatures. In the traditional transaction process, in order to ensure that contract documents are stolen, a seal or a handwritten signature is generally used to prove identity [1]. In the Internet age, today's documents are transmitted through the network, and the type of documents has changed from paper to electronic format. Under such an era background, the traditional manual stamping and signature can no longer adapt to the modern transaction mode [2]. In order to improve the security of electronic documents, electronic signature technology has been developed in today's Internet, and there are relevant laws to protect electronic signatures. Electronic signatures are clearly regulated in China's "Electronic Signature Law" issued in 2005. Among them, reliable electronic signatures, handwritten signatures, and seals are given the same legal effect as traditional manual seals and signatures. Electronic signatures can clearly indicate the true identities of both parties in electronic documents, ensuring the security and authenticity of the document transmission process and nonrepudiation. Many technologies are involved in electronic signature today, including combined public key technology, time stamp technology, digital watermark technology, and PKI technology. Many experts and scholars have studied how to improve the security and confidentiality of electronic signatures. Literature [3] proposes to use the combined public key technology to improve and perfect the electronic signature. Reference [4] proposes to use timestamp technology to make electronic signatures time-sensitive. Literature [5] and Literature [6] propose that the combination of digital watermarking technology and PKI technology can make the issuance and recycling of electronic signatures a complete process. This study investigated and discussed many other studies and finally decided to combine and improve the excellent parts of these literature studies to form a complete electronic signature system. According to the requirements and connotation of PKI technology, this system

builds a complete public key infrastructure device including certification authority, digital certificate library, key backup, recovery system, certificate invalidation system, and application interface, which can provide users with complete and confidential data serve. At the same time, this system integrates digital watermarking technology into electronic signature technology, which can provide users with secure and nonreproducible digital signatures, so that users' electronic signatures can be more secure. After using the digital watermarking technology, in order to double guarantee the user's digital signature, this study also applies the USB Key technology to the system. After the system detects the insertion of the USB Key, the PIN code will be verified. Here, under the premise, the user can enter the system [7]. Under the protection of these technologies, this system can provide users with a comprehensive and confidential electronic signature system, which makes the contracts, certificates, and policy issuance of enterprises and government departments more secure.

2. Explanation of Relevant Theoretical Knowledge

2.1. PKI Technology. PKI technology generally refers to public key infrastructure. A public key infrastructure includes hardware, software, people, policies, and procedures. A public key infrastructure can implement keys based on public key cryptography and generate, manage, store, distribute, and revoke key certificates. The PKI system combines computer software technology, computer hardware technology, authoritative institutions, and application systems, which can make the automated office procedures performed on computers for e-government and e-commerce more complete [8]. PKI technology enables users who do not know each other or who are far away to communicate securely through a chain of trust.

As shown in Figure 1, a standard PKI system includes PKI policy, software and hardware system, certificate authority CA, registration authority RA, certificate issuing system, and PKI application.

PKI security policy is the key to defining a cryptosystem. A PKI security policy is responsible for establishing and defining guidelines for an organization's information security, organizing the way a system handles keys and valuable information, and determining the level of security controls in a system.

The certificate authority CA is the foundation of trust in the PKI system. The certificate authority CA can issue certificates and stipulate the validity period of the certificate and revoke the certificate when necessary.

The registry RA can provide users with an interface with the CA. After the registration authority RA obtains and authenticates the identity of the user, it will make a certificate request to the CA. In the PKI international standard recommendation, an independent RA is required to complete the task of registration management, which can improve the security of the application system [9].

The certificate issuing system issues certificates through users or directory servers.

The application of PKI is very extensive. In the process of people using the Internet, PKI technology can be used in a large number of places, such as communication between

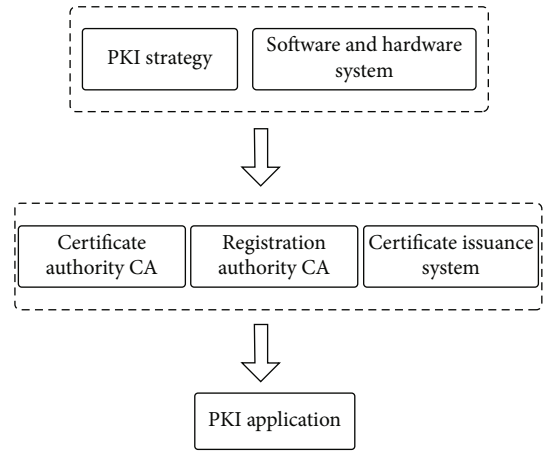

Figure 1: PKI system structure.

web servers and browsers, electronic data exchange, e-mail, credit card transactions on the Internet, and virtual private network.

2.2. USB Key Technology. USB Key is a hardware device with USB interface. The USB Key has a single-chip microcomputer or a smart card chip and has a certain storage space, which can store the user's private key, digital certificate, and other security certificates. Since the USB Key has a public key algorithm inside, it can realize the authentication of the user's identity, and this technology is relatively safe [10].

USB Key is the solution adopted by most Chinese banks to protect user information security. The bank will use the USB Key to store the digital certificate representing the user's unique identity and the user's private key. The user's private key is generated in the high-security USB Key and cannot be exported to the outside of the USB Key, which is why the USB Key is highly secure [11].

2.3. Electronic Signature Technology. An electronic signature is an electronic code that can identify a user. Electronic signatures correspond to real signatures or seals and can determine the identity of the sender and the authenticity of the original text. The electronic signature adopts a certain data exchange protocol and uses a cryptographic algorithm to encrypt the data that has not been sent to generate a piece of information, which is attached to the original text and sent together. The original text can be corporate documents, contracts, notices, etc. [12]. Electronic signatures protect against counterfeiting when transferring files on a computer. Figure 2 shows the implementation of digital signature.

3. Electronic Signature System Framework

The electronic signature system constructed in this research mainly has two parts: server side and client side. The server-side software system is an electronic signature center, which can apply for, make, distribute, and destroy electronic signatures [13]. Client software can place electronic signatures on files and can also verify electronic signatures on files. The specific frame structure of the system is shown in Figure 3.

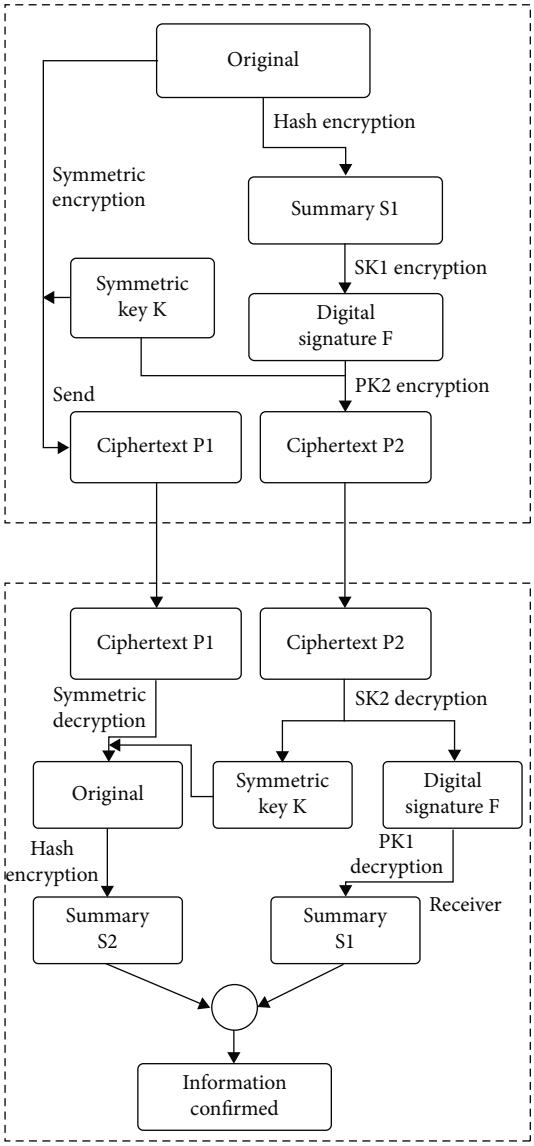

Figure 2: Implementation of digital signature.

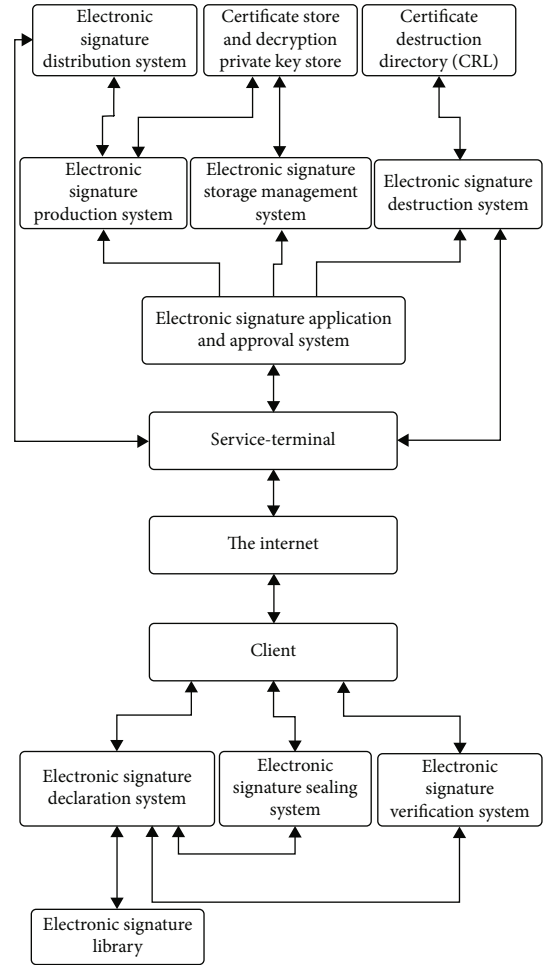

Figure 3: Framework of the electronic signature system.

The electronic signature application and approval system can review and destroy the applications of legitimate users. After the review results are successfully destroyed, a receipt will be sent to the user.

The electronic signature production subsystem can make the user's electronic signature into a pdf file, edit the signature image according to the user's requirements, add the anticounterfeiting information of the digital watermark to the electronic signature, and generate a high-quality signature key pair. This module is responsible for accepting the confirmation information from the electronic signature distribution system and adding the generated signature public key certificate and encryption public key certificate to the certificate library [14]. Figure 4 shows the steps to verify the validity of the public key.

The electronic signature storage management system is responsible for efficient management of the certificate library and decryption private key library. The decryption private key store is only open to server-side administrative users. The certificate store stores the legal user's electronic signature certificate and encryption public key certificate. The encryption public key certificate is open to online users, while the electronic signature certificate is not open to online users. The electronic signature storage management system can provide users with the functions of retrieving and querying the certificate library and decrypting the private key library and can verify the application of the legitimate user, recover the decrypted private key, and send it to the legitimate user [15].

The electronic signature distribution system is responsible for the filing management of electronic signatures. This system is related to the security policy of the electronic signature system and has a great impact on the security of electronic signatures.

The electronic signature destruction system is used to destroy electronic signatures. After accepting the user's application, the system will verify the user's electronic seal destruction application, after confirming the application, destroy the corresponding certificate, and record the destruction name in the CRL. In this system, users are also provided with the functions of querying, browsing, and downloading CRLs. Figure 5 shows the verification process of signature in the electronic signature system [16].

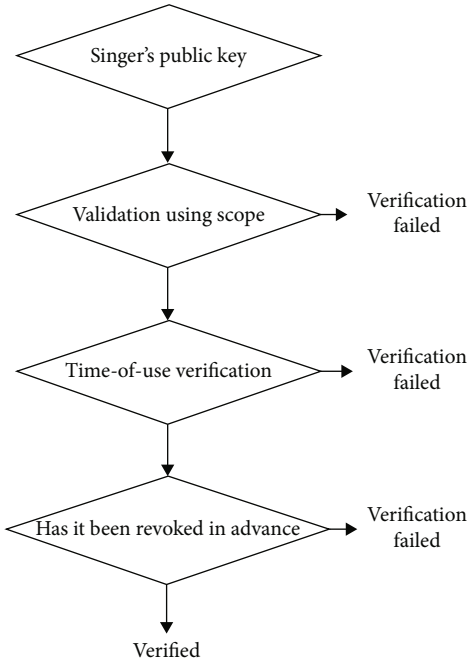

Figure 4: Steps to verify the validity of the public key.

4. Design of Watermark Embedding Algorithm

In order to ensure that the user's electronic signature cannot be copied, the system will embed a digital watermark in the electronic signature. Digital watermarks are invisible and very fragile, which leads to the fact that if someone tries to destroy the information on the digital watermark, the electronic signature will also be destroyed [17].

To ensure the security of electronic signatures, the wavelet decomposition signal is used in the digital watermark embedding method proposed in this study. The system converts the digital watermark information into a binary bit sequence for rearrangement [18]. After rearrangement, the image is subjected to wavelet transform to obtain the multilayer wavelet transform decomposition coefficients. There are certain regular eigenvalues in the high-frequency components of the multilayer wavelet transform decomposition coefficients, and the system will find these eigenvalues and arrange these eigenvalues. The arrangement order is performed by the arrangement rule of the watermark bit sequence. In this way, the digital watermark information can be hidden in the arrangement order of the feature values [19].

The steps of the watermark embedding algorithm are as follows:

(1) Using wavelet transform, the electronic signature image is subjected to wavelet transform of 2-layer scale

First, a given square-integrable two-dimensional discrete signal is assumed and set as $A_0(m, n)$. Using the pyramid algorithm of the two-dimensional image, the image can be decomposed into the low-frequency image $A_{j+1}(m, n)$ with the scale of $j + 1$ and the high-frequency image $H_{j+1}(m, n)$, $V_{j+1}(m + n)$, and $D_{j+1}(m, n)$. The specific formula is as follows:

$$\begin{aligned} A_{j+1}(m,n) &= \sum_{k\in Z}\sum_{l\in Z} h(k-2m)h(l-2n)A_j(k,l), \\ V_{j+1}(m,n) &= \sum_{k\in Z}\sum_{l\in Z} h(k-2m)g(l-2n)A_j(k,l), \\ H_{j+1}(m,n) &= \sum_{k\in Z}\sum_{l\in Z} h(k-2m)g(l-2n)A_j(k,l), \\ D^3_{j+1}(m,n) &\sum_{k\in Z}\sum_{l\in Z} h(k-2m)g(l-2n)A_j(k,l). \end{aligned} \tag{1}$$

In the formula, h is the low-pass filter obtained by the wavelet multiresolution analysis, and g is the high-pass filter obtained by the wavelet multiresolution analysis. The first line of the formula can keep the low frequency components of the original image. The second line of the formula can maintain the horizontal edge details of the original image. The third line of the formula can maintain the oblique edge details of the original image [20].

(2) Find the local maxima in the decomposition coefficients

The wavelet coefficients can be obtained in the previous step. The horizontal edge details of the original image can be displayed in the H component coefficients. The V-component system can show the vertical edge details of the original image. Calculating the two component coefficients gives the magnitude and argument of the vector. The formula for calculation is as follows:

$$\begin{cases} \mathrm{ABS}(m,n) = \sqrt{|H_2(m,n)|^2 + |V_2(m,n)|^2}, \\ \mathrm{Arc}(m,n) = \mathrm{arctg}\left[\dfrac{V_2(m,n)}{H_2(m,n)}\right]. \end{cases} \tag{2}$$

Arc is the argument matrix, which represents the direction of the vector and the horizontal direction, and represents the normal direction of the edge of the image. Perpendicular to the Arc angle is the image gradient direction. A local maximum point is a point with a local inflection point along the gradient direction. An example of a local extra-large value is shown in Figure 6.

The value of Arc (m, n) is defined as between [-π/2,π/2], to perform a merge transformation on the angle values of elements in Arc.

According to formula 2, the modulus image ABS and the corresponding direction image ABS and the corresponding direction image Arc on the scale of 2 layers are obtained. According to the angle merge transformation of Arc elements, a new angle matrix can be obtained. If one point in the ABS is larger than the two adjacent points in its eight fields, then this point is a candidate local maxima. Among the candidate local maxima, if a point is larger than the two adjacent points in the angular direction and exceeds the threshold t_2, then this point is the local maximum point.

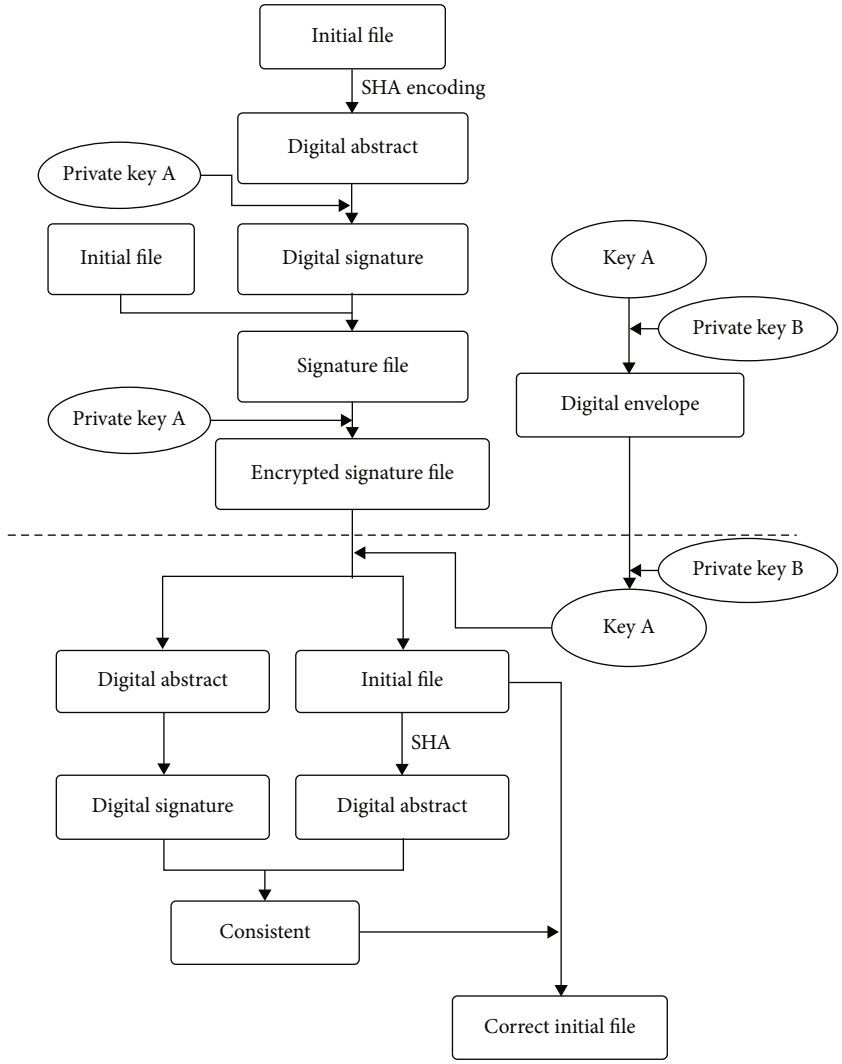

Figure 5: Verification process of signature in the electronic signature system.

$$\begin{bmatrix} 0 & 0 & 0 & 171.25 \\ 0 & 160.61 & 233.73 & 0 \\ 263.71 & 31.466 & 0 & 0 \\ 0 & 0 & 0 & 114.9 \end{bmatrix}$$

(a) Modulus matrix

$$\begin{bmatrix} 0 & 0 & 0 & 135 \\ 0 & 135 & 135 & 0 \\ 0 & 135 & 0 & 0 \\ 0 & 0 & 0 & 135 \end{bmatrix}$$

(b) Argument matrix matrix

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

(c) Maximum point decision matrix

Figure 6: Example of a local maximum point.

After the wavelet coefficients are inversely transformed, the electronic signature embedded with the digital watermark can be obtained.

5. Conclusion

This study constructs an electronic signature system, in which a series of services related to electronic signatures are provided to users, including the application, approval, and destruction of electronic signatures. In this system, embedding digital watermark into electronic signature is the key technology. In this paper, the digital watermark embedding technology is analyzed in detail, and a digital watermark embedding method based on wavelet decomposition signal is proposed. Compared with the traditional electronic signature scheme, this method is more secure and more concealed, which can ensure the uniqueness and security of the electronic signature. The overall layout of the system is still in its infancy in this research. Next, this research will improve the various functions of the system, improve the stability and efficiency of the system, and make the system more user-friendly. The improvement of this system will have a positive impact on the development of electronic signature technology. With the continuous improvement of communication efficiency, the confidentiality and security of such electronic signature technology will also be improved. In the foreseeable future, the era of people using computer technology for full-scale office has come.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no competing interest.

References

[1] H. Wang, L. Chengzhe, L. Xiangyang, and Z. Han, "Batch verification of digital signatures based on orthogonal Latin square theory," *Journal of Communications*, vol. 43, no. 2, pp. 44–54, 2022.

[2] D. Laila and C. Panos, "Legitimating digital technologies in industry exchange fields: the case of digital signatures," *Information and Organization*, vol. 32, no. 1, p. 100392, 2022.

[3] C. Xiao-Qiu, T.-Y. Wang, W. Chun-Yan, and F. Gao, "Cryptanalysis of quantum digital signature for the access control of sensitive data," *Physica A: Statistical Mechanics and its Applications*, vol. 593, p. 126949, 2022.

[4] M. H. Mohamed, Computer Department, MTC, Cairo, Egypt, W. I. El Sobky, S. Hamdy, Math Department, Benha University, Benha, Egypt, and Electric Department, Benha University, Benha, Egypt, "Elliptic curve digital signature algorithm challenges and development stages," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 10, no. 10, pp. 121–128, 2021.

[5] X. Yang, "Overview of digital signature technology," *Computer Programming Skills and Maintenance*, vol. 11, 2021.

[6] C. Man, *Research on NTRU-based digital signature scheme*, Shandong University, 2021.

[7] M. R. Alagheband and M. Atefeh, "Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous IoT: taxonomy, capabilities, and objectives," *Internet of Things*, vol. 18, p. 100492, 2022.

[8] Z. Zhu and T. Fei, "Comparison and intelligent analysis of NTRU and ETRU signature algorithms for public key digital signature," *Journal of Physics: Conference Series*, vol. 2083, no. 4, p. 042009, 2021.

[9] C. Osman and Y. Ihsan, "Ring-based quantum network with quantum key distribution (QKD) and quantum digital signature (QDS)," *IOP Conference Series: Materials Science and Engineering*, vol. 1187, no. 1, p. 012020, 2021.

[10] W. C. Xun, L. YuShuo, G. R. Qi et al., "Secure and practical multiparty quantum digital signatures," *Optics express*, vol. 29, no. 17, 2021.

[11] R. C. Ribeiro, M. G. de Almeida, and E. D. Canedo, "A digital signature model using XAdES standard as a rest service," *Information*, vol. 12, no. 8, p. 289, 2021.

[12] O. Ruan, C. Jichen, and H. Mao, "An efficient SM2 digital signature batch verification algorithm," *Computer Engineering and Science*, vol. 43, no. 7, pp. 1236–1242, 2021.

[13] B. N. Mojtaba, A. Reza, and M. K. Mehran, "Cryptographic accelerators for digital signature based on Ed25519," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 7, pp. 1297–1305, 2021.

[14] Z. Wei, S. Ronghua, S. Jinjing, R. Xinchao, Y. Guo, and H. Duan, "Quantum digital signature based on measurement-device-independent continuous-variable scheme," *Quantum Information Processing*, vol. 20, no. 7, 2021.

[15] D. M. Kuryazov, "Development of electronic digital signature algorithms with compound modules and their cryptanalysis," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 4, pp. 1085–1099, 2021.

[16] X. Wenfang, Z. Shuwen, Z. Xian, C. Changping, and X. Shengming, "Current situation research and hotspot analysis of digital signature based on bibliometrics," *Science and Technology Information*, vol. 19, no. 12, pp. 48–50, 2021.

[17] M. Bo, X. Wang, X. Zheng, and L. Qin, "A secure two-way heterogeneous digital signature scheme between PKI and IBC," *Journal of South-Central University for Nationalities (Natural Science Edition)*, vol. 40, no. 2, pp. 184–192, 2021.

[18] K. B. Prabhu and G. Sannasi, "A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves," *INTERNATIONAL ARAB JOURNAL OF INFORMATION TECHNOLOGY*, vol. 18, no. 2, 2021.

[19] C. K. Won, K. Y. Seok, and C. Jeongil, "A study of factors affecting intention to adopt a cloud-based digital signature service," *Information*, vol. 12, no. 2, p. 60, 2021.

[20] Q. Wang, "Overview of coding-based digital signature technology," *Digital Technology and Application*, vol. 38, no. 9, pp. 186–189, 2020.