Research on Anonymous Scientific Research Project Evaluation Information System

Xianguo Wang[1], Zhongli He[1,*], Juan Ding[1], Chunxi Guan[1], He Huang[1], Bowei Pang[1] and Guangfa Tang[1]

[1]*School of Information Science, Guangzhou Xinhua University*
7 Yanjiangxiyi Road, Mochong Town, Dongguan, Guangdong, China, 523133
[*]*Corresponding author: 1210461200@qq.com*

Abstract

In order to ensure the information security in the evaluation process of scientific research projects, eliminate bias and violations in the evaluation process, and promote the fairness, justice and information security protection of scientific research academic evaluation. This paper focuses on the framework and process of anonymous scientific research project evaluation information system, and proposes a scientific research project evaluation information system with double-blind mechanism. This study proposes a reasonable and credible scientific research project evaluation information system, which can also be embedded in the scientific research project management information system of enterprises and institutions and other related project management information systems.

Keywords: *project evaluation, digital signature, ElGamal algorithm, anonymity, double blind mechanism*

1. INTRODUCTION

To implement the spirit of the State Council's notice on several measures to optimize scientific research management and improve scientific research performance, the Ministry of Science and Technology of the People's Republic of China organized the comprehensive performance evaluation of national key R&D projects (GF [2018] No. 25),on deepening the reform of project evaluation, talent evaluation and institutional evaluation, and opinions on further strengthening the construction of scientific research integrity, especially the code for comprehensive performance evaluation of national key R&D projects (Trial) have been formulated. Scientific research project management includes project life cycle PDCA management. Its core contents include project initiation management, project performance management, project closure management, etc. Review is an important part of project management.

Project evaluation is the focus of scientific research project management. In order to prevent power rent-seeking and favoritism, the appropriate use of anonymous evaluation is very important. With the acceleration of the process of informatization, the scientific research institutes and universities in all provinces have introduced informatization management systems for scientific research projects to achieve a more effective evaluation process for scientific research projects. In order to ensure fairness, impartiality and information security, the evaluation system of scientific research projects should be designed with high security, keep anonymous function, and achieve fair, scientific and effective results. In order to prevent applicants and scientific research evaluators from practicing favoritism and malpractice, the evaluation system should be designed to ensure anonymity in the evaluation process. If the project application materials are found to be untrue, the appraiser has the right to decode and access the personal information of the corresponding applicant, and be responsible for the personal information of the applicant. Based on RSA and Elgamar algorithms, and the introduction of digital signature technology, Xiaotong Zhang [10] improved it and applied it to the internal control information system in 2016. On the basis of Xiaotong Zhang's research and the same model, Hanbin Yan [2] made some modifications to reduce the vulnerability risk and improve the overall security level by adjusting the algorithm. The above concepts will be introduced in the design of scientific research project evaluation information system. The algorithm is divided

S. A. R. Khan et al. (Eds.): ICMSSE 2022, AHCS 12, pp. 266–272, 2023.
https://doi.org/10.2991/978-94-6463-056-5_38

into eight phases: system initialization, project applicant registration, applicant account verification, application material submission, internal evaluation processing (evaluation materials of scientific research project evaluators), external evaluation invitation (evaluators of other schools, organizations or institutions), external evaluation processing, result confirmation and announcement. The research on the last seven phases will focus on discussing its contents, and proposing a solution that can meet the requirements of computational security and theoretical security.

2. LITERATURE REVIEW

With the development of information technology and the popularization of the Internet, information security technology has been widely used to reduce deviation and problems caused by manual processing. The introduction of information management system is a key solution to improve complexity management. It can not only reduce management costs and improve work efficiency, but also identify operational risks in project management, thereby improving the efficiency of project implementation. Anonymous function is a key technology in the project evaluation system. It not only meets the needs of solving problems in the process of project evaluation, but also has great value in other fields and industries.

At present, the research on project evaluation mainly focuses on the level of system guarantee. Yang xuting and Qiao gang, as representatives of peer evaluation and scientific research performance evaluation in New Zealand, have established a project evaluation material review system, a stakeholder avoidance system, a review system for the whole evaluation process, a confidentiality and appeal system, and adopted systems to standardize evaluation behaviors and protect the rights and interests of all parties [11]. On the basis of reviewing and commenting on the research of R&D project evaluation, Youmin Xi and Liexun Yang put forward an overall model of R&D project evaluation in combination with the project life cycle theory, compared three types of evaluation in the overall model, namely, project approval evaluation, progress evaluation and performance evaluation models, and studied the correlation, relative importance, evaluation enforcement and other factors of the three types of evaluation. Propose the project evaluation chain, and study how project undertaker, evaluator and manager use the evaluation results according to the evaluation chain to establish an overall model evaluation chain for R&D project evaluation [1] [3] [12] [14].

In recent years, several scholars [2] [4] [10] have applied the digital signature technology of information security to the design of information systems, combining theory with practice. According to this design concept, this research will propose an anonymous scientific research project evaluation information system. It is expected that the research will bring some enlightening suggestions and may improve this kind of system.

3. RESEARCH METHOD

Based on the concept of information security technology and management, it aims to introduce cryptography and information security mechanism into the scientific research project evaluation information system [13] to meet the requirements of the system. When the project applicant submits the application materials, the information system can be set in two modes:

- Applicants identification information is available;
- Applicant identification information is not available (double blind mechanism).

Based on this design concept, the applicant and external appraisers are anonymous to each other. The anonymous solution in this study is conditional, that is, during the submission process, the submitter and the external evaluator are anonymous to each other, and the internal evaluator and the external evaluator are anonymous to each other, which means that the information system and the internal evaluator are respectively responsible for contacting and announcing the evaluation results.

The algorithm can be divided into seven phases: project applicant registration, project applicant account verification, application material submission, internal evaluation processing (evaluation materials of unit evaluators), external evaluation invitation (evaluators of other schools, government organizations or institutions), external evaluation processing, confirmation and announcement of results. The process of each phase will be described as follows:

Phase 1: the applicant registers an account in the system.

Phase 2: verify the application and the applicant processing accounts.

Phase 3: the applicant submits the application materials for professional title.

Phase 4: school evaluators obtain system application materials.

Phase 5: school assessors invite external assessors from other schools, organizations or institutions.

Phase 6: external evaluators accept the invitation, conduct evaluation and give feedback.

Phase 7: internal assessors confirm the assessment results and announce them.

As showed in figure 1.

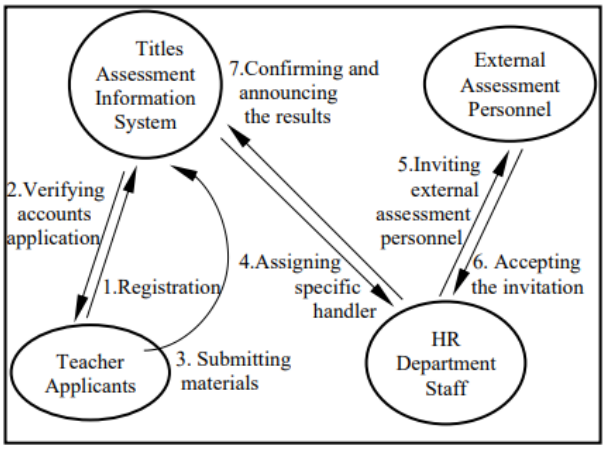

Figure 1: The conceptual framework of the study.

pi: a prim, normally with the length of 1024 bit or longer.

g: the primitive root of the prim pi.

yi: the value of a public key.

xi: the value of a private key.

3.1 The Phase of System Initialization

In the phase of system initialization, all applicants of the system, including thesis defense graduate, system center, internal assessment staff and external assessment personnel, register accounts and set passwords, and share the parameter of primitive root and a prim.

Applicant randomly selects a number as his satisfied secret key, calculates his public key.

(1) ya ≡gxa (mod p)

System center (scientific research information system center) randomly selects its secret key, calculates their public key and then publishes the public key.

(2) yb ≡ gxb (mod p)

Internal assessment staff (staff in scientific research department) randomly select their secret key, calculate their public key and then publish the public key.

(3) yc≡ gxc (mod p)

External assessment personnel randomly select their secret key, calculate their public key and then publish the public key.

(4) yd≡ gxd (mod p)

As showed in figure 2.

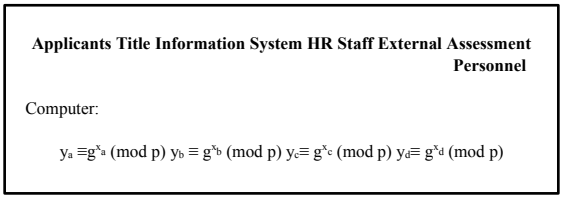

Figure 2: The phase of system initialization.

3.2 The Phase of Applicants' Registration

Applicants use their secret key and the public key in the system center to calculate a temporarily effective account.

(5) $R_a \equiv y_b^{x_a} \pmod p$

As showed in figure 3.

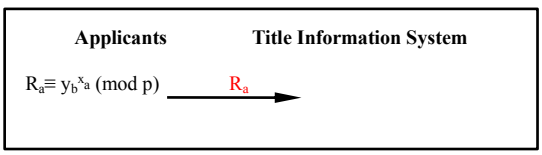

Figure 3: Registration.

3.3 Verification of Applicants' Accounts

When receiving the applicants registration, the system center will verify and reply that is:

(6) P0≡ (Ra)xb-1 (mod p) and

(7) Pa≡ (P0)kb (mod p)

As showed in figure 4.

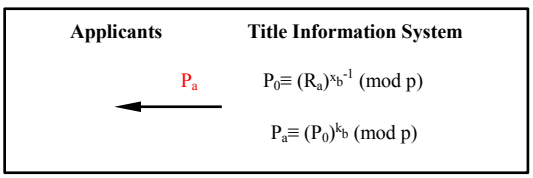

Figure 4: Verification of the application of accounts.

3.4 The Phase of Application Materials Submission

Applicants get effective accounts and submit all the required digital materials anonymously through the accounts.

(8) Sa≡ (Pa).ycka .m (mod p)

As showed in figure 5.

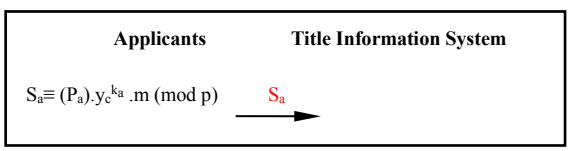

Figure 5: The phase of system initialization.

3.5 The Phase of Internal Assessment Staff Processing

Once receives the application materials from applicants, the system center will forward to internal assessment staff for processing. The process please refers to Formula (9).

(9) $Fa \equiv (Sa).ya\text{-}kb \pmod p$

As showed in Figure 6.

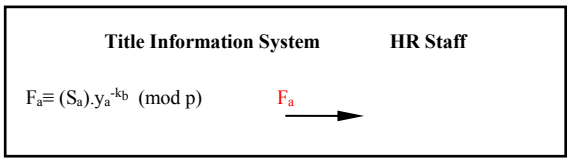

Figure 6: Internal assessment staff processing the applications.

3.6 The Phase of Invitation of External Assessment

Once receive the notification from system center, internal assessment staff invite the external personnel to do assessment. The process please refers to Formula (10).

(10) $Ia \equiv (Fa).ydkc .raxc \pmod p$

As showed in Figure 7

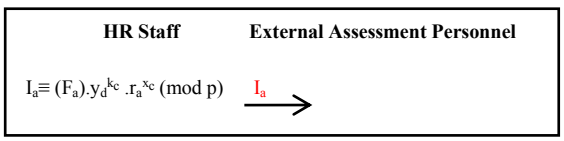

Figure 7: Inviting external assessment personnel.

3.7 The Phase of External Assessment Processing

External personnel accept the invitation and do the assessment, referring to the Formula (11) and (12) and give feedback to internal assessment staff later. The process please refers to Figure 8.

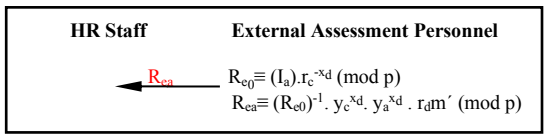

Figure 8: External assessment personnel confirming results and giving comments.

(11) $Re0 \equiv (Ia).rc\text{-}xd \pmod p$ and

(12) $Rea \equiv (Re0)\text{-}1. ycxd. yaxd. rdm' \pmod p$

3.8 The Phase of Result Confirmation and Announcement

Once internal assessment staff receive the feedback from external personnel, they will check the content and announce the assessment result. (Refers to Formula (13)).

(13) $Ca \equiv (Rea). yd\text{-}xc \pmod p$

As showed in Figure 9.

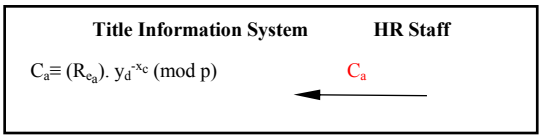

Figure 9: Confirmation and announcement of the results.

Proof:

(14) $m' \equiv (Ca) \pmod p$

$\equiv (Rea). yd\text{-}xc. m\text{-}1 \pmod p$

$\equiv (Re0. ycxd. m') \pmod p$

$\equiv m. ycxd . m'.yd\text{-}xc. m\text{-}1) \pmod p$

$\equiv m' \pmod p$

As showed in Figure 10.

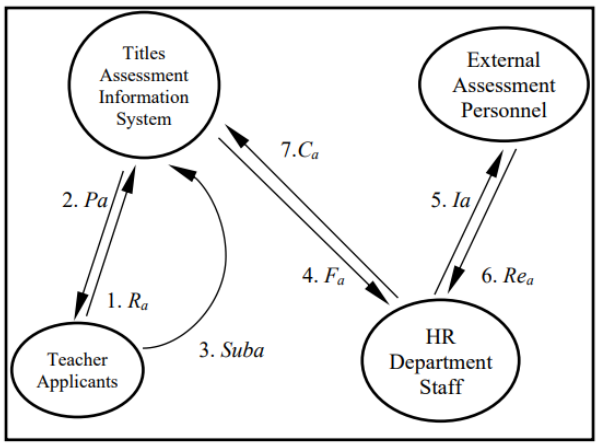

Figure 10: The transfer of parameters in the solution.

4. SECURITY ANALYSIS

Definition1. Discrete Logarithm Problem, DLP.

When the formula comes to $y_i \equiv g^{x_i} \pmod p$, and parameters $\{p, g, y_i\}$ are given, the parameter x_i needs to be solved. When the prim becomes p bigger, it is hard to calculate x_i from the algorithm available currently, which makes x_i impossibly be solved in the foregoing formula.

This is so-called Solving Discrete Logarithm Problem [10]. The parameter p in the current public key cryptosystem based on discrete logarithm are larger than 1024bit length or 2048bit length.

Definition 2 Computation Diffie-Hellman Problem, CDHP

The Computation Diffie-Hellman Problem [8] derives from the theory of Diffie–Hellman Key Exchange, with the main idea as following:

When $\{g, g^x, g^y\}$ are given, g^{xy} needs to be solved. The parameter g is known, and the other parameters x and y are unknown.

Definition 3 Decisional Diffie-Hellman Problem, DDHP [5] [6] [7] [8] [9].

Decisional Diffie-Hellman Problem (Wikipedia, Discrete logarithm) is the variant from Computation Diffie-Hellman problem, in which we need to find out the possibilities in z_p that satisfy z=xy with the given parameters $\{g, g^x, g^y, g^z\}$. When $\{g, g^x, g^y\}$ are given, g^{xy} needs to be solved.

The parameter g is known, and the other parameters {x, y, z} are unknown.

4.1 Theoretical Security Level Analysis

Lemma 1. If applicants are honest, the Formula (6) will be effective, that is system center verifies applicants.

Proof:

An applicant submits R_a registration application to system center Formula (5)

System center calculates $P_0 \stackrel{?}{\equiv} y_a \pmod p$ with its secret key x_b^{-1} Formula (6)

If the results are not identical, the applicant did lie. Since the applicant has already used its secret key x_a in Formula (1), he cannot deny his action. Therefore, in this solution, applicants' actions are undeniable.

Lemma 2. If system center is honest, the Formula (7) will be effective, that is applicants verify system center.

Proof:

The system center will calculate P_a from k_b and P_0 Formula (5)

Return to applicants, and the applicants can calculate $P_a \stackrel{?}{\equiv} r_b$ Formula (15)

If the results are not identical, the system center may lie.

(15) $r_b \stackrel{?}{\equiv} (P_a)^{-x_a} \pmod p$

$\equiv (P_0^{k_b})^{-x_a} \pmod p$

$\equiv (y_a^{k_b})^{-x_a} \pmod{}$

$\equiv (g^{x_a k_b})^{-x_a} \pmod p$

$\equiv r^b \pmod p$

Lemma 3. If the internal assessment staff are honest, the Formula (9) will be effective, that is

system center verifies internal assessment staff.

Proof:

System center forwards F_a to the internal assessment staff, Formula (9)

Since there is no direct links between applicants and internal assessment staff, internal assessment staff cannot access the personal identification information and the submitted materials of the applicants. If internal assessment staff need to use their own secret keys to decode the content of F_a, which is showed like in Formula (16).

(16) $m \equiv F_a . r_a^{-x_c} \pmod p$

(17) $m \stackrel{?}{\equiv} (F_a) . r_a^{-x_c} \pmod p$

$\equiv y_c^{k_a} . m . r_a^{-x_c} \pmod p$

$\equiv g^{x_c k_a} . m . g^{-k_a x_c} \pmod p$

$\equiv m \pmod p$

Lemma 4. If both internal assessment staff and external assessment personnel are honest to each other, the Formula (10) and (12) will be effective, that is internal assessment staff and external assessment personnel verify each other.

Proof:

The internal assessment staff forward I_a to external assessment personnel. External assessment personnel can decode it with their secret key x_d, to restore R_{e_0} to m, which is showed like in Formula (11), otherwise the external assessment personnel are believed to be conducting lies.

Please refer to Formula (18) for detailed explanation.

(18) $m \stackrel{?}{\equiv} R_{e_0} \pmod p$

$\equiv m . y_d^{k_c} . r_c^{-x_d} \pmod p$

$\equiv m \pmod p$

External assessment personnel send back the R_{e_a} to internal assessment staff. Internal assessment staff can get the assessment comments m′ if they do use their secret key x_c to decode, which is shows as in Formula (13). otherwise, the internal assessment staff are believed to be conducting lies. Please refer to Formula (19) for detailed explanation.

(19) $m' \stackrel{?}{\equiv} C_a \pmod p$

$\equiv R_{e_a} . y_d^{-x_c} . m^{-1} \pmod p$

$\equiv m . y_c^{x_d} . m' . y_d^{-x_c} . m^{-1} \pmod p$

$\equiv m' \pmod p$

4.2 Practical Security Level Analysis

Table 1: The framework of the solution.

Model	P1	P2	P3	P4	Notes
1	0	0	0	0	
2	0	0	0	1	
3	0	0	1	0	
4	0	0	1	1	
5	0	1	0	0	
6	0	1	0	1	
7	0	1	1	0	
8	0	1	1	1	
9	1	0	0	0	
10	1	0	0	1	
11	1	0	1	0	
12	1	0	1	1	
13	1	1	0	0	
14	1	1	0	1	
15	1	1	1	0	
16	1	1	1	1	

The definitions and usages of some symbols:

P1: applicants' identifications are available to internal assessment staff.

P2: applicants' materials are available to internal assessment staff.

P3: applicants' identifications are available to external assessment personnel.

P4: applicants' materials are available to external assessment personnel.

Here 1 refers to Yes, and 0 represents No. For example, 0111 in model 8, which means that internal assessment staff have the access to the applicants' materials instead of their personal identification information. Meanwhile, external assessment personnel have the access to both the applicants' materials and their personal identification information. By analogy, we can have 16 different conditions.

Our solution is just as model 6, which means that internal assessment staff do not have access to applicants' personal identification information. Under certain conditions, materials submitted by applicants are available to them. Besides, external assessment staff do not have access to the applicants' personal identification information, but the materials they submitted.

The concerns of the confidentiality of applicants' identification: applicants submit the materials to system center anonymously. Internal assessment staff access the original content through the Formula (16), while applicants' personal identifications are still available to them. External assessment personnel access the original content through the Formula (11), while applicants' personal identifications are still available to them. Therefore, applicants are anonymous to both internal and external assessment staff. To a certain extent, it prevents the reveals of the applicants' personal identification.

The risks of the reveals of the content: if the system center gets invasion, hackers' intension to steal the contents submitted by applicants will be in vain. Only internal assessment staff and external assessment personnel can restore digital content under certain conditions. In any other phases, for example (8), (9) and (13), system center is unable to restore the encrypted digital content to. No matter hackers come from internal assessment staff or external assessment staff, they can only get the, but not the personal identification information. Therefore, there is no need to worry about the confidentiality of applicants' identification even the original contents are revealed. The problem of secret key embezzlement: applicants, system center, internal assessment staff and external assessment will keep their own secret keys, even their public keys are available to each other. Hackers are unable to calculate the corresponding secret key with the given public key, which has been fully discussed in the Discrete Logarithm Problem in definition 1, unless the possessors reveal their secret keys purposely. This study will not discuss this hypothesis.

5. CONCLUSIONS

The improved algorithm is applied to the scientific research evaluation information system for the first time. This is an anonymous system, in which the identity information of the applicant is strictly confidential. If the content submitted by the applicant is untrue, the internal evaluators and the system center can track the anonymous identity under certain conditions and evaluate the applicant's true identity, which can not only protect the confidentiality of the applicant's identity information, but also prevent the applicant from appearing.

Deliberately solve the problems and difficulties in the process of project evaluation when applying. In this paper, three lemmas, three definitions and 19 formulas are proposed, which have a strong theoretical basis. This study is practical and may bring some enlightening suggestions to similar research and the practice of actual project evaluation.

ACKNOWLEDGEMENTS

This work was financially supported by Educational Commission of Guangdong Province, China (Grant

No.2020KTSCX201, No.2021KTSCX169, No.2021ZXRC001, Educationa Foundation of Guangzhou Xinhua University (Grant No.2021XX003, 2021YQSX004, 2022J024).

REFERENCES

[1] Gang Zhao (2022). Analysis on financial acceptance of scientific research project funds. J. Brand Research.11.

[2] Hanbing Yan (2017) Comments and improvements on the scheme of dual complexity and anonymity.J. Journal of Fujian Polytechnic Normal University. 2,23-29.

[3] Jiaming Yu (2022). Research on cost management of scientific research projects in Colleges and Universities. J. Co-Operative Economy & Science.11.

[4] Minjuan Lin (2015). Design and implementation of personnel file management system based on B/S mode.J. Computer CD Software and Applications. 18(01), 33-34.

[5] Wikipedia. Access Control Matrix.EB/OL, https://en.wikipedia.org/wiki/Access_Control_Matrix.

[6] Wikipedia. Computational Diffie–Hellman assumption. EB/OL, https://en.wikipedia.org/wiki/Computational_Diffie%E2%80%93Hellman_assumption.

[7] Wikipedia. Decisional Diffie–Hellman assumption. EB/OL, https://en.wikipedia.org/wiki/Decisional_Diffie%E2%80%93Hellman_assumption.

[8] Wikipedia. Diffie–Hellman key exchange. EB/OL, https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange.

[9] Wikipedia. Discrete logarithm. EB/OL, https://en.wikipedia.org/wiki/Discrete_logarithm.

[10] Xiaotong Zhang (2016). Research on internal control information system based on double complexit.J. Journal of Fujian Polytechnic Normal University.5,27-34.

[11] Xuting Yang (2022). Peer reviews in New Zealand Research Fund Project.J.. Higher Education Development and Evaluationh.38(02).

[12] Youmin Xi (2002). Research on the overall model of R&D project evaluation.J. Systems Engineering-Theory & Practice.10.

[13] Zhenglian Liu (2018). Research on anonymous petition information system.J. Journal of Fujian Polytechnic Normal University. 2,46-52.

[14] Zhizhou Ji (2022). Evaluation and incentive of scientific research projects based on the whole life cycle. J. Enterprise Management.3.