Publicly Verifiable Rational Secret Sharing

[1]Cai Yongquan, [2]Luo Zhanhai, [3]Yang Yi
College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China, cyq@bjut.edu.cn
College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China, siyueheliu@163.com
College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China, chelsealove@126.com

Abstract

In this paper we mainly focus on the cheating problem between secret dealer and players as well as players themselves in Maleka's scheme. Based on the existing scheme, we adopt non-interactive zero knowledge protocol to provide proof so that any arbitrary player who use published data and constructed proof can verify the sub-secret share during distribution phase and more significantly, reconstruction phase. Our scheme remarkably resolve the cheating issue in rational secret sharing with a prominent improvement on safety, generality along with execution efficiency.

Key words: *secret sharing; rational; zero knowledge proof; verify*

1. Introduction

As an important branch of the modern cryptography, secret sharing technology has many implementations in many application area of secret key management. With the continuous development of secret sharing, secret sharing becomes the basic design of many security modules and protocols. In 1979, Shamir proposed the first scheme using LaGrange interpolation [1]. After then, considerable amount of efforts have been dedicated into this field thus inspiring lots of classical secret sharing schemes, such as the visual secret sharing for binary image [2] and the secret sharing with general access structures [3]. First combining the knowledge of Game Theory with secret sharing, Halpern and Teague raised the concept of rational player [4] leading the rational secret sharing as the research focus of the area. In rational secret sharing, rational participants decide whether to cooperate or not strictly depending on his payoff of the protocol. In this situation, the previous secret sharing scheme could not be applied appropriately; therefore the secret sharing scheme based on rational participant is indispensable. In Gordon-Katz's scheme [5], they choose a random parameter β to achieve the purpose of uncertainty of sub-secret distributed by the dealer. If achieving the Nash equilibrium is possible under certain circumstance, any rational participants will not deviate from the protocol. Abraham proposed a rational secret sharing scheme with the feature of anti-collusion [6]. This scheme randomly processes the polynomial, and distributes the secret with the probability of α. They claimed if α is reasonably chosen, it will meet the Nash equilibrium against collusion attack up to k participants. In 2008, Maleka proposed a deterministic protocol for rational secret sharing scheme based on the knowledge of game theory [7]. The scheme constructs the sub-secret by choosing different depth of the sub-polynomial so that participants are not aware of the end of the game thus follow the protocol in accordance with the requirements. However, the scheme is not capable of dealing with the fraud problem between the dealer and the participants, the security level needs to be improved [8]. Soon afterwards, based on the theory of repeated games, Maleka proposed a new rational secret sharing scheme that resolves the above problem [9]. In 2009, Micali and Schelat proposed a purely rational secret sharing based on the pure strategy Nash equilibrium [10]. Fuchsbauer and Katz proposed a rational secret sharing scheme in standard communication networks; this scheme has a great improvement in the applicability [11]. In recent years, many research achievements in rational secret sharing raised by the study of the scholars, such as the references [12], [13], [14], [15] and [16]. In order to solve the cheating problem, in this paper, we combine non-interactive zero-knowledge proof protocol and theoretical knowledge such as discrete logarithm problem to improve Maleka's scheme

and proposed a publicly verifiable rational secret sharing scheme. What's more, the security and versatility have been greatly improved.

2. Related theory

In order to have a further understanding of the scheme, we introduce some related theory, such as discrete logarithm problem, Non-interactive zero-knowledge proof and Game Theory Model.

2.1 Discrete logarithm problem

As the security of foundation of many cryptographic protocols, the discrete logarithm problem has many applications in information security field, such as secret sharing scheme, secure digital signature and secure secret exchange protocol. Since the secure nature of the discrete logarithm problem, in many verifiable secret sharing schemes, it was been used for the verification of the sub-secret in distribution phase and reconstruction phase. Many cases have proved that the discrete logarithm problem has an effective improvement in the security of the secret sharing scheme. The discrete logarithm problem based on the finite cyclic group can be described as follows:

Given a large prime number p and a large prime number q, it meets that $q \mid p-1$. Select the generator g and the finite cyclic group z_p^*, select the element β in finite cyclic group z_p^*, for any algorithm A of random polynomial time, it is impossible to find an number x that meet the following equation $g^x \equiv \beta \bmod p$.

2.2 Non-interactive zero-knowledge proof $DLEQ(g_1, h_1, g_2, h_2, \alpha)$

Compare with the zero-knowledge proof, the non-interactive zero-knowledge proof has many advantages in execution efficiency and security. The number of times in interaction between the demonstrator and the verifier is at most once. In other words, it just need the demonstrator send a message to the verifier, then the demonstrator can make sure that it has the ability to solve a difficult problem for verifier.

In order to achieve the purpose of the minimum number of interactions, the demonstrator and the verifier were given the authority of access to a trusted third party with the nature of pre-determined and random. In the reality, the trusted third party is often a cryptographic hash function such as SHA, MD5.

Compared with the theoretical interactive zero-knowledge proof protocols, non-interactive zero-knowledge proof protocols have more practical significance. In reality, the widely used public-key cryptographic protocols and digital signature protocols can be viewed as the instance of the non-interactive zero-knowledge proof protocol.

The non-interactive zero-knowledge proof can be described as follows:

Select a large prime number, denote by p and a large prime number, denote by q, it meets $q \mid p-1$, Select = the finite cyclic group z_p^*, g_1, g_2 are the generators of the cyclic group z_p^*. $H()$ is a one-way hash function. $h_1 = g_1^{\alpha}, h_2 = g_2^{\alpha}$.

The demonstrator P select $w \in_R Z_p^*$, then computes the following equation:

$$b_1 = g_1^w \bmod p \quad (1)$$

$$b_2 = g_2^w \bmod p \quad (2)$$

$$c = H(b_1 \| b_2) \quad (3)$$

$$r = w - \alpha c \bmod p \quad (4)$$

The demonstrator P publish the data (r, c) as the proof of knowing α..

The verifier V verifies the equation $c = H(g_1^r h_1^c \| g_2^r h_2^c)$ to verify whether the demonstrator P knows α [17].

In our scheme, we used the improved non-interactive zero-knowledge proof to achieve the function of publicly verification in the distribution phase of the secret sharing scheme.

2.3 Game Theory Model

Game theory is an important branch in the applied mathematics. With the development of the game theory field, it has become a standard analytical tool in the field of economics. In recent years, based on the nature of the game theory, the game theory model has a wide application in the field of computer science and other related fields. The game theory model can resolve the problem of formulated interaction between the excitation structures. As a mathematical analytical tool and analytical method, it has been used in many security protocols which satisfy the nature of competitive.

In the game theory model, the most famous theory is the concept of the Nash equilibrium. In the field of economics, Nash equilibrium is the stable equilibrium value in the relevant strategies. In reality, the Nash equilibrium is a stable game result. Every player is in the situation that the equilibrium strategy is the best strategy for him when the other players do not change the corresponding Nash equilibrium strategies.

The classification of the game in game theory has many forms depending on different classification benchmarks. In general, based on the relation between the players, the game can be divider into cooperative game and non-cooperative game. In the cooperative game, the relation among the players has a binding agreement, in contrary, in the non-cooperative game, the relation among the players has no binding agreement.

In the field of secret sharing, the relation among the players is the instance of the excitation structures and competitive structures.

With the method of game theory model in our scheme, we can get the predictions of player's behavior and actual behavior in secret sharing scheme, thus we can deduce the most optimization strategy of the players. Thus, we can design the secure rational secret sharing scheme based on the game theory model and related theory.

The Nash equilibrium is defined as follows:

Let $\{A_i\}_{i=1}^n$ be the set of participants, $\{u_i\}_{i=1}^n$ is the payoff function of the participants in game model, $\Gamma = (\{A_i\}_{i=1}^n, \{u_i\}_{i=1}^n)$ be the normal form of the game, and $A = A_1 \times A_2 \times \ldots A_n$. If for all participant A_i and any random strategy $a_i' \in A_i$, there is a tuple $a = (a_1, a_2, \ldots a_n) \in A$ that satisfies the inequality $u_i(a_i', a_{-i}) \le u_i(a)$, then that is a pure Nash equilibrium [18].

Assume info (r) is a n-tuple $(s_0, \ldots s_n)$, if the participant i gets the secret, then $s_i = 1$. $u(r)$ is the payoff of the participants. The follow assumptions are:

U1: if info (r) =info (r'), then $u_i(r) = u_i(r')$

U2: if info $_i(r)$ =1, info $_i(r')$ =0, then $u_i(r) > u_i(r')$

U3: if info $_i(r)$ = info $_i(r')$, info $_j(r) \le$ info $_j(r')$, $j \ne i$, and that exits info $_j(r)$ <info $_j(r')$,then $u_i(r) > u_i(r')$.

If the payoff function of the participants satisfy U1-U3, then in a game where all the participants are not aware of the end of the game, there exists a Nash Equilibrium $\{\Gamma, \sigma_*\}$ that of practical meaning which will realize rational secret sharing in finite time span.

We define the income U_i^+ is the income of participant A_i when A_i get the secret and deviate from the Nash equilibrium, the probability is β. U_i^- is the income of participant A_i when A_i did not get the secret and deviate from the Nash equilibrium ,the probability is $1-\beta$. U_i is the expect income of participant A_i when A_i followed the Nash equilibrium. The mixted Nash equilibrium is defined as follows:

$$\beta \times U_i^+(\sigma_i', \sigma_{-i}) + (1-\beta) \times U_i^-(\sigma_i', \sigma_{-i}) < U_i(\sigma_i, \sigma_{-i}) \tag{5}$$

3. Introduction of Maleka's Scheme

For n participants, the dealer first randomly selects a polynomial F with the depth of m-1.

Compute $s_1.....s_n$ according with the polynomial F, construct polynomials $f_1.....f_n$ with the depth of d_i for every secret $s_1.....s_n$, $|d_i - d_j| \le 1, i \ne j$. For every secret s_i, the dealer computes $\{f_i(1).....f_i(d_i)\}$, and sends the message to participant i as the sharing secret. To get the secret S, everyone needs at least $m-1$ secrets. Thus, everyone needs to cooperate with other participants to get the secret.

The protocol of the dealer:

(1) Randomly select a polynomial $F(x)$ with the depth of m-1, S= $F(0)$, compute the sub share $\{s_1.....s_n\}$.

(2) Construct polynomial $f_1.....f_n$ for the depth of d_i, $|d_i - d_j| \le 1$, $i \ne j$.

(3) Compute the sub secret $\{s_{i1}, ...s_{id_i}\}$ according to f_i, and send the message to participant P_i $(1 \le i \le n)$.

The protocol of the participant:

(1) In the first round, the participant P_i sends s_{i1} to other m-1 participants.

(2) If in the r-1 round, the participant P_i received sub secret form other m-1 participants, then in the r round (except the first round) send the sub secret s_{ir}.

(3) Reconstruct the sub share $\{s_1.....s_n\}$ and the secret S.

4. Publicly Verifiable Rational Secret Sharing Scheme

4.1 Initialization phase

Select large prime number p, q, and $q \mid p-1$, G_q is a cyclic group with the order of q, g_1, g_2 are generators of G_q, $\log_{g_1} g_2$ is unknown. Select a hash function H. Assume the participants set is $\{P_1, P_2, ...P_n\}$, and select $x_i \in Z_q^*$ for these n participants, public the data $y_i = g_2^{x_i}$.

4.2. Distribution phase

Step1: The dealer chooses $S \in Z_q$ as the secret to be shared. Select random polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + ...a_{m-1} x^{m-1}$ with the depth of m-1 and needs $S = f(0)$. Compute the following equation:

$$S_i = f(i), i = 1, 2, . \tag{6}$$

$$C_j = g_1^{a_j} \bmod p, j = 0,1,2,.....m-1 \tag{7}$$

$$Y_i = y_i^{f(i)} \bmod p, i = 1,2,.....n \tag{8}$$

$$X_i = g_1^{f(i)} \bmod p \tag{9}$$

Publishes the data C_j, Y_i

Construct the proof with zero-knowledge as follows:

Select $w_i \in_R Z_q^*, i = 1,2,.....n$ randomly

Compute the following equation:

$$E_{1i} = g_1^{w_i} \bmod p \tag{10}$$

$$E_{2i} = y_i^{w_i} \bmod p \tag{11}$$

$$c = H(g_1 \| y_1 \| ..... \| y_n \| X_1 \| ..... \| X_n \| ...\} \| Y_1 \| .....Y_n \| E_{11} \| ... \| E_{1n} \| E_{21} \| ... \| E_{2n}) \tag{12}$$

$$r_i = w_i - c \times f(i) (\mathrm{mod}\, q) \tag{13}$$

The dealer published the data $proof = (c, r_1, r_2, ...r_n)$.

Step2: Select random polynomial $f_i = a_{i0} + a_{i1}x + a_{i2}x^2 + ...a_{id_i}{}^{d_i} (1 \le i \le n)$ with depth of d_i , $S_1 = f_i(0)$, $|d_i - d_j| \le 1, i \ne j$.

Step3: Compute the sub secret of the S_i as follows:

$$S_{ik} = f_i(k), k = 1, 2, ...d_i, i = 1, 2, ...n \tag{14}$$

Send $S_{i1}, S_{i2}, ...S_{ik}$ to participant P_i .

4.3 Distribution phase

After getting the sub-secret $S_{i1}, S_{i2}, ...S_{ik}$, the participants construct the secret S_i with the method of Lagrange interpolation. Use the follow equation to verify authenticity of the sub share.

Participant P_i compute the following equation:

$$Q_i = \prod_{j=0}^{m-1} C_j{}^{i^j} (\mathrm{mod}\ p) \tag{15}$$

Verify the correctness of the following equations:

$$E_{1i} = g_1{}^{r_i} Q_i{}^c \bmod p \tag{16}$$

$$E_{2i} = y_i{}^{r_i} Y_i{}^c \bmod p \tag{17}$$

$$g_1{}^{S_i} = Q_i \bmod p \tag{18}$$

If the above equations are validity then the sub share S_i is correct. Thus it can verify whether the dealer is cheating. If not, implement the following protocol. Otherwise, the sub share S_i is not correct; all participants stop and exit the protocol.

Step1: In the first round, participant P_i sends the first message S_{i1} to other participants.

Step2: In the r-1 round, If the participants received the sub secret. Then in r round, send the rth secret .

Step3: Repeat the interaction protocol, until get the all sub secret or a compulsory end of the protocol.

At the same time, each participant can verify the correctness of other's sub share using equation $g_1{}^{S_j} = \sum_{i=0}^{n} C_i{}^{j^i} \bmod p$. If correct, reconstruct the secret S with the method of Lagrange interpolation.

5. Analysis of Our Scheme

5.1 Nature of equilibrium

This scheme is an improvement scheme of the Maleka's scheme. The interactive process is equivalent to the stages of repeated games in game theory. Since the depth d_i of polynomial is selected randomly, the participants are not aware of the number of the others' sub secret. Thus participant will send sub secret to other participants. The participant can reconstruct the secret S. $\sigma=(\sigma_i , \sigma_{-i})$ is the strategy of implementing the protocol, $\sigma'=(\sigma_{i'} , \sigma_{-i})$ is the strategy of deviating from the protocol. Based on Nash equilibrium theory, $u_i (\sigma_i , \sigma_{-i}) > u_i (\sigma_{i'} , \sigma_{-i})$, then the rational

participant will follow the protocol according to the payoff function. Compared with Halpern, Gordon Katz, Abraham, this scheme can choose select distribution function of random variable flexibly. It has an improvement in versatility and safety.

5.2 Nature of anti-cheating

This scheme use non-interactive zero-knowledge proof protocol to complete the verification of the secret distribution. It is based on the discrete logarithm problem. Given the group G, the order p, the generator g, and $g^{\alpha} \bmod p$. It is difficult to compute α in random polynomial time. So it is no feasible for the cheater to forge $g_1^{r_i} Q_i^{c}$ and $y_i^{r_i} Y_i^{c}$, and the attack can not get the secret share by the published data. So it can effectively prevent the fraud problem between the dealer and the participants, and also prevent the fraud problem among the players. In our scheme, the players can verify the correctness of the secret share with the equation $E_{1i} = g_1^{r_i} Q_i^{c} \bmod p$. Due to C_j is published to all players. So if dealer cheated, it simply tricks the all participants, which is meaningless. This verification resolved the conspiracy problem between the dealer and the other participants. With the published data and equation $E_{2i} = y_i Y_i^{c} \bmod p$, this scheme can verify the correctness of the sub share distributed by de dealer, successful resolves the exited cheating problem in the Maleka's scheme.

5.3 Advantages of our scheme

Through the analysis of our scheme and the exited classical rational schemes , we get the result in versatility, security, execution time and other aspects of our scheme and exited classical rational secret sharing schemes. The following table 1 shows the comparison among our scheme and other schemes. From the following Table 1, we can see that our scheme has a larger application range than other former schemes in versatility.

Table 1. Comparison

scheme	Versatility	security	Synchronization Channel	Execution time	Random number selected
Halpern-Teague	T≥3，n>3	general	yes	$O(5/\alpha^3)$	$\frac{1}{4}u_i(\sigma_i',\sigma_{-i})+\frac{3}{4}$ *0< $u_i(\sigma_i,\sigma_{-i})$
Gordon-Katz	t≥2，n>2	general	yes	O(1/β)	$\frac{1}{4}u_i(\sigma_i',\sigma_{-i})+\frac{3}{4}$ *0< $u_i(\sigma_i,\sigma_{-i})$
Abraham	t≥2，n>2	general	no	O(1/α)	$\alpha \le \min_{i\in n} \frac{u_i(N)-u_i(\phi)}{m^i-u_i(\phi)}$
our scheme	t≥2，n>2	higher	yes	$O(n^2)$	random

In the aspect of security, by using the non-interactive zero-knowledge proof in the distribution phase, our scheme has higher security level with a little expense of the execution time. In the aspect of the selection of the parameter, our scheme has a great flexibility compared with the exited rational secret sharing scheme because we have no limitations strained on the probability.

It's easy to tell that our scheme has many improvements considering the time and space efficiency. Besides our scheme works in the frame of public verification, that means players build the protocol on mutual detection of each other, they has more incentive to follow the protocol rather than deviate. With the public verification mechanism, our scheme has a more practical meaning if it's implemented in real use. Considering many restrains of other schemes, our scheme shows a great prospective in this field.

6. Conclusion

Our paper improves Maleka's scheme and resolves the existing problems. We proposed a publicly verifiable rational secret sharing scheme. For the sub-share s_i, select the polynomial f with the depth of d_i randomly so that the participants are not aware of the end of the game, so can successfully reconstruct the secret S. By using the non-interactive zero knowledge proof protocol and the intractability of the discrete logarithm problem, the scheme is an effective solution to the fraud problem between the dealer and the participants and participants can also verify the correctness of the other participant's sub share. This scheme is of simple, strong versatility, higher efficiency in implementation, and the security level has been greatly improved in comparison to other rational secret sharing schemes.

7. Acknowledgement

This work was supported by the Beijing Municipal Natural Science Foundation (Grant No. 1102003) and National Natural Science Foundation (Grant No.61170221). Thanks very much for the support of the Foundations, and thanks very much for the help of the professors in the process of this paper, without the support of them, we can not finish the scheme in this paper.

8. References

[1] Adi Shamir, "How to share a secret. Communications of the ACM", vol.22, no.11, pp.612-613, 1979.
[2] Thekra Abbas, Zou Beiji, "A Novel Non-Expansion Visual Secret Sharing Scheme For Binary Image ", Journal of JDCTA, vol.4, no. 6, pp.106-114, 2010.
[3] Yongxuan Sang, Jiwen Zeng, Zhongwen Li, Lin You, "A Secret Sharing Scheme with General Access Structures and its Applications", Journal of IJACT, vol.3, no.4, pp.121-128, 2011.
[4] Joseph Halpern, Vanessa Teague, "Rational secret sharing and multiparty computation extended abstract", Proc of 36t ACM Symposium on Theory of Computing (STOC), pp.623-632, 2004.
[5] S. Dov Gordon, Jonathan Katz, "Rational secret sharing, revisited", In 5th Intl. Conf. on Security and Cryptography for Networks (SCN), pp.229-241, 2006.
[6] Ittai Abraham, Danny Dolev, Rica Gonen, Joe Halpern, "Distributed computing meets game theory. Robust mechanisms for rational secret sharing and multiparty computation", Proc of 25th ACM PODC. Denver, pp.53-62, 2006.
[7] MALEKA S, Amjed SHAREEF, C. Pandu RANGAN, "The deterministic protocol for rational secret sharing ", Proc of IEEE International Symposium on Parallel and Distributed Processing(IPDPS 2008), Miami IEEE, pp.1-18, 2008.
[8] Jonathan Katz. "Bridging game theory and cryptography: Recent results and future directions". In 5th Theory of Cryptography Conference-TCC, pp.51-272, 2008.
[9] Shaik MALEKA, Amjed SHAREEF, C. Pandu RANGAN, "Rational secret sharing with repeated games", Proc of 4th Information Security Practice and Experience Conference (ISPEC 2008), pp. 334-346, 2008.
[10] Silvio Micali, Abhi Shelat, "Purely Rational Secret Sharing (Extended Abstract)", 6th Theory of Cryptography Conference, pp.54-71, 2009.
[11] Georg Fuchsbauer, Jonathan Katz, Eric Levieil, David Naccache, "Efficient rational secret sharing in standard communication networks", 7th Theory of Cryptography Conference, pp. 419-436, 2010.
[12] Yevgeniy Dodis, Shai Halevi, Tal Rabin, "A cryptographic solution to a game theoretic problem", 20th Annual International Cryptology Conference, pp.112-130, 2000.
[13] LI Da-wei，YANG Geng，Yu Chang-guo, "A Survey of Rational Secret Sharing schemes", Journal of Nanjing University of Posts and Telecommunications(Natural Science), vol.30, no.2, pp.89-94, 2010.
[14] Gilad Asharov, Yehuda Lindell, "Utility dependence in correct and fair rational secret sharing", JOURNAL OF CRYPTOLOGY, vol. 24, no. 1, pp.157-202, 2011.

[15] Amjed Shareef, “Brief Announcement: Collusion Free Protocol for Rational Secret Sharing”, 29th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, pp.402-403, 2010.
[16] Zhang E, Cai YQ, “A New Rational Secret Sharing Scheme”, CHINA COMMUNICATIONS, vol. 7, no. 4, pp.18-22, 2010.
[17] Berry Schoenmakers, “A simple publicly verifiable secret sharing scheme and its application to electronic voting”, Advances in Cryptology-CRYPTO'99, vol. 1666/1999, no. 784, pp.148-164, 1999.
[18] Yevgeniy DODIS, Tal RABIN, Algorithmic Game Theory, Cambridge University Press, UK, 2007.