SECURE MULTI-PARTY COMPUTATION AND ITS APPLICATION STUDY IN THE FIELD OF MECHANICAL ENGINEERING

JIAN LI

Organization Department, Handan Polytechnic College, Hebei 056001, Handan, China,

E-mail: jianli_tou@163.com

ABSTRACT

Along with the development and globalization of information technology and manufacturing industry, the transmission and exchange of engineering information more and more depends on the network in the process of the enterprise cooperation and negotiation. It becomes more and more frequent to ensure the security of the information engineering, which will be the reality problems that more and more countries and enterprises pay attention to. The paper first gives an elaborative description of the concept of secure multi-party computation (SMC). Then the paper analyses the typical protocol of secure multi-party computation, further researches on the application in the field of engineering machinery manufacturing, eventually gets the conclusion that the secure multi-party computation has been the both public and confidential information exchange model, which also has brilliant application development prospect and huge potential in other engineering field.

Keywords: *Secure Multi-party Computation, Mechanical Engineering, Information Exchange, Computation Agreement, Correlation Coefficient*

1. INTRODUCTION

With the further research on intelligent monitoring diagnosis, the future application of intelligent monitoring system includes all aspects of information science. The diagnosis and application of intelligent engineering machine fault is based on CBR diagnosis technology, which provides reference for the future engineering practice [1]. In addition, based on the application of intelligent machines, the future development of science technology should be widely applied in all aspects, especially in metal mining industry in spite of high operation risk. The use of intelligent machines could replace manual labor, which can greatly ensure the personal secure. Secure multi-party computation can be understood as a group consisted of many members, and each member has a private variable input. Everybody's common goal is to calculate the same function, whose result is that everyone can get the right function solution, the whole project and the illicit close input information of all members in the process. But it couldn't tell any member in addition to the operator himself or herself.

The development of information technology makes the network users increase widely, and the computation and collaboration of the users also become more and more frequently. In another way, the collaboration project of internet users also needs more and more cooperation computation[2]. The project cooperation of enterprises has no trust in each other's ingredients in a certain degree. It also has the presence of competition among enterprises, so secure multi-party computation has certain complexity and distrust in the project cooperation among groups. As an important branch of modern cryptography field, secure multi-party computation is an important research object in the field of information security, whose task is to ensure that participants take participation in the projects. No common private input respectively is presented, but the whole team has a common output. That is to say, we should not only ensure the secure, but also ensure that the exceptant private information leak doesn't happen.

When the project cooperation appears the distrust phenomenon, security multi-party computation will play its important role at this time. We should effectively apply the whole multi-party computation in the project cooperation in order to reduce the danger coefficient of hidden data, to improve data security, which appears in the concept of secure computation[3]. The traditional distributed computing and information security multi-party computation have a new expansion as a new computing model appeared in network computing collaboration. For the current development of information technology, network, automation, intelligence, it is becoming more and more popular for the cooperation implementation of network project, which has very important practical value to solve the information security problems in network-related fields.

2. THE BASIC CONCEPT OF SECURE MULTI-PARTY COMPUTATION

2.1 Core Ideas Of Secure Multi-Party Computation

The core idea of secure multi-party computation includes many participants. Everyone can use a special way to calculate variable function. Each participant knows the eventual output results of the function, but all participants don't know the input which is variable conditions of the other members[4]. The difficulty degree of computation is decided by the individual behavior of the protocol members of secure multi-party computation. According to the individual behavior characteristics of the participation in security multi-party computation, we can divide the participants into three types, and the specific division is as below.

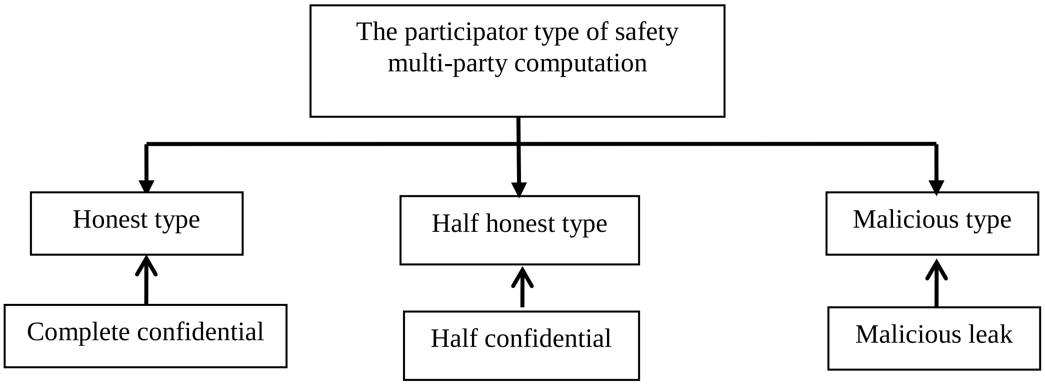

Figure 1: The Participants Type Of Secure Multi-Party Computation

As shown in Figure 1, the honest type members of secure multi-party computation can keep all the input information confidential according to the basis of the required input agreement in the computation. The half honest type participation members also should complete the computation protocol input in accordance with the required, but always keep the security of the input information in a half confidential state, for the detail operation has certain risks. For the malicious type participants, the process will not finish the corresponding information input according to the agreement, but also the whole information malicious may leak out[5]. In the whole implementation process of secure multi-party computation, we need to try our best to protect the secure demand of participant, and we should also protect the security needs of half honest participants and keep off the malicious members participants.

The whole process is shown in Figure 2, it includes the following several parts: Firstly, to establish the case database, and select the corresponding approximate case and current fault based on large scale case, to carry on complete alignment, and then through the computer operation, the intelligent control system from the database retrieves current case's some obvious features, to list one or more similar failure cases that can be available for reference; Secondly, by comparing with the listed fault cases, the intelligent monitoring system is not just a pure intelligence system that still contains artificial operation[6]. According to the selected and listed case from the relevant technical experts, to choose most similar fault with the present case, and then to register it. At the same time, use intelligent machine for equipment parts to carry on automatic coupling diagnosis. Then, based on experts' opinion, find out the current system or breakdown state of digital programming, so as to make the diagnosis conclusion; Finally, the diagnostic results of new case are input to the computer control system through intelligence machine, and the new case is compiled into the database that can be available for later reference learning[7,8].

2.2 The Security Of Secure Multi-Party Computation

In the practical application process of security multi-party computation, we must keep the agreement to solve the problem safely. For specific verification, the practice is to observe the whole secure multi-party computation whether can completely against attacks that are all known by us. Suppose we have m attack factors, it has the following equation[9]:

$$\begin{array}{ccccc} t & x_1^{(t)} & x_2^{(t)} & \cdots & x_n^{(t)} \\ 1 & x_1^{(t)} & x_2^{(t)} & \cdots & x_n^{(t)} \\ 2 & x_1^{(t)} & x_2^{(t)} & \cdots & x_n^{(t)} \\ & & \cdots & & \\ n & x_1^{(m)} & x_2^{(m)} & \cdots & x_n^{(m)} \end{array} \quad (1)$$

Namely,

$$\left\{X_1^{(0)}(t)\right\},\left\{X_2^{(0)}(t)\right\},\ldots,\left\{X_m^{(0)}(t)\right\} \quad (t=1,2,\ldots,N) \quad (2)$$

In formula (2) ,N is the input computation protocol length, which is equal to the number of datas, m is for sequence representive, m is for attack factors (variable). In addition, we can set time series for the following series[10]:

{X0(0)(t)} (t=1, 2, …, N) (3)

The time series is called for mother sequence, and the above m attack factors (variable) is referred to the subsequence, the protocol determination of multi-party computation is relative dynamic. Suppose $P=\{ p_1, p_2 ... p_0 \}$ is n members set, $F=(f_1, f_2..., f_n)=(y_1, y_{2...}, y_3)$ is known to participants and it is expected to calculate the objective function. The individual members have personal private input. Suppose the secret input of p_i is x_i, the expected computation ideal model of secure computation, we can add the trusted third party in addition to intrinsic participation members. And the third party can have the secret communication with any participant in the security channel. Since the secure coefficient of the third party is very high, we must complete it through the safe passage in the multi-party computation process. Each participant p is approved only through the third party in the whole process, which can obtain the objective function of the solution Wythe attacker m also can get x_i, therefore, the ideal model of secure multi-party computation includes the whole expected members.

2.3 The Application Implementations Of Secure Multi-Party Computation

The position of security multi-party computation in cryptography increasingly rises, and there is increasingly rich and safe in the traditional distributed computing and information security within the category. It also provides a new type of multi-party computation model in the modern network information computing. In today's expanding background of the electronic information, it becomes the popularization of the related research results, which also have a lot of, important applications in many fields. The specific is as below.

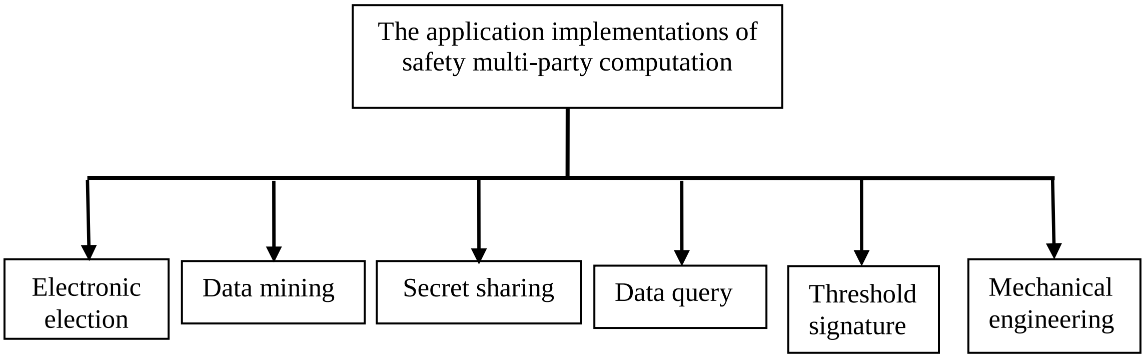

Figure 2: The Application Realization Field Of Secure Multi-Party Computation

As shown in Figure 2, secure multi-party computation has been realized in many fields. As the society develops quickly, and the information level of people is rising, the sensitive data collection and data processing secure has caused some confusion to related operations department in the enterprise cooperation. The existed data mining algorithm can lead information data leak out to a certain extent. So we need to find the applications of secure multi-party computation in more areas, which reflects its biggest application value[11].

3. THE APPLICATION OF SECURE MULTI-PARTY COMPUTATION IN ENGINEERING

Mechanical engineering effectively makes use of the theory natural science and technology to set production practice experience in human survival environment research and to solve the mechanical relevant areas of development, design, manufacturing, installation, use and repairment of the combination of practice and theory. It is one of the five elements in the human society for production and service , and it has important participant composition in energy and material production.

With the globalization of market competition, the manufacturing industry faces to more situations. As the intense competition of the global market, production mode is set by all kinds of large quantities, which is gradually transformed into many varieties. Product design of manufacturing process is no longer by an enterprise alone to have complementary characters. The powerful combination among enterprises focuses on the distributed design and manufacturing, product manufacturing, agile manufacturing, virtual manufacturing technology and advanced manufacturing mode. Manufacturing engineering and technology is becoming the focus of research and application of all fields[12]. However, there is also competition between enterprises, so the problem how to protect itself is the thing that every enterprise are caring about. They wonder whether the commercial secret might be leak under the premise of cooperation in a distributed design. So secure multi-party computation is very necessary. Therefore, how to design meters high efficiently, and safe secure multi-party computation protocol is a challenging wars. The cryptography is one of the important research task.Goldreich put forward general agreement for a solution plan. The secure multi-party meter is a problem in some special cases. Some special problem needs to use some special methods to achieve high efficiency. The thought was promoted that the rapid secure multi-party computation should be researched in some special fields in recent years. Many scholars have brought secure multi-party computation technology into the traditional data mining, computational geometry, private information retrieval cable, statistical analysis and other fields, which results in some new research directions, such as privacy protection in data mining, privacy of computational geometry, private letter information retrieval, privacy of the statistical analysis and so on.

With industrial development and the globalization of information technology, mechanical manufacturing competition is become more and more intense, many professional designs and major marketed produces have changed in the field of mechanical engineering, such as different product manufacturing and design regions. We could use the advanced technology to complete mechanical engineering research, which has become the research focus in the field. Assume mechanical engineering characteristic A can be divided into r class, i=1,2,……, characteristic B can be divided into c class, n_{ij} is the individual, which has characteristics of A, B , i=1,…,r； j=1,2,…,cither group statistic results of mechanical engineering properties are shown below.

Table 1: R X C Contingency Table

		mechanical characteristic A						total
		A1	*A2*	……	*Aj*	……	*Ac*	
Characteristic B	B1	*n11*	*n12*	……	*n1j*	……	*n1c*	n1.
	B2	*n21*	*n22*	……	*n2j*	……	*n2c*	n2.
	…	……	……	……	……	……	……	……
	Br	*nr1*	*nr2*	……	*nrj*	……	*nrc*	nr.
total		*n.1*	*n.2*	……	*n.j*	……	*n.c*	n

In Table 1,we use p_{ij} to describe the union probability of B_i and A_j , the marginal distribution probability of mechanical properties A classification, namely, one dimensional multiple probability distribution is expressed as p_j , and the marginal distribution stands for probability of mechanical properties of B classification, namely, one dimensional multiple probability distribution is expressed as p_i .Then the several probability distribution table of mechanical engineering is just as follow.

Table 2 : Many Probability Distribution

		mechanical characteristic A						total
		A1	A2	……	Aj	……	Ac	
Characteristic B	B1	*P11*	*P12*	……	*P1j*	……	*P1c*	*P1.*
	B2	*P21*	*P22*	……	*P2j*	……	*P2c*	*P2.*
	…	……	……	……	……	……	……	……
	Br	*Pr1*	*Pr2*	……	*Prj*	……	*Prc*	*Pr.*
total		*P.1*	*P.2*	……	*P.j*	……	*P.c*	*1*

If the mechanical engineering characteristic A and characteristic B have no relevance, then we assume that two classification A and B is not independent with each other, so we can make the null hypothesis:

$$\text{H0}: \; p_{ij} = p_i \cdot p_j \qquad (4)$$

In formula (4),the two classification is independent of each other in mechanical engineering. At this time, we can prove that n value depends on $E(n_{ij})$ > 5.We can get the statistics according to Pearson theorem[13]:

$$\chi^2 = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{\left[n_{ij} - E(n_{ij})\right]^2}{E(n_{ij})} \sim \chi^2[(r-1)(c-1)] \qquad (5)$$

In formula (5),the expected frequency mechanical engineering is[14]:

$$E\left(n_{ij}\right) = np \qquad (6)$$

And when H0 is founded by the formula:

$$E(n_{ij}) = np_{ij} = np_{i.}p_{.j} \qquad (7)$$

For formula (6) and (7) are unknown, we usually use estimate $\hat{p}_i = n_i / n, \hat{p}_j = n_j / n$ to replace it. So the expected frequency of characteristic theory is as follows:

$$\hat{E}\left(n_{ij}\right) = n_i.n_j / n \qquad (8)$$

It is generally a mechanical engineering enterprise to complete the project cooperation, then compose an enterprise associated with material supplier, material vendors, the related design unit or person in charge of the project design. Choosing these partners are based on their expertise, competition ability and business reputation, etc. Given significance level is under the following conditions:

when $\chi^2 > \chi^2_\alpha[(r-1)(c-1)]$,it refuses H_0 , attributing A, B is not independent, there exists relationship;

when $\chi^2 \le \chi^2_\alpha[(a-1)(b-1)]$, it accepts H_0 , attributing A, B is independent, there is no relevant.

So the mechanical enterprise mainly depends on the correlation analysis of its characteristics while combined engineering manufacturing technology is always ready to improve employees' comprehensive quality, to train employees' unity consciousness, to enhance staff team cohesion with participating dynamic, implement enterprise network cooperation and strategic inheritance. Thus, to form rapid network integration and to incent manufacturing system of secure multi-party computation market to become more social. Namely, in the mechanical field, with such fierce competition today, how to do the secure computation well is the key thought of each enterprise, secure multi-party computation in engineering application is the urgent need of the field of mechanical engineering.

Thus, the possibility of machine failure is accounted the vast majority in the unbalanced fault case. In the possibility of machine failure, the unbalanced fault case is accounted by the vast majority, and the rotor bar breaking is caused by machine fault case that is only a very small part. The machine is not the probability of failure so that it is relatively small because the machine works, whose bearing will wear out. At the same time, the occurring inter-turn short circuit also can hardly be avoided. The activation rate of two indicators is 100%. Therefore, the machine warranty terms should be emphasized on the maintenance and protection.

4. THE ADVANTAGE ANALYSIS OF MANUFACTURING TRAINING APPLICATION OF SECURITY MULTI-PARTY COMPUTATION

In the rapid development of the economic globalization today, mechanical engineering should not only focus on mechanical manufacturing technology, but also pay more attention to the whole manufacturing training. The pursuit of high and new technology mechanical engineering is too utilitarian, which results in that mechanical manufacturing training is left out in the cold days, ignored by people for it is even thought no need. But the actual practice manufacturing training has a very important position in the field of mechanical engineering. Not only the training mode and method is colorful, the training mode is also a organic integration to be variety of college training means. As in the practical training, the training methods of the data conversion for mother series can be recorded as {X0 (t)}, the son series can be recorded as {Xi (t)}.In the time t = k ,mother sequence{X0 (k)} and son sequence {Xi (k)}of the correlation coefficient L0i (k) can be calculated by the formula:

$$L_{oi}\left(k\right)=\frac{\Delta_{\min}+\rho\Delta_{\max}}{\Delta_{oi}\left(k\right)+\rho\Delta_{\max}} \qquad (9)$$

In formula (9), Δ0i (k) is for the absolute difference of two training method by comparison sequence in the k time. Namely,Δ0i (k)=│x0 (k)–xi (k)│ (1 ≤ i ≤ m); $\Delta_{\max}$ and $\Delta_{\min}$ are respectively expressed for the time sequence maximum and minimum value in the process of the mechanical manufacturing training. The application of security multi-party computation will make all implementation produce of training plan become a real-time interactive behavior, so as to avoid the behavior data leaking with the condition $\Delta_{\min}=0$;And ρ is for resolution factor, whose main function is effective to reduce the largest absolute difference caused by the numerical big manufacturing training distortion. So the application of security multi-party computation can effectively improve the correlation coefficient, such as ρ∈(0, 1).And its value is usually from 0.1to 0.5.

The application of security multi-party computation in manufacturing training apply can reflect the training mode and training process data and compare sequence correlation degree in each time through the correlation coefficients, so as to analyze the secure performance of secure multi-party computation. As in the moments Δmin, Leo = 1, and in the moments Δmax, the correlation coefficient is the minimum value. Therefore, the range of correlation coefficient is 0 < L ≤ 1. Namely, the application of manufacturing training security has an obvious advantages of multi-party computation.

5. CONCLUSION

Secure muhi-party computation plays an important role in information security under the circumstance of network cooperation. The paper firstly introduced the basic concept of SMC and related knowledge of cryptology. Then we illustrated its application in electronic vote, electronic signature and threshold signature. A new application direction in mechanical engineering design was introduced, such as product designing and manufacturing in other places, flexible and virtual manufacture techniques and so on. Finally, some worth-researching hot questions about cooperative SMC on the condition of privacy protection are presented. Effective and reasonable use of secure multi-party computation is focused on in that internet cooperation project was increasingly developed, taking the following aspects for examples: early securing degree of key management, electronic voting, electronic auction, database access, data mining, hacker intrusion detection, high efficiency statistics, scientific analysis, confidential management and so on. It has a very wide range of applications. In future, we should constantly review various attack practices in solving difficulties, thus further let secure multi-party computation can be widely deepened and developed.

ACKNOWLEDGMENTS

This work was supported by the Twelfth-Five-Year Planning Issues of Science Education in Heber Province with the project name 1250182 and the project name The Empirical Research on the Convergence of Universities' Occupation Training and Labor Market in Heber Province. I would like to express my appreciation to all the people who have given some advices to us.

REFERENCES:

[1] Q. Li, H. Yan, K. Chen, “Secure multi-party computation protocol research and application”, *Computer science*, Vol.5, No. 9, 2012, pp. 56-61.

[2] Ch. Yu , F. Min, W. Zhu , “Relationship between Covering-based Rough Sets and Free Mastoids”, *Advances in Information Sciences and Service Sciences*, Vol. 4, No. 12, 2012, pp. 193-200.

[3] X. Feng, “Analysis of Field of Stress and Displacement in Process of Meshing Gears”, *International Journal of Digital Content Technology and its Applications*, Vol. 5, No. 6, 2011, pp. 345-357.

[4] I. Damgard, M. Jurik, Efficient protocols based on probabilistic encryption using composite degree residue classes, Proceedings of International Conference on Green Power, Materials and Manufacturing Technology and Applications, Trans Tech Publications, July 17-19, 2012, pp. 1355-1364.

[5] M. Hirt,U. Maurer, Complete characterization of adversaries tolerable in secure multi-party computation, Proceedings of the 16th ACMSymposium on Principles of Distributed Computing, IEEE Conference Publishing Services, August 15-17, 2007, pp. 125-134.

[6] S. Fehr, U. Maurer, “Linear VSS and distributed commitment schemes based on secret sharing and pairwise checks”, *Lecture Notes in Computer Science*, Vol. 10, No.2, 2010, pp. 565-580.

[7] C. Crepeau, J. Kilian, “Discreet solitary games”, *Lecture Notes in Computer Science*, Vol. 773, No.8, 2009, pp. 319-330.

[8] V. Niemi, A. Renvall, “How to prevent buying of votes in computer elections”, *Lecture Notes in Computer Scienc*e, Vol. 917, No.5, 2010, pp. 164-170.

[9] H. Nurmi, A. Salomaa, L. Santean, “Secret ballot elections in computer networks”, *Comput. Security*, Vol. 5, No. 3, 2011, pp.553-560.

[10] Wang, S. H., Melendez, S. and Tsai, C. S., “Applications of parametric sketching and Associability in 3D CAD”, *Computer Aided Design and Applications*, Vol. 5, No. 6, 2011, pp. 822-830.

[11] Sung, W. T., Ou, S. C., “Web-based learning in the Computer Aided Design curriculum”, *Journal of Computer Assisted Learning*, Vol. 18, No. 2, pp. 187-195. 175-187.

[12] Sorka Bizon, M., Geometry and Engineering graphics in engineering education illustrated by example of advanced 3D modeling course, Proceedings of International Conference on Engineering Education, July 3-7, 2010, pp. 1425-1432.

[13] H. Li, S. Wang, “About the division of the secure computation protocol”, *Computer engineering and application*, Vol. 5, No. 7, 2010, pp. 15-17.

[14] J.Zhang, S. LiuandK. Kim, “Based on Round An then tieated Tripartite Key Agreement with Pairing”, Proceedings of International Information Theory, IEEE Conference Publishing Services, September 9-12, 2011, pp. 3268-3276.