Journal of Sociology and Ethnology (2021)
Clausius Scientific Press, Canada

DOI: 10.23977/jsoce.2021.030718
ISSN 2616-2318 Vol. 3 Num. 7

Application of Mathematical Signature Technology in Computer Information Security Design

Yongqiang Shang

Xinyang Agriculture and Forestry University, Department of Information Engineering Information Engineering Department, Xinyang, Hennan, 464000, China

Keywords: Computer network, Security protection, Digital signature technology

Abstract: Digital signature technology is an effective means to ensure the confidentiality, integrity and security of information transmission, and it plays an important role in computer security protection. Based on this, this paper analyzes the application of digital signature technology in computer security protection in detail.

1. Introduction

At present, the network environment management process has become increasingly standardized. In the process of the development of electronic computer technology, the security protection of computer has become one of the problems that the network technology industry needs to face. Because of its own characteristics, computer technology has been more widely used in many industries, such as military, office and so on. Once there are security protection problems in it, then Then it will inevitably cause economic losses and security loopholes. In the current situation, in the work of computer security protection, the biggest application is digital signature technology. The computer uses cryptographic algorithm to encrypt the data to be transmitted, automatically generate information, send this detection information together with the original, so that the receiver can verify the authenticity of the information, Detection information can be understood as signature, which is a way to judge the original text, to ensure the safety of computer use, and to prevent the spread of bad information.

2. The Principle of Digital Signature Technology

Digital signature technology is an important technology for computer security protection. It can provide security for information verification and effectively prevent the spread of bad information such as viruses. In the application process, digital signature technology has the characteristics of integrity and privacy, which can further provide security for information transmission. In today's modern network, digital signature technology has become computer security The most core technology in the whole protection work. 1. The significance of digital signature technology. Digital signature is a very complex system, mainly through data encryption and transformation as the main way, and then with specific protocol as the standard, to generate a digital signature that can reflect the characteristics of the signer. The main content of digital signature technology is to sign documents and signers. The basis of implementing digital signature technology is cryptography,

which encrypts the core and realizes the encryption of various transmission information. 2. Application principle of digital signature technology. In application principle, digital signature technology is a breakthrough of traditional computer security protection technology. It uses digital conversion and encryption technology to realize automatic inspection in the process of information transmission and acceptance. The application principle of digital signature technology is that through the digital conversion of information, the information corresponds to the original information. After receiving the information, the information needs to be converted to get the original text. Therefore, only the digital conversion method needs to be innovated, so the security of information transmission will be improved, and it is difficult to be cracked[1].

3. The Function of Digital Signature Technology

In order to ensure the security of network information, we need to take corresponding security measures to provide users with more secure services. Digital signature mechanism is a main means to ensure the security of network information, which can effectively solve the problem of forgery. The main goal of digital signature is to play the same role as signature in network technology. 1. Anti counterfeiting: first of all, digital signature technology can effectively prevent the phenomenon of forgery of information signature. Because the private key is only known by the signer himself, no one else can produce effective signature results except the signer himself, so it is necessary to keep his own private key. 2. Identification. In the traditional mode, the signature is always met directly by both parties, so the identity of both parties can be confirmed directly. In the network environment, the receiver can directly identify the identity of the sender. 3. Prevent replay. In daily work, both parties need to tear up the contract after completing the contract to prevent repudiation by using the contract again. Therefore, in digital signature, we need to apply time stamp and other technologies to prevent reuse. 4. Non repudiation: because the digital signature technology can identify the identity of the other party, there is no chance of forgery, so only the message needs to be properly saved, and then the evidence can be left, so that the signer cannot repudiate the contract content. 5. Confidentiality: due to the low confidentiality of the traditional signature technology, once the document is lost, it will cause the document information to be leaked[2].

4. Digital Certificate and Pki

At present, the most commonly used signature method for electronic documents is the digital signature method based on public key infrastructure (PKI) technology. PKI is an online security mechanism consisting of private key and public key. By encrypting, decrypting and not using the same key, PKI can guarantee the security of network information transmission process to the greatest extent. In the online security mechanism, the public key is public, and the private key is kept by the user alone. No matter the public key or the private key, as long as one of the keys encrypts the data, even if the information is stolen in the transmission process, the thief cannot easily decrypt the data. The other of the two keys can be used for decryption to obtain the original data content. In the process of computer network information transaction, public key infrastructure is regarded as the most secure means of protection, which is mainly based on the public key cryptography technology. In addition to the important public-private key technology, the core of PKI lies in certificate authority (CA). CA must be a third party, such as government, bank, general legal person, etc. the public key is authenticated by Ca center, and the private key can be obtained by one party of the transaction who requests from the other party, while the two parties of the transaction cannot share CA center. In the network transaction environment, in addition to Ca center authentication, it is also necessary to establish a trust mechanism similar to signature or seal, and the electronic authentication mechanism constructed by digital signature technology can effectively

provide network related seal functions, thus meeting the different security needs of network transactions[3].

5. Application of Digital Signature Technology in Computer Protection

5.1 Application of Digital Signature Technology to the Problem of Factorization of Large Prime Number

With the continuous development of Internet technology, in order to better ensure the network information security of the people, China has also made great efforts in the research of computer security protection. Through continuous research and exploration, a new type of digital signature technology has been widely used. Digital signature technology has a very significant effect in ensuring the security of computer information. There are many kinds of digital signature schemes in the problem of factorization of large prime number. For example, RSA signature scheme and rbani signature scheme are two commonly used schemes. The protection effect of applying them in computer security protection is very good[4].

5.2 Application of Digital Signature Technology to Discrete Logarithm Problem

The digital signature scheme of discrete logarithm problem is also a very widely used digital signature technique. Compared with the digital signature scheme of big prime factorization problem, it has great difference, but it is very ideal in the computer security protection effect. In terms of computing data and exponential operation, there is a certain gap between the two signature schemes. In terms of computing data, the digital signature technology of the discrete logarithm problem is more complicated, while the digital signature technology of the large prime factorization problem is simpler, but in terms of exponential operation, the digital signature technology of the discrete logarithm problem is more simplified, while the large prime problem is more simple The digital signature technology is more complicated. It is because the exponential operation of digital signature technology, which is a discrete logarithm problem, is relatively simple, so the design scheme that can solve the problem in the process of processing is more clear, clear and detailed[5].

5.3 Application of Flow Information Oriented Digital Signature Scheme

Flow information oriented digital signature is a new type of digital signature scheme, which can better guarantee the computer security, and it is also an important security processing technology in digital signature technology. The flow information oriented digital signature is different from the traditional signature scheme. The flow information may be an infinite sequence, and the receiver needs to receive the information in time, which also ensures the security of network communication to a large extent. Stream information mainly includes data stream, digital audio, digital video, etc. Generally, the flow information oriented digital signature can be divided into two situations. The first is to prove the security of the signature scheme, the sender does not know how long the information is, and the second is that the sender has known the length of the information in advance. The efficient signature strategy can be designed by this constraint condition[6].

5.4 Verifiable Secure Digital Signature Scheme

Efficient and verifiable secure digital signature scheme is also an important technical content to ensure the security of computer information. The application of this scheme can prevent variable attack based on guess RSA algorithm to the greatest extent, and further improve the role of

computer security protection. Efficient verifiable secure digital signature scheme mainly uses the paradigm of mark and hash to establish security. If the verifiable secure digital signature scheme is assumed to be an important guarantee of uniqueness in digital signature technology, its security can be reflected in three aspects. First of all, a prediction model is constructed. The model is not constructed by certain planning, but by random. On the basis of random establishment, the reliability of the model should be strictly guaranteed. Secondly, a hash function is used to replace the random prediction model, in which the hash function can meet the specific calculation characteristics. Finally, through research and analysis to prove that hash function can exist, at the same time to demonstrate the rationality of the hypothesis. Through these three steps, we can prove the efficient and verifiable secure digital signature scheme[7-8].

6. Conclusion

In the current situation, digital signature technology is more suitable for many fields such as government affairs, finance and trade in the work of computer security protection. This technology is more common in dealing with business and communication business. However, in the process of application, there are still some problems such as invalid special authentication and low popularity. In the process of application of digital signature technology, comprehensive improvement and improvement are needed to improve the application.

References

[1] Xu Danhui. Design and analysis of designated verifier signature scheme [D]. Tianjin: Tianjin University of technology, 2015.

[2] Du Chengbin. Design and analysis of quantum proxy multiple blind signature protocol [D]. Anhui: Anhui University, 2017.

[3] Yao Hongdi. Research on quantum multi proxy signature protocol [D]. Anhui: Anhui University, 2017.

[4] Li shangze. Improvement and application of scalar multiplication algorithm of elliptic curve [D]. Beijing: Beijing University of chemical technology, 2017.

[5] Liu le. Two types of signature scheme design and related issues research [D]. Shaanxi: Xi'an University of Electronic Science and technology, 2017.

[6] Zhang Jun. a quantum proxy signature scheme based on EPR entangled state [J]. Telecommunication science, 2012,28 (11): 92-97.

[7] Li Fei, Gao Wei, Wang Guilin, et al. General construction of compact security signature based on the hash function of strong chameleon [J]. Computer research and development, 2017,54 (10): 2244-2254.

[8] Zhou Xufeng. The impact of quantum informatics on information security [J]. Value engineering, 2015, 34 (33): 192-195.