The Design System of XBRL Software Tax Registration and Data Transmission Encryption

Yisong Peng

School of Accounting, Hunan University of Finance and Economy
Changsha,Hunan,China

***Abstract* - The security of Extensible Business Reporting Language (XBRL) instance is not high because of its extension and openness. As the XBRL software tax statements often involved in business secrets, it is necessary to input the protect password in the XBRL software. In this paper, we design a protection scheme based on RSA encryption algorithm of XBRL software, and implement sub element encryption to protect software in the transmission process of XML data, which will make XBRL tax software have high security and practicability.**

Key words - XBRL software; Tax system; Encryption; Design

I. INTRODUCTION

The application of Extensible Business Reporting Language (XBRL) spreads more and more widely in the world, many stock exchanges require XBRL instance of the listing corporation financial statements, and it is also widely applied in tax reports. The Royal tax and customs (HMRC) has been used XBRL inline, Hong kong, Singapore and other countries or regions also require the use of XBRL instance to carry out tax reports. Through the application of XBRL, the tax information of each enterprise can be directly produced by the same database of the company's financial statements. However, the extension and openness of XBRL makes the security performance of the report not high, while the XBRL software tax reporting information is often involved business secrets, the protection of the password in the XBRL software is a prerequisite for the application of XBRL software in the field of tax payment. In this paper, we design and implement a XBRL software tax registration code protection scheme based on RSA encryption algorithm, and overcome the shortcomings of the traditional code protection technology security, and implement the software protection in the process of XML data transmission, so that the security and practicability of XBRL tax payment application software is relatively high.

The main design goal of the system is to improve the security of the registration code. A high security registration code protection system must have the security of registration code verification mechanism and anti dynamic debugging and so on. The overall design goal of the security registration code system based on RSA Public Key System (RSA) algorithm can be summarized as the following four points: Firstly, it has secure registration code generation and verification algorithm. From the research on the form of the registration code, we can see that the security encryption and decryption algorithm is the core of the registration code protection technology, only the use of complex encryption and decryption algorithm to a certain extent to prevent the algorithm to be cracked easily. Secondly, it has secure registration code verification mechanism. Different registration code verification mechanism will bring different levels of security risk, especially the use of the registration code verification algorithm, the registration code and other information in the main memory of the user authentication mechanism, the threat to the security of the registration code is fatal. Thirdly, the registration code bands the host hardware information. Using the unique and non variability of the host hardware parameters, the protection mode of the code of a machine is realized, which is also a security policy for the current mainstream code protection technology. Fourthly, the registration code system has a certain reverse analysis ability. Using the reverse analysis tool, we can analyze and debug the verification process of the registration code, and realize the crack of the code by extracting the algorithm or modifying the program jump instructions. So the time of anti-cracking of software can be effectively prolonged by using the anti-reverse analysis technique.[1,2,3]

II.SYSTEM ARCHITECTURE AND MODULAR DESIGN

According to the requirements of the overall system design, the XBRL security registration code system is mainly composed of the main hardware information acquisition and processing module, encryption dog processing, verification module, registration code verification module, as well as anti-reverse analysis, software verification code authentication and other security auxiliary module[4,5], Figure 1 is the overall architecture diagram for the security code system.

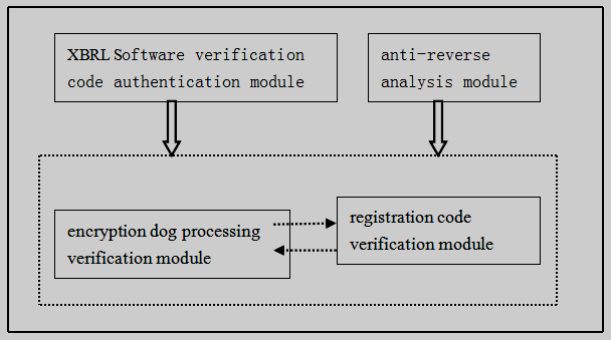

Fig.1 The Overall Architecture Diagram For The Security Code System.

A. XBRL Registration Verification Code Authentication Module

The main function of the module is to verify the validity of the software distribution version, software dealers will provided a software verification code to the user to bind the software. Users in the software registration operation before the first software verification code certification operation, only through the certification of the module to carry out the registration operation, the module is actually attached to the security module.

B. Encryption Dog Processing Verification Module

The module has two functions. On the one hand is the acquisition of the user's hardware information such as disk serial number, Media Access Control(MAC), etc., and the relevant hardware information for the Hash operation to get the user name ID required by the registration operation, to hide the host expressly hardware information[6]. On the other hand, the module generates the relevant parameters of the registration code generation algorithm, and the ID information provided by the software users to do encryption operation, generate the corresponding mathematical mapping results, and the registration code and verification algorithm related parameters are distributed to the software user.

C Registration code verification module

The module is to verify the authenticity for the user input of the user name ID and registration code based on the selection of the registration code verification mechanism, through the registration code to decrypt the operation to obtain the corresponding user name ID* and compared with ID to determine the results of the verification[7,8].

D Anti-reverse Analysis Module

The main function of this module is to make the system have the ability of anti reverse analysis by using the anti - static disassembly and anti - dynamic debugging strategy in the security registration system. Because of the use of reverse analysis technology can be used to tamper with the implementation of the program, and extract the registration algorithm and other methods to achieve the software crack and make the corresponding registration machine, therefore, the ability to reverse the reverse analysis of the system is very important for the safety of the registration system[9,10,11].

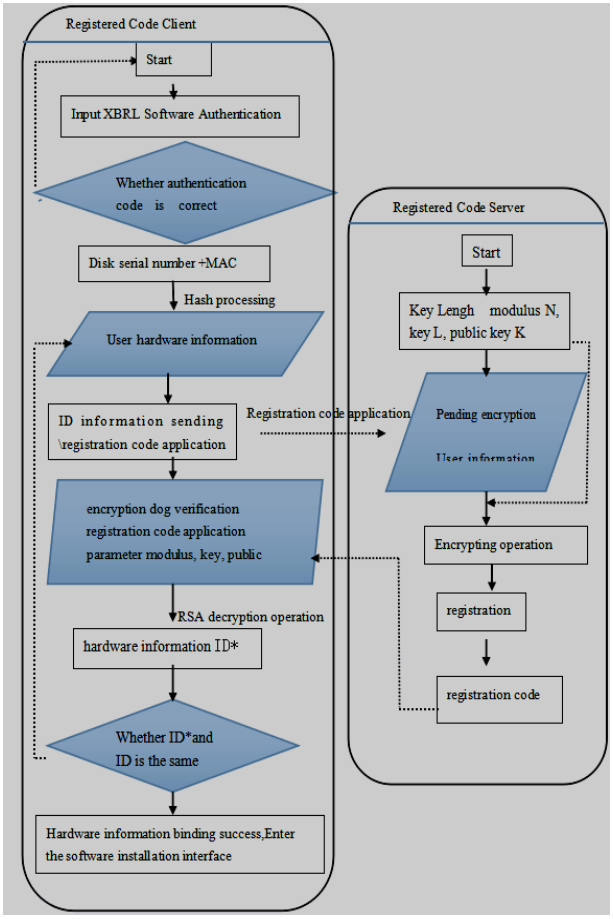

Fig.2 Detail Design Flow Chart of The Secure Registration Code System

Figure 2 is detail design flow chart of the XBRL secure registration code system based on the RSA algorithm. The whole system is divided into the registered code client and the server side of the registration code. The registered code client mainly provides the registration code for the software user, the registration code verification, the registration code server side mainly provides the registration code generation, the registration code distribution and so on.

III. IMPLEMENTATION AND VERIFICATION OF SYSTEM

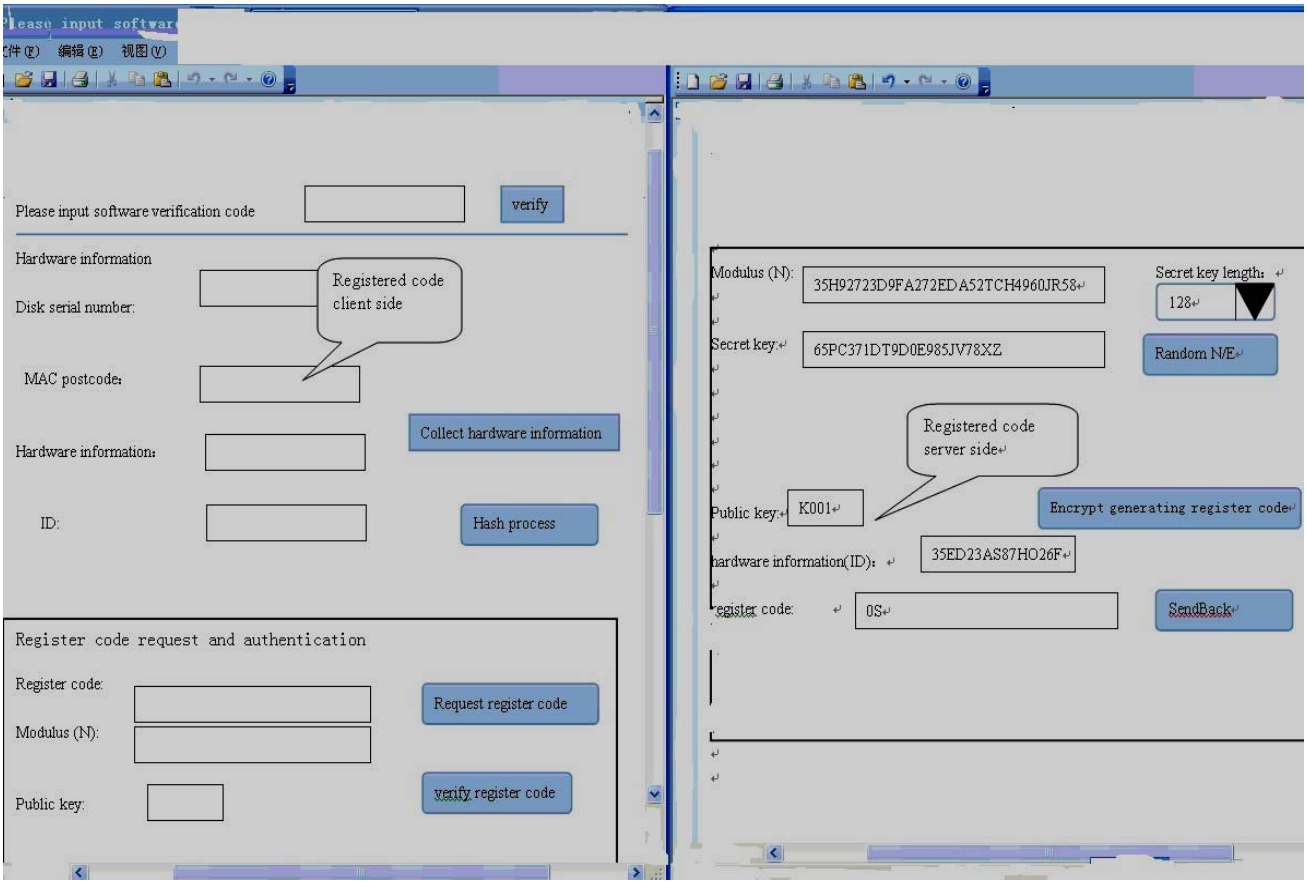

Fig.3 Security Registration Code System

Figure 3 is based on the RSA algorithm to achieve the security registration code system demonstration platform, the demonstration platform is divided into three parts: the registered code client window, the registered code server and the output window. The following section based on the detailed design of the system process and in accordance with the actual operating sequence, the system involved in the functional modules of the test validation, as follows:

A. XBRL Software Verification Code Authentication Module.

Enter the security registration code system platform, only software verification code recognition The card module and the register code generating module are in the active state. Software users need to enter the correct software verification code[12]. The hardware information acquisition and processing module of the software can be activated. Enter the correct software verification code in the dialog box. "MUCT", click the "verify" button, and the results are shown in Figure 4.

B. Module of the Encryption Dog Verification Software.

After the completion of the verification code, click on the "collection hardware information" button, to obtain the user's disk serial number and MAC address information, and the combination of both. Then click on the "Hash" button, the host hardware information to do Hash processing to get ID. After the use of the ID as a registered code name, to prevent the host hardware expressly information appear in memory.

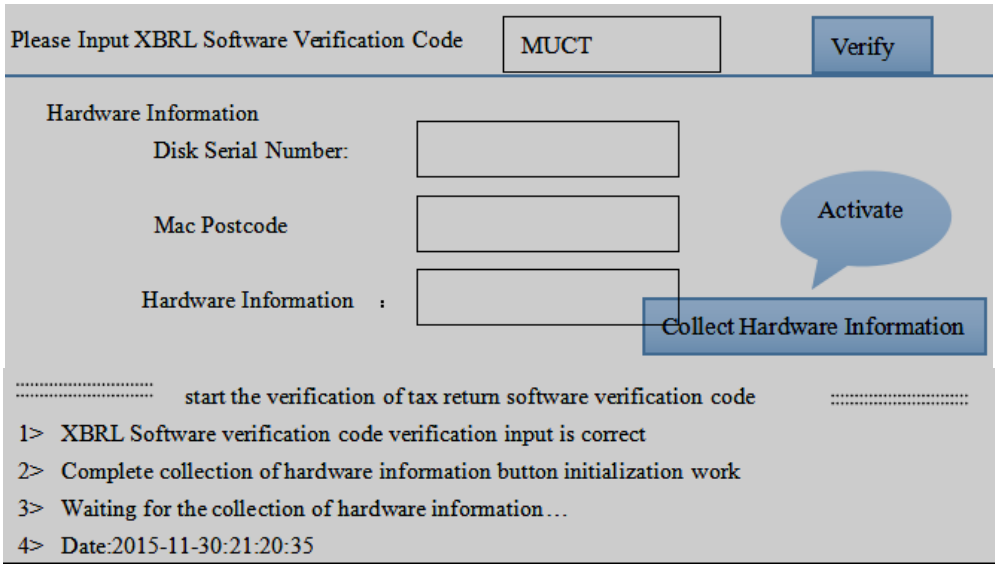

Fig4. Functional Demonstration of the Verification Code Authentication Module

First of all, the user needs to enter the correct software verification code, and then collect the host hardware information and the collection of good hardware information for Hash processing, get the user ID. Click on the "request for registration code", will send the ID information to the server side, request to generate the serial number as shown in Figure 5.

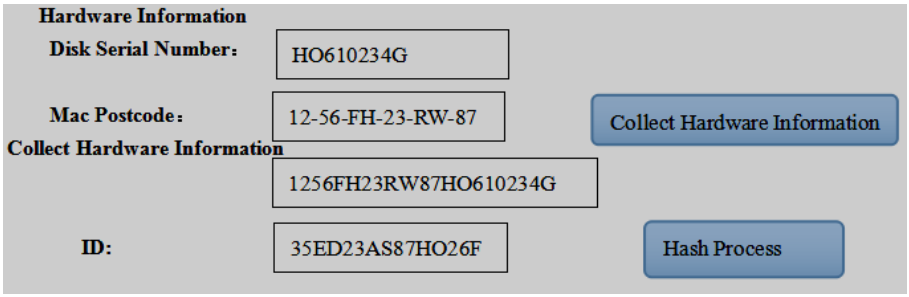

Fig.5 Process Functional Demonstration of Hardware Information

After the completion of the last step, click on the registration code, the ID information will be passed to the registered code server, thereby entering the registration code generation module. In this module, we need to set the relevant parameters of RSA encryption algorithm, first select the key length in the drop-down list, and then click on the "N/E" button, will be randomly generated parameter modulus, key, public key. Click to generate the registration code, the user's hardware information RSA ID encryption operation, get the corresponding registration code information as shown in Fig.6).

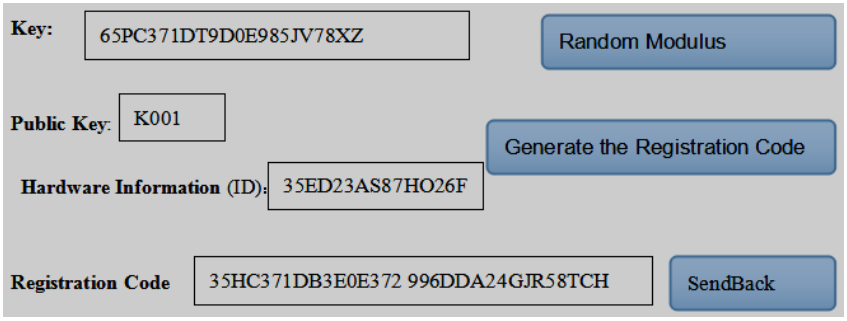

Fig6. Functional Demonstration of Generating the Registration Code

C Registration Code Verification Module.

After the registration code is generated, the SendBack button is clicked, the registered code server sends the generated registration code to the registered code client, and the RSA algorithm is used for registration code verification. Click on the "verify registration code" button, the software by the use of RSA algorithm to decrypt the user entered the registration code to obtain its corresponding ID', ID and ID' comparison to determine the authenticity of the registration code, the specific reference in Fig.(7).

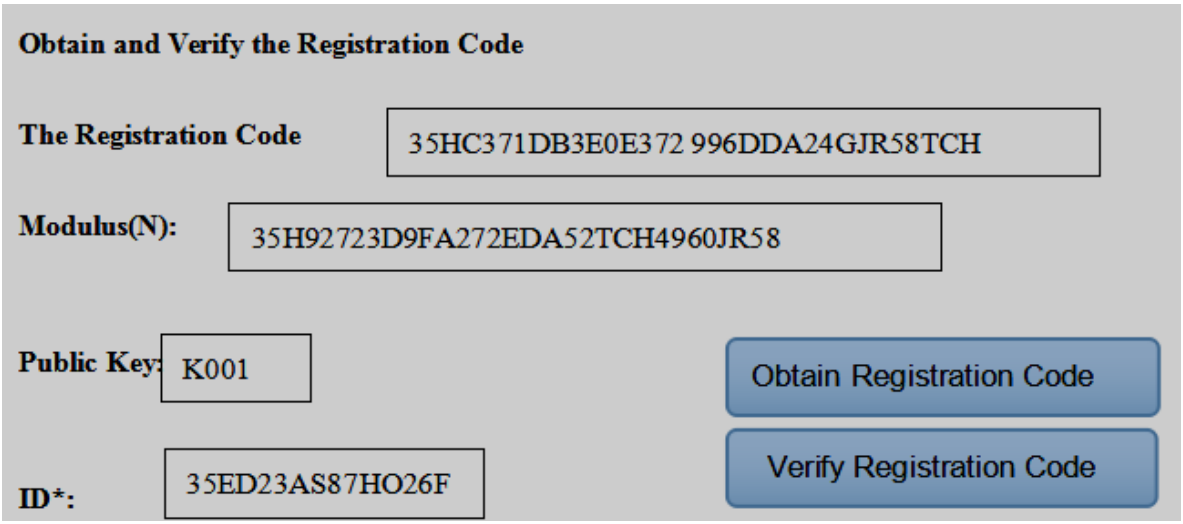

Fig.7 Functional Demonstration of Verifying the Registration Code

D. Reverse analysis module.

Anti-reverse analysis module is designed to protect the safety of the code system to resist static analysis and dynamic debugging. The specific protection measures can be determined by software developers themselves.
At this point, the functional verification of the security registration code system based on RSA algorithm is completed. Through the functional test, the registration code system can effectively avoid the defects of the traditional registration code protection technology, and the use of asymmetric encryption technology and reverse analysis technology has greatly improved the security of the registration code generation and verification process[15]. In certain, the registration code system in the implementation of efficiency will be subject to the RSA algorithm encryption speed slow, but for the safety performance requirements of higher software or has its unique advantages.

IV.THE TAX ELEMENT ENCRYPTION

For XM format data, key encryption can be used for the full text encryption, but also can be used for the element encryption , which is very important in practical application. It not only makes the encryption can be accurate to the sub elements, but also can be seamlessly combined with the encryption elements and the non encryption elements in a document[13,14]. The following is a XML format description of the steel simulation offer.

<? xml version=”1.0”encoding=”UTF-8”?>
<Value added tax sheet>
<addresser name=” Wuhan iron and steel”></ addresser>
<addressee name=”Shanghai Automobile”><price sheet>steel><encrypted element algorithm=”des/cbc”contenttype=”text/xml” encoding=”base64”?
>Fdakjjljw4563763hfls678432987fhlry689y698y7r29yuh fkjs007r836653t52hfkdshfshkjfuw+qtewyquuewhfdksn43 56+8tyuwyi2yr34y4hrkewhkwjfl+cj+tdhjhfkwhlfjhksdhfli jw/fhkdshflkdsfhslfoire9cs/jflsjfpmm=fhdkjsh+7ss</ encryptedelement>
<validtime>2015-11-30</ validtime></steel ></price ></addressee >
</addressee name=”Shanghai Automobile”>
……
</ Value added tax sheet>

In this VAT tax returns, value-added tax is not open, the taxpayer can set the VAT tax according to the factors of the market volume , production cost and tax rates, to produce a piece of the original tax returns, then encrypt the purchase price, and hand it over to the computer agents (in a computer message queuing), the next step is agent extract and transfer the purchase price to the

corresponding tax authorities (Addressee) , the whole process agent always don't know steel sales purchase price quotation.

V. CONCLUSION

The tax check system can automatically identify the different relationships among the information elements of financial reporting by implementing a security registration code system based on RSA algorithm, meanwhile, add the tax element encryption in the system, which can combine the encryption elements with the non encryption elements in a document. The system will develop an in-depth analysis of automatic inspection model, which is conducive to the service institution quickly and accurately locked tax doubts, and it will greatly reduce the tax cost, eliminate tax trouble of the taxpayer may return the tax reports to the tax authorities during the period of tax reports, construct and maintain a good tax environment.CONFLICT OF INTERESTThe authors confirm that this article content has no conflicts of interest.

ACKNOWLEDGEMENTS

This research was financially supported by the Science & Technology Planning Fund of the Science & Technology Department of Hunan, China (No.2015TP1048), the Education Science Fund of the Education Department of Hunan, China (No.2015C236), and Hunan Financial and Economic Institute research topic of Hunan, (No.k201315)

REFERENCES

[1] P.Beaucamps and E.Filiol. “On the possibility of practically obfuscating programs towards a unified perspective of code protection”, Journal in Computer Virology. Vol.2 No.01,pp.3-21, 2007.

[2] Sun Jing, Wang Yajun. “XBRL, the impact of tax collection and administration in China”, Financial supervision. Vol 13, pp. 64-66,2014.

[3] Matthias Jacob, Mariusz H. Jakubowski, Ramarathnam V. “Towards integral binary execution implementing oblivious hashing using overlappedinstruction encodings”, Proceedings of the 9th Workshop on Multimedia & Security, New York: ACM Press,pp. 129-140 , 2007.

[4] Brumley D, Poosankara P, Xiaodong D, et al. “Automatic Patch-Based ExploitGeneration is Possible”, Techniques and Implications. IEEE Symposium on S&P. NewYork:IEEE, pp.143-157, 2008.

[5] Chen Hong, Hu Xiaoqin. “A software protection method based on. RSA ” ,Journal of Sichuan University (NATURAL SCIENCE),Vol 4,pp. 789-795,2011.

[6] Shang Tao, “the valley of Dawu. Software anti compilation technology research. ” , The research and application of computer, Vol 12,pp. 4553-4557,2009.

[7] Kuang Ling Yun, Wu Lijia. “ The tax inspection system of L technology based on R platform X B”, Professional time, Vol 10,pp.103-106,2013.

[8] Leewei “the.XBRL revolution regulation”. Securities market Herald, Vol 1. pp.4-8,2009.