Advances in Artificial Intelligence, Big Data and Algorithms
G. Grigoras and P. Lorenz (Eds.)

doi:10.3233/FAIA230906

Research on the Application of Domestic Autonomous Cryptography Algorithms in the Field of Ecological Environment Information Security

Ying YU [a], Kangping ZHAO [a], Zhiyang YU [b] and Zhiyu LANG [c,1]
[a] *Sichuan Academy of Environmental Policy and Planning, Chengdu, Sichuan, China*
[b] *Henan Agricultural University, Zhengzhou, Henan, China*
[c] *CETC Cyberspace Security Technology Co.,Ltd., Chengdu, Sichuan, China*

Abstract. Passwords are not simply the crystallization of scientific and technological progress, but also a sharp tool for maintaining network security and order, and an indispensable strategic resource for safeguarding national security. Ecological and environmental informatization is not only an important component of national cyberculture and informatization construction, but also the core content and support guarantee of ecological and environmental protection work, which is related to the practical performance ability of ecological and environmental departments at all levels. The rapid development of ecological environment informatization construction not only brings efficient and fast office experience, but also enhances the security risks of network information. The ecological environment protection work involves a variety of types and a large amount of multi-source heterogeneous data, and there are many practical operations such as data collection, data analysis, data storage, and data application. The frequent occurrence of high-risk risks in information security, including data theft and vulnerability attacks, has led to numerous security risks in the construction of ecological environment informatization, seriously affecting the security, scientifically, and standardization of ecological environment protection work, and even threatening national security. This article focuses on the network information security issues exposed in the process of ecological environment informatization construction, focusing on the security issues faced by data storage and transmission, and conducting research on the application of domestically produced autonomous password algorithms in the field of ecological environment information security. On the basis of continuously improving the standardized storage of data, this article effectively ensures the security of various types of data during transmission. It has played a positive role in promoting the improvement of information security in the field of ecological environment.

Keywords. information security, ecological environment, Domestic password algorithm, information construction

[1] Corresponding Author: Zhiyu LANG, CETC Cyberspace Security Technology Co.,Ltd.; e-mail: zhiyu126@163.com

1. Introduction

Information security, as an important component of the national security strategy system, is an effective response strategy to the diverse network information security needs of government, finance, universities, enterprises, and other sectors, which involves multi-party collaboration and joint supervision. In today's rapidly changing information technology, the construction and development of diversified network informatization are rapidly improving, while network information security is also constantly facing challenges [1]. Unlike in the past, the negative impact of the internet as a double-edged sword is more complex and diverse, and the construction of cyberculture space provides a solid guarantee for the integration of space and space in China. Comprehensively promoting the development and application of big data and accelerating the construction of a data powerhouse has become China's national strategy. The Party Central Committee and the State Council attach great importance to the position and role of big data in promoting ecological civilization construction. By utilizing digital and intelligent methods such as mathematical models, computer technology, and geographic information systems to conduct research on environmental planning and policy simulation, it will help achieve refined management of the ecological environment and comprehensive decision-making of the environmental economy [2]. The data types and sources involved include not only the image data of water environment, climate change, soil environment, ecological protection and other elements, but also the attribute data of the policy database and indicator database related to environmental policy and planning, as well as the structured data stored in various systems and databases. Various sources and types of environmental data have a corresponding value, and using such data can mine valuable information through processing and analysis. However, there are also huge risks hidden behind the value, such as sensitive data trafficking, theft, and unauthorized abuse. The continued existence of these problems will seriously affect the security, scientifically, and standardization of ecological environment protection planning, and even threaten national security [3].

2. Research Status of State Security Algorithm in the Field of Ecological Environment Information Security

2.1. Basic Overview of Domestic Autonomous Cryptography Algorithms

With the promulgation and implementation of the Password Law of the People's Republic of China, passwords have risen from basic systems and basic national policies to national laws, and password applications have changed into standardized applications according to law [4]. In order to ensure the security of information transmission process in communication and the Storage security of sensitive information at various terminals, it is urgent to encrypt and protect communication information and stored sensitive data. The basic cryptographic algorithms mainly include symmetric cryptographic algorithms, public key cryptographic algorithms, cryptographic hash algorithms, and message authentication algorithms. Next, this article will take SM2, which belongs to the public key cryptographic algorithm, and SM4, which belongs to the symmetric cryptographic algorithm, as examples to provide a brief overview of these two domestically produced autonomous cryptographic algorithms.

The National Cryptographic Administration released the Elliptic Curve Public Key Cryptography Algorithm SM2 on December 17, 2010. Based on its higher cryptographic complexity, faster processing speed, and smaller machine performance consumption, it has been used to replace the 1024 bit RSA algorithm that is currently facing serious security threats, and has officially become an international standard. SM4 is a block cipher standard issued by the State Password Administration on March 21, 2012. The SM4 block cipher algorithm has a plaintext packet length of 128 bits and a key length of 128 bits. The plaintext encryption will generate ciphertext through 32 rounds of iterative encryption operations. The encryption operation is carried out in words (32-bit), and each iteration operation is a round of transformation function F. The structure of the SM4 algorithm for encryption and decryption is the same, with only the round key used being the opposite, where the decryption round key is the reverse order of the encryption round key.

With the development of cryptography and computing technology, many cryptographic algorithms, including RSA, proposed and developed by Western countries for encryption standards and usage specifications, have been announced to have been breached. In the process of ecological environment informatization construction, combined with the actual work of ecological environment protection, domestic autonomous password algorithms will be applied to the ecological environment field to meet the application needs of information security in this field [5-10].

2.2. The Research Objectives of this Article

To effectively enhance the scientifically, standardization, and operability of ecological environment informatization construction, and assist in achieving defined management of ecological environment and comprehensive decision-making of the environmental economy. This article will conduct research on two aspects of data center security strategies for ecological and environmental informatization construction: firstly, conduct research on the current status of national security algorithms in the field of ecological and environmental information security. Summarize current mainstream domestic autonomous password algorithms, and conduct analysis work based on current policies and situations, from predictable security risks to actual need, to prepare for the next step of application research and design work. The second is the application research of national secret algorithm in the field of ecological environment information security. This article focuses on the research of information security issues in the process of ecological environment informatization construction, starting from the actual needs of the application of national secret algorithm in the field of ecological environment information security, and considering the application and design of national secret algorithm for ecological environment information security.

3. Research on the Application of National Security Algorithm in the Field of Ecological Environment Information Security

3.1. Risk Analyses of Information Security in the Field of Ecological Environment

The information security risks in the field of ecological environment mainly focus on various terminal devices, service platforms, and entrusted communication channels.

From the perspective of information security elements, the main security risks can be divided into the following three aspects:

- Confidentiality. The ecological environment information involves the visualization, stigmatization and structured data of landform, sewage outlet, water source, soil, climate, species, etc. These data are sensitive and have security risks in storage, transmission, access, backup, fault tolerance and other operations.
- Integrity. In the process of ecological environment informatization construction, various systematic and plagiarized office and monitoring government platforms have been integrated. This type of platform poses security risks in the integrity verification of functional operations such as identity management, permission management, key management, and authorization management.
- Availability. In most cases where private networks are used for construction, ecological environment informatization still faces security risks in the underlying operating environment and local area network available.

3.2. Analysis of the Demand for National Secret Algorithm in the Field of Ecological Environment

Compliance requirements. Since the official implementation of the "Password Law of the People's Republic of China" on January 1, 2020, localized password transformation for the government system has been put on the agenda. Taking the construction of ecological and environmental informatization as an example, currently most government office systems and platforms use international cryptographic algorithms, which cannot meet compliance requirements in terms of security. Therefore, it is urgent to replace the basic algorithms with higher security national cryptographic algorithms to ensure the network security, application security, and data security of the platform, and thus meet the national standard specifications of the "Technical Specification for Environmental Information System Security".

Application requirements. The application of national security algorithms in the field of ecological environment is mainly reflected in three aspects: cryptographic algorithms, protocols, and key management, which must strictly comply with relevant norms and standards. According to the requirements of standards such as "Basic Requirements for Information System Password Application" and "Security Technical Requirements for Password Modules", define the password application strategy and password modules for standardized data centers, using the SM2/SM3/SM4 password algorithm recognized by the national password regulatory agency.

Ease of use requirements. In order to reduce the difficulty and complexity of the security application ecosystem information security center, the information security service center should unify standards, specifications, and formats, shield the heterogeneity of the underlying password service infrastructure, adopt a unified and standardized interface encapsulation, and provide unified password services and interfaces for security applications. In the scenario of ubiquitous terminal and diversified server deployment, through the overall design of password service models, we aim to create an access as a service ubiquitous password basic service platform for the ecological environment information security service center, meeting the password usage needs of ubiquitous ecological environment business applications. It has good flexibility, versatility, and convenience, which can minimize the complexity and difficulty of integrating security applications and shorten the integration time to the greatest extent.

3.3. Analysis of Ecological Environment Information Security Application Technology

Cryptography, as the most reliable key technology for ensuring information security, can play a decisive role in implementing the construction of ecological environment informatization and promoting the steady development of ecological environment information security. Next, this article will analyze password based technologies that can be applied to the field of ecological environment information security.

Digital signature. This technology has the characteristics of anti-counterfeiting, tampering resistance, and non repudiation when applied to the field of ecological environment information security. The result obtained by the signer using a private key to perform cryptographic operations on the hash value of the signed data can only be verified using the signer's public key, which is used to confirm the integrity of the signed data, the authenticity of the signer's identity, and the non repudiation of the signature behavior.

Digital envelope. This technology is applied in the field of ecological and environmental information security, with designated special recipients to ensure confidentiality during the information transmission process. As a data structure, the technology includes ciphertext encrypted with symmetric-key algorithm and the symmetric key encrypted with the public key. Composed of encrypted data and a ciphertext containing at least one recipient's data encryption key. Among them, encrypted data is encrypted using a data encryption key, which is encrypted using the recipient's public key.

Password protocol. The application of this technology in the field of ecological environment information security can achieve secure interaction activities between devices, managers, and users. A series of steps taken by two or more participants to achieve a specific purpose using a cryptographic algorithm according to agreed rules.

The application of national encryption algorithms in the field of ecological environment not only plays a positive role in various businesses, processes, and data management in the process of information security construction, but also depicts the understanding of the value of encryption technology through this profound application process, thereby further strengthening the sense of responsibility to protect national information security.

3.4. Application Design of National Security Algorithm for Ecological Environment Information Security

In order to effectively meet the urgent demand for information security in the field of ecological environment, effectively expand the practice of domestically produced autonomous password algorithms in the field of ecological environment information security, further enhance the scientific, normative, and operational nature of protection work, and assist in achieving refined management of ecological environment and comprehensive decision-making of environmental economy. While deploying the ecological environment information security service system, Provide password computing capability for multi-source heterogeneous data interaction.

In the overall architecture of the national security algorithm application design in the ecological and ecological environment information security field mentioned above. The password service layer plays the role of underlying basic support. Next, we will review the key technical routes involved in the ecological and ecological environment

information security service center proposed in this article from two aspects: key management and practical application of passwords.

Firstly, key management. The full lifecycle management of keys in the Ecological Environment Information Security Service Center includes the entire process of key generation, key distribution, key storage, key update, key backup, key recovery, and key destruction.

Secondly, password application. This aspect will be sorted out from five aspects: identity authentication, digital signature and verification, data encryption and decryption, important data integrity protection, and nonrepudiation of entity behavior.

Identity authentication: identity authentication in the process of secure communication between the terminal and the service background is carried out through the message authentication code mechanism, and its working principle is shown in the Figure 1.

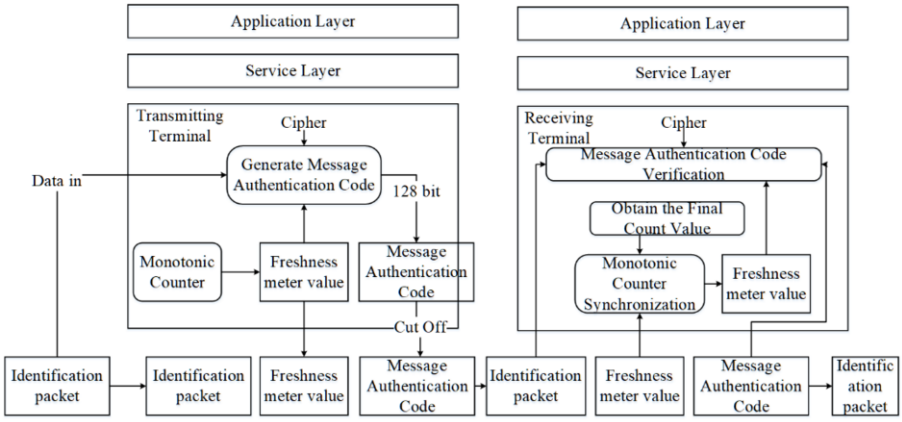

Figure 1. Design of National Security Algorithm Application in the Field of Ecological Environment Information Security, Security Identification and Freshness Verification.

Digital signature verification: Digital signature verification mainly includes signature verification of information and signature verification during secure startup process. To support integrity detection of transmitted data, cryptographic calculations are used to hash the transmitted data, generate message summaries and their digital signatures. The security module located on the opposite end implements integrity detection of the received data based on signature verification mechanism. An encrypted channel is established between the server and the security module through HTTPS to ensure the secure transmission of data.

Data encryption and decryption: Data encryption and decryption mainly include data encryption and decryption during the communication process. To ensure the confidentiality of sensitive/private data, the data security module provides data security encryption and decryption services based on a secure key storage mechanism.

Important data integrity: Important data integrity mainly includes integrity verification of communication data to prevent tampering with relevant data or systems. To ensure the integrity of data, the system provides data integrity protection and detection services. The system provides a data integrity protection API, with input being application data and output being application data abstract ciphertext. Once the integrity of the application data is compromised, the application can detect it by calling the data integrity detection API.

Nonrepudiation of entity behavior: The implementation methods mainly include. Firstly, identity authentication during secure communication. The second is digital signature and signature verification. Thirdly, by encrypting, storing, exporting, and encrypting the content of security audit information, real-time monitoring of device network intrusion and violations is carried out, providing evidence collection means.

4. CONCLUSION

The ecological environment information security service center applying domestically produced autonomous cryptographic algorithms is a systematic and long-term work that involves a large amount of data, rich data types, and a wide range of segmented fields. Therefore, while effectively promoting the construction of ecological environment informatization, it should focus on the research of national cryptographic algorithms in the field of ecological environment information security and the construction of related systems. On the basis of referring to relevant national norms and standards such as environmental information systems and information system password applications, combined with the current situation of ecological environment information security, this article studies the actual need of ecological environment information security. On the basis of continuously improving standardized data storage, it provides security guarantees for various types of environmental data during transmission and storage. The next step will focus on the landing and implementation of an ecological environment information security service center that applies domestically produced autonomous password algorithms, enabling it to effectively ensure the construction of ecological environment information security.

References

[1] Xi Jinping. Speech at the Special Seminar on Learning and Implementing the Spirit of the Fifth Plenary Session of the 18th Central Committee of the Communist Party of China by Major Leading Cadres at the Provincial and Ministerial Levels [J]. China Emergency Management, 2016 (5): 11-19.
[2] Environmental Protection Law of the People's Republic of China [J]. Environmental Protection Work Data Selection, 2014 (4): 7.
[3] Notice of the State Council on Issuing the Action Outline for Promoting the Development of Big Data [J]. State Council Communique of the People's Republic of China, 2019 (6).
[4] Notice on Issuing the Overall Plan for the Construction of Ecological Environment Big Data[J]. Environmental Protection Work Data Selection, 2016,0 (3): 21-25.
[5] Wang Binyong. Research on the Network Security Technology System of Ecological Environment Big Data Platform [J]. Network Security Technology and Applications, 2021 (12): 128-129.
[6] B Ravi Prasad, Hussain Mohammed Ashfaq, K Sridharan, CosioBorda Ricardo Fernando, C Geetha. Support vector machine and neural network for enhanced classification algorithm in ecological data[J]. Measurement: Sensors. Volume 27 , Issue . 2023.
[7] Shi Kaixin. The Impact of Ecological Environment on the Development of Digital Economy [J]. Environmental Engineering, 2021 (12).
[8] Miao Gangsong, Wang Wei. Construction and Thinking of Environmental Protection Big Data Platform [J]. Technological Innovation and Application, 2020 (20).
[9] Hafiz Muhammad Waseem, Hwang Seong Oun. A probabilistic model of quantum states for classical data security [J]. Frontiers of Physics. Volume 18 , Issue 5 . 2023.
[10] Cryptography Law of the People's Republic of China [J]. Communique of the Standing Committee of the National People's Congress of the People's Republic of China, 2019 (6).