Journal of Computers Vol. 32 No. 2, 2021, pp. 213-221
doi:10.3966/199115992021043202018

Design and Realization of Cooperative Processing System for Cross-regional Judicial Business

Kun Mi[1*], Yajing Wang[1], Zhenjiang Zhang[2], Yang Zhang[3]

[1] Beijing Thunisoft Information Technology Corporation Limited, Beijing 100084, China
mikun@thunisoft.com; wangyajing@thunisoft.com

[2] School of Software Engineering, Beijing Jiaotong University, Beijing 100044, China
zhangzhenjiang@bjtu.edu.cn

[3] Key Laboratory of Communication and Information Systems, Beijing Municipal Commission of Education, School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
zhang.yang@bjtu.edu.cn

Received 2 January 2021; Revised 2 February 2021; Accepted 31 March 2021

Abstract. In the present age, courts at all levels are actively using modern computer and network technology, Transfer its management and service functions to the network to complete, and realize the informatization of the court's internal government affairs. The establishment of a cross-regional judicial business collaborative processing system is of great significance to promote the coordination of courts at all levels, improve work efficiency, and improve social satisfaction. At the same time, due to the strictness and seriousness of the court's judicial business, the entire process can be made more secure through SM9 encryption. Aiming at the actual needs in the informatization of government affairs, this paper designs a cross-regional collaborative processing system based on the analysis of the advantages and technical trends of similar systems at home and abroad. Discussed the system's work flow, safe realization of data sharing and exchange and related functions, and discussed the two key issues of using SM9 to realize data encryption and decryption and the realization of safe data sharing and exchange. The realization of "overall planning and resource sharing" has greatly improved the office efficiency of courts at all levels.

Keywords: judicial business, collaborative processing system, SM9, data sharing

1 Introduction

With the rise of the information revolution and the rapid development of network technology, a rapid wave of informatization is setting off around the world, presenting a brand-new look with informatization as the fundamental feature. In the construction of the national informatization system, government informatization has become the key to the entire informatization, and initial results have also been shown in improving the quality and efficiency of judicial business processing at all levels of courts, as well as scientific decision-making and macro-control capabilities. In recent years, both the Central Government and the Ministry of Justice have put forward clear requirements and guidance on the construction of informatization. In order to further strengthen and standardize the informatization construction of the judicial administration system and ensure the healthy and orderly development of judicial administration informatization, the Ministry of Justice has successively studied and formulated 19 informatization standards including "National Technical Standards for Management Information System of Judicial Offices". The promulgation of these standards puts forward clear standards and system construction requirements for the realization of the interconnection, business collaboration, and resource sharing of judicial administrative information systems. Among them, the coordinated processing of government

[*] Corresponding Author

affairs is an important part of information construction. The purpose of the construction of a cross-regional judicial business collaborative processing system is to carry out the transmission and processing of cross-regional judicial business between different court departments in accordance with unified norms and standards, and to ensure the safety, timeliness and efficiency in the process of delivery and processing. At the same time, with the continuous maturity and development of information technology, the informatization of judicial administrative management should also build a new system to meet the new business development requirements and technological progress. In 1982, the General Office of the State Council put forward the goal and specific implementation plan of building an office decision-making service system for national executive heads, and promoted office automation in the national government system. On the basis of information construction, after more than ten years of development, electronic official documents in our country have undergone several changes in their technical and application forms, and accumulated rich practical experience. After 2001, the legal status of electronic official documents was established, marking that my country's electronic official documents entered a relatively mature and stable development period.

In the wave of global informatization, governments of various countries have clarified their strategic goals and intensified the construction of government informatization. Taking the European Union as an example, it has also formulated an information society action plan. Its member states have also formulated their own information society action plans and government informatization plans, and actively put them into action. The development of government informatization has also made great progress. At the same time, we have also seen different levels of government informatization development.

Looking at the development of government informatization in developed countries, we can see that the development of government informatization should be closely integrated with government reform. In the construction of government informatization, the national government needs to formulate unified planning and technical standards to regulate the development of government informatization, pay attention to practical application, and put the service of enterprises and the public and the realization of resource sharing in an important position. In terms of specific implementation, developed countries generally implement a phased implementation strategy, from simple to complex, from easy to difficult. In the construction of government informatization, the processing of government documents has also been continuously established in the construction of informatization, and its real-time, high efficiency, and security have been guaranteed. However, the research on government information construction involves many theoretical and technical aspects such as system architecture, application standards, process design, and information security. The e-government collaborative office system of various government departments is a huge and complex system. The official documents and their processing involved are intricate. At the same time, the existing collaborative system can only support the collaboration within the province, and with the development of the times and the increase in data to be processed, the previous systems have gradually failed to keep up with the pace of the times.

The so-called cross-regional judicial business collaborative processing system refers to the use of modern computer and network technology by courts at all levels to transfer their business transmission, management and processing functions to the network to complete, and at the same time realize the reorganization and optimization of organizational structure and work flow, beyond time and space Restrictions on separation from departments, to achieve "overall planning and resource sharing", to promote the transformation of government work methods and the improvement of efficiency. Its core content is to construct a virtual court system at all levels, to realize the informatization of internal court activities, fundamentally change the behavior of traditional courts, and make management and service business computerized, networked, and informatized, which greatly improves Administrative Efficiency. Courts in different provinces can apply for coordinated case handling, breaking provincial restrictions, and truly realizing the automatic recommendation of coordinated cases in national collaborative case handling. For some common collaboration situations, identification conditions can be set, and then the cross-regional system can automatically recommend law enforcement officers, which cases need to be coordinated, form a collaborative team online, clear division of labor, smooth information sharing, and leave traces throughout the process, enabling richer collaboration The method supports remote online collaboration, multiple courts participate in offline execution online, and the process is open and collaborative.

This paper designs and implements a cross-regional judicial business collaborative processing system, meets the new information construction industry standards promulgated by the Ministry of Justice, and meets the needs of the latest development of judicial business, making this system a truly valuable tool for judicial office business work.

2 Related Work

In order to further strengthen and standardize the informatization construction of the judicial administration system and ensure the healthy and orderly development of judicial administration informatization, Domestic scholars Ma Xiaotian [1] proposed an overall design idea for the operation platform of the basic-level judicial administration management. It can realize the supervision and management of the entire city's judicial office information management business work, complete the basic information of judicial office organization, staff information, judicial office business housing information, judicial office transportation information, staff transfer and other information integration, Achieve full coverage of judicial offices, real-time display of important data and pending work.

Kong Waiping et al [2]. established a collaborative processing system for graduates leaving school. It is of great significance to promote departmental coordination, improve work efficiency, and improve student satisfaction. This article analyzes the management process of graduates leaving school, discusses the system's work process, data integration and functional modules. Discusses two key issues in the realization of database access and data synchronization. Based on the relevant technologies of the above literature, this article designs and implements the cross-regional judicial system in view of the characteristics of the cross-region.

3 System Architecture and Functions

As shown in Fig. 1, the system is mainly divided into six functional modules, the first three are basic functions, and the last three are service functions. The basic functions can be divided into three parts, which are also the three life cycles of collaborative cases.

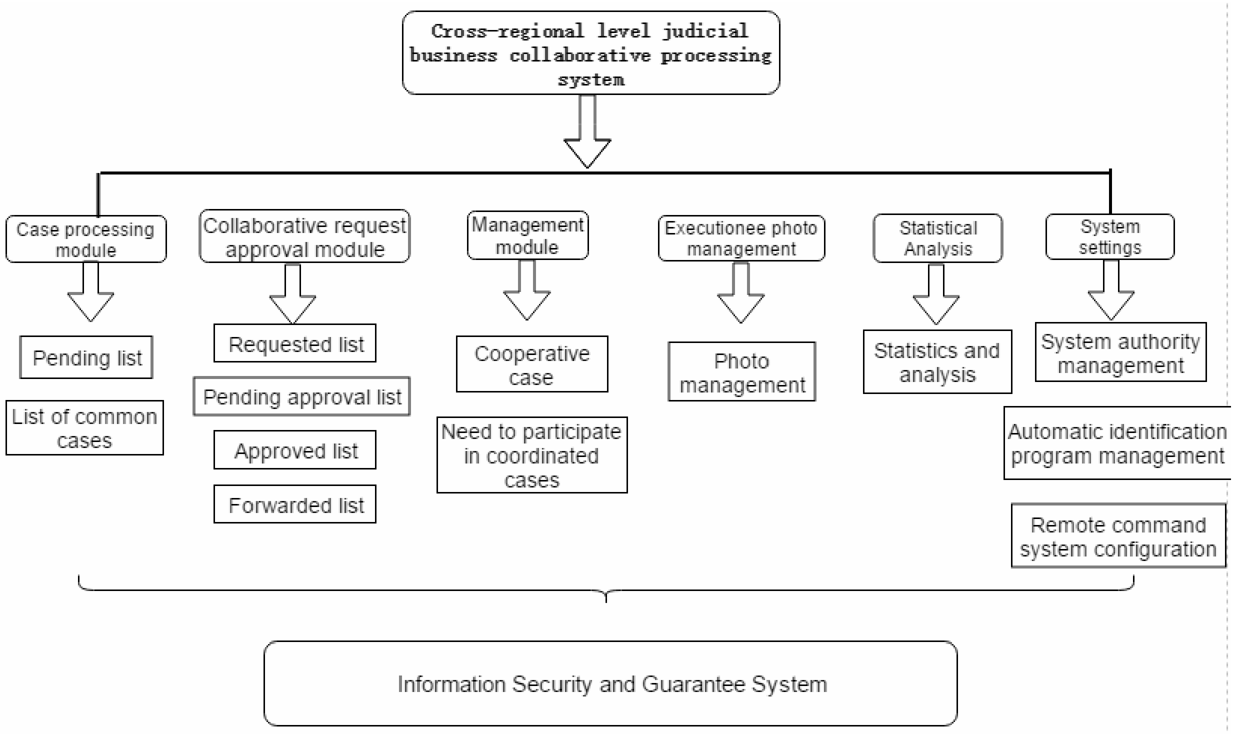
Cross-regional level judicial business collaborative processing system
Case processing module
Collaborative request approval module
Management module
Executionee photo management
Statistical Analysis
System settings
Pending list
List of common cases
Requested list
Pending approval list
Approved list
Forwarded list
Cooperative case
Need to participate in coordinated cases
Photo management
Statistics and analysis
System authority management
Automatic identification program management
Remote command system configuration
Information Security and Guarantee System

Fig. 1. System structure

3.1 Case Processing Module

In this module, it is judged whether the case needs coordination, that is, the management of the case is executed, which is divided into a list to be confirmed and a list of ordinary cases. Fill in the corresponding form in the list to be confirmed to apply for a collaborative case. You need to select the collaborative type of the case, the reason for the collaborative application, detailed information, and the applicant's contact information. You can also upload attachments. You can also choose to apply for a court for coordinated enforcement.

A major feature of this system is that the system can automatically identify cases with collaborative situations. After the automatic identification is turned on, the system will regularly push the identification results to the list to be confirmed, and then the application officer will determine whether to apply for collaboration [3]. You can view the details one by one. You can also confirm in batches or choose not to need collaboration temporarily. After the selection, the judge is required to fill in the corresponding reasons to prevent accidents and complete the identification of the case. At the same time, it also supports inter-provincial coordination. At the same time, the leader also has the duty of supervision. If it is found that there is a coordination situation in the case, it can send a suggestion to the accepting officer, and the accepting officer will decide whether to coordinate.

In the list of common cases, the system will automatically identify cases that do not require coordination and store them in this list [4]. If the judge finds that coordination is needed during the handling of the case, he can also apply for coordination, and the leader can also send some suggestions to the judge.

3.2 Collaborative Request Approval Module

In the processing of applications in this module, cooperative cases generally involve at least two or more court systems, which is a relatively complicated model. The courts and scope involved are also broader than ordinary enforcement cases, so The approval process is also more stringent. The system adopts a level-by-level approval method. Depending on the type of collaboration selected during the application, the final approval court is also different. If the authority is insufficient, the application can also be forwarded to the corresponding court.

This module is responsible for approving collaborative applications. The higher court decides whether this case really requires collaboration, that is, collaborative application management. You can view the cases that have been applied for, pending approval, forwarded, and approved [5]. They have different functions. Application list: You can view the detailed information of the applied collaborative case. Pending approval list: You can view the detailed information of the collaborative cases waiting for approval. Taking into account the complexity of the case, you can also modify some case information here to improve administrative efficiency. Or choose to forward the application to the corresponding court, where the application is confirmed and approved, and finally the execution decision is uploaded. Forwarded list: View the detailed information of the cases forwarded to the corresponding court. Approved list: After the operation is successful, you can view the detailed information of the confirmed collaborative case here.

3.3 Management Module

In order to facilitate the overall management, the system will generate a collaborative case studio in this module, which is divided into the collaborative case of the court and the case that requires the participation of the court, and then the courts jointly complete the established collaborative content, that is, studio management [6-7]. Click to enter the studio, you will enter the function page and process tracking.

In the cooperative case inter module of this court, the cases applied by the court itself will appear here. You can enter the studio here to make overall planning of the case, conduct team management, consultation management, remote command, and data management.

Team management can modify the permissions of team members, assign tasks, and track and record the work process, making work more convenient and faster. Conference management can conduct various online conferences to ensure smooth information exchange. Remote command is also a feature of this system. If the needs of multiple courts need to be executed by one court, and the situation on the scene is complex and changeable, you can fill in relevant information on the system, select a specific time, and use the local camera. Online command can reflect the advantages of remote collaboration to a greater extent. Data management can record the detailed information of the entire case process and control the progress stage of the collaborative case.

In the module of cases requiring participation of this court, this court will not take the lead, but the cases involved will be summarized here.

3.4 Accessibility

In order to facilitate system maintenance and management, this system also has some service functions for assistance, which can be roughly divided into three parts. The first is the photo management of the person to be executed, which is entered in the remote command. The face recognition photos of passersby and other portrait information will be recorded and organized here, and relevant personnel information can be consulted at any time, and the untrustworthy status can be changed. Perform data recording and analysis to facilitate future reference.

The last is the system settings. In the system management, some administrator operations can be performed, such as collecting court information at all levels, personnel information, and related personnel authority. In the automatic identification program management, you can set whether to enable automatic identification of collaborative cases and the setting of detailed rules, which can be automatically pushed after opening. In the remote command system configuration, carry out the related settings of remote command.

4 Related Technology Research

4.1 Data Sharing and Secure Transmission

The current electronic system construction of the judicial system has made certain achievements, but there are still certain problems: first, there is a lack of top-level design, an incomplete data sharing mechanism, and a lack of a complete government information resource catalog system and data sharing and exchange technical specifications [8]. The second is that the data sharing model is simple in design. Departments are often oriented toward their own business needs. The data sharing system is built to facilitate the department’s access to data, and it lacks overall consideration. The third is the poor quality of data submitted by the grassroots and high work pressure. Many business systems of higher-level departments need to submit data from the grassroots, which often results in similar data. Different staff at the grass-roots level report to different departments at different time periods. The quality of reported data is difficult to guarantee. In order to better solve the existing problems, in accordance with the principle of “sharing as the principle, non-sharing as the exception; demand-oriented, unified standards, overall construction; establishment of mechanisms to ensure safety” judicial information resource sharing principles, to build a vertical link to all levels of courts, Horizontally connect the judicial unified data sharing system of various departments to provide convenient data sharing services for government departments at all levels. The judicial business data sharing system mainly does a good job in the overall architecture design of the data sharing system, the hierarchical data sharing system design, the data sharing security management design, etc. [9], the compilation of the judicial business information resource catalog system and the data sharing and exchange standard specifications, and the formulation of related regulations and laws, Provisions, etc., to ensure that information resources are used in compliance with laws and regulations.

4.1.1 Data Sharing Overall Architecture

The data sharing system is mainly divided into four levels. The county-level data sharing system is responsible for the collection of original data and is the basis for the construction of other levels. It has the characteristics of wide distribution, low application difficulty, and easy promotion. Establish a county-level data sharing system first through a bottom-up approach, and then advance the construction level by level. The data sharing system at each level only connects with the adjacent upper and lower systems to ensure the integrity and uniqueness of data sharing. The data is first extracted by the underlying data sharing system, and then sent to the higher-level information sharing system after processing the information. The overall architecture of the data sharing system is shown in Fig. 2.

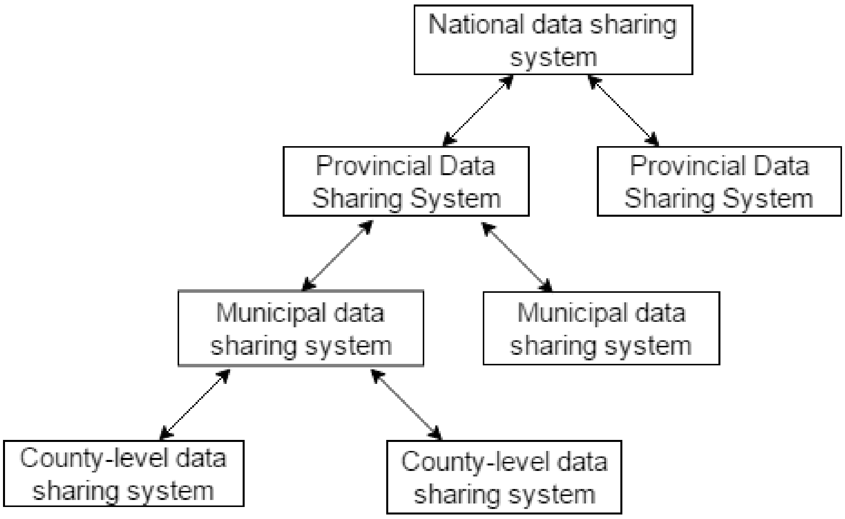
National data sharing system
Provincial Data Sharing System
Provincial Data Sharing System
Municipal data sharing system
Municipal data sharing system
County-level data sharing system
County-level data sharing system

Fig. 2. Data sharing system

4.1.2 Hierarchical Data Sharing System Architecture

The hierarchical data sharing system is a data sharing system built by courts at all levels. Constructing a hierarchical data sharing system can realize interconnection and data sharing between courts at the same level, and at the same time realize the docking with the data sharing system at the upper and lower levels, and open up data sharing channels between the courts at the upper and lower levels. Taking county-level courts as an example, the county-level data sharing system covers all departments of county courts, villages and related units. The data generated by the business systems of the various departments of the county-level courts forms the county-level government information resource database, which provides data sharing services for the business systems of the local and subordinate departments. The data sharing system guarantees the validity, completeness and timeliness of the submitted data. At the same time, it can also reduce the pressure of data reporting. The hierarchical data sharing model is shown in Fig. 3.

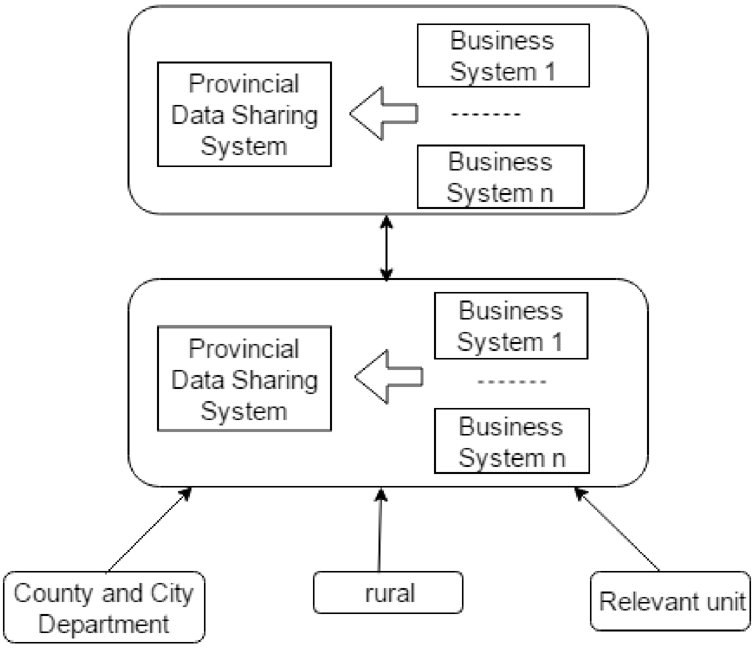

Fig. 3. Hierarchical data sharing model

4.2 Data Sharing Security

In order to ensure the safe transmission of case information in courts at all levels, the construction of the system must consider both the safety of the data transmission process and the safety of data storage. If the data is true and reliable and cannot be arbitrarily tampered with, do a good job in data encryption and decryption, storage and backup management, Data use authority, and user identity authentication management measures. The SM9 identification cryptographic algorithm is the first identification-based cryptographic algorithm standard issued by the State Secret Bureau of my country in 2016 [10]. The standard specifies the specific implementation algorithms for digital signatures, secret key exchange, and public key encryption and decryption. The SM9 identification cryptographic algorithm has the advantages of both ECC and IBC. Its biggest advantage is that it is convenient for key management. Users in the system do not need to apply for digital certificates, nor do they need to query and verify certificates online, which greatly simplifies the links of secure communication. It is especially suitable for realizing identity authentication and data encryption in a mass user environment. In this paper, the encryption and decryption of data is carried out based on the domestic password SM9, which has a significant impact on improving the security of the shared system.

4.2.1 Digital Visa and Verification

In the data sharing system, we need to verify the identity and integrity of the received information. In the digital signature process, the sending court uses the private key to sign the information, while the receiving court uses the corresponding public key to verify the signature. For traditional public key cryptosystems, the signer first calculates its corresponding public key through its own private key, and then applies for a certificate from the CA [11]. The certificate contains the user's identity information, public key, and CA's signature, and then the certificate is issued to the verifier through a public channel. The verifier can determine the source of the public key by verifying the CA's signature, and use the public key to verify the signature. The SM9 identification cryptographic system calculates the public key through user identification, avoiding the complicated certificate exchange process and greatly improving the efficiency of information transmission. The use of bilinear mapping to achieve the integration of the identity makes the signature algorithm more efficient and safe.

4.2.2 Data Encryption

Data encryption is an important method to ensure the safe transmission of arrays, and to ensure the safe transmission of information on open channels. Fig. 4 shows the working principle of the SM9 public key encryption algorithm.

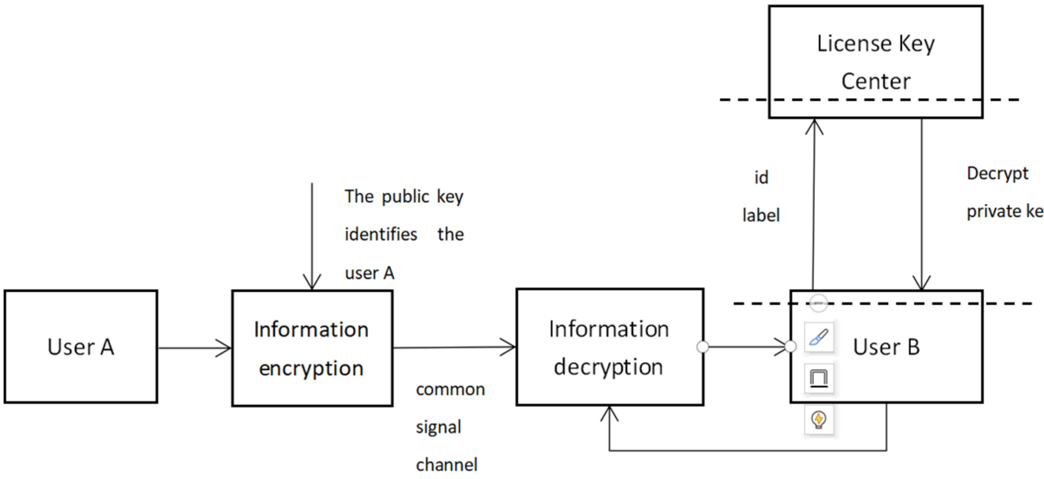

Fig. 4. The working principle of SM9 public key encryption algorithm

User A needs to send encrypted information to User B. Firstly, User A encrypts the information by using the calculated identity of User B as the public key, and then sends the ciphertext information to

User B through the open channel. After receiving the ciphertext information, User B decrypts it by using the decryption private key. The private key of User B is distributed by the key generation center [12]. When the system is initialized, the key generation center authenticates the identity of User B, then calculates the decryption private key with its identity and system parameters, and sends it to User B through the secure channel for storage. Encryption and Decryption Algorithm of Elliptic Curve Cryptography This encryption method will be less secure, but the speed will be greatly improved. In the SM9 identification password algorithm, the data encryption algorithm adopts the hybrid encryption method. In other words, the key used for data encryption is encoded on a point of the elliptic curve, and then the symmetric encryption key is calculated by the key derived function KDF, and then the key is used to encrypt the data. The specific encryption steps are as follows:

(1) Calculate element $Q_B = [H_1(ID_B \| hid, N)]P_1 + P_{pub-e}$ of group G_1;

(2) Generates a random number $\gamma \in [1, N-1]$;

(3) Calculate the element $C_1 = [\gamma]Q_B$ in group G_1 and convert the data type of G_1 to a bit string;

(4) Calculate the element $g = e(P_{pus-e}, P_2)$ of group G_τ;

(5) Calculate the element $w = g^r$ of group G_τ, convert the data type of w to a bit string;

(6) Calculate $klen = mlen + K_2\_len$, then calculate $K = KDF(C_1 \| w \| ID_B, klen)$, let K_1 be the leftmost mlen bit of k, if K_1 is a string of zero bits, then return A_2;

(7) Calculate $C_2 = K_1 \oplus M$ and $C_3 = MAC(K_2, C_2)$, output ciphertext $C = C_1 \| C_3 \| C_2$.

When User B receives the ciphertext message, it needs to decrypt the ciphertext and take out the plaintext information. The above steps show the flow of the public key decryption algorithm. Where mlen is the bit length of C_2 in ciphertext $C = C_1 \| C_3 \| C_2$, K_2_ len is the bit length of key K_2 in function MAC (K_2, Z), User B uses the decryption private key to decrypt the ciphertext.

In the data sharing system, all courts at all levels use SM9 for encryption and decryption and unified key management when transmitting data. In the system, users do not need to apply for digital certificates, nor do they need to query and verify certificates online. They can all be assigned permissions in the studio, which greatly simplifies the link of secure communication.

5 Conclusion and Outlook

Government agencies use modern computer and network technology to transfer their management and service functions to the network to complete. At the same time, it realizes the reorganization and optimization of the government's organizational structure and work flow, transcends the constraints of time, space and departmental separation, and provides efficient, high-quality, standardized, transparent and all-round services to the whole society. The core content is to construct a virtual state government and its departmental institutional system to realize the informatization of government activities within the government.

According to actual needs, this paper designs a cross-regional collaborative processing system based on the analysis of the advantages and trends of similar systems at home and abroad. Discussed the system's work flow, safe realization of data sharing and exchange and related functions. The SM9 encryption process makes the whole process more secure. Gradually realize the office automation, modernization of management, and scientific decision-making of the district agencies, and promote the transformation of government work methods and the improvement of efficiency.

In terms of the current development trend of electronic official documents in my country, years of practice show that the characteristics of the development of electronic official documents in my country can be summarized in the following three aspects: First, technology maturity often lags behind application needs. Second, the system often lags behind practical needs. Third, the operational skills of personnel often lag behind technological development. Combining the three characteristics and the development trend of international e-government, we can make the following prospects for the future: The electronic official document processing process is developing towards standardization, the connotation extension of electronic official document is developing towards expansion, the diversified mode is developing towards unity, and the technical standard of electronic official document is developing towards internationalization.

Acknowledgements

This work was supported by the National Key Research and Development Program of China (grant number 2018YFC0831304).

References

[1] X. Ma, Research on the correlation between smart courts and judicial reform [dissertation], Liaoning Normal University, 2020.

[2] W. Kong, Using the data center to realize the wisdom of college graduates leaving school, Fujian Computer 36(12)(2020) 130-132.

[3] F. Zhang, X. Li, L. Yu, Hongyang Zhang, Kedi Tang, Research and Application of Domestic Cipher, Telecommunications Engineering Technology and Standardization 33(12)(2020) 19-24.

[4] Z. Qu, W. Yi, X. Fang, On the cross-administrative area law enforcement and administrative law enforcement license law enforcement area limitation, Legal System Expo 30(2020) 34-36.

[5] Beijing Municipal Bureau of Justice, Emphasizing business leadership, the construction of "digital rule of law and smart justice" has reached a new level, China Justice 8(2020) 48-49.

[6] Q. Song, H. Guo, Service-oriented data sharing and exchange model, Electronic Design Engineering 29(02)(2021) 174-178.

[7] H. Lu, P. Zhou, The application of big data in the unified business application system under the background of judicial system reform, Legal System Expo 4(2018) 23-25.

[8] X. Shao, Y. Dong, M. Liu, F. Tu, Design of collaborative integrated information system, Computer Engineering and Applications 6(2003) 216-218.

[9] Y. Zhou, Research on the Big Data Cooperative Processing System of the Internet of Things in Shipping, Ship Science and Technology 39(02)(2017) 135-137.

[10] J. Cai, Design of collaborative management system for subway electromechanical installation and construction, Engineering Technology Research 5(13)(2020) 230-231.

[11] S. Zhong, Research on Information System Architecture Transformation of Provincial Data Center of the People's Bank of China, FinTech Times 2(2021) 70-72.

[12] Z. Xie, K. Dong, J. Zhen, Introduction to domestic commercial cryptographic algorithms and related standards, China Quality and Standards Guide 6(2020) 12-14+23.