International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.13-22
http://dx.doi.org/10.14257/ijsia.2015.9.11.02

Achieve Fairness in Rational Secret Sharing Protocol

Wang Jie

College of Mathematics and Computer Science,
Shanxi Normal University, Linfen 041004, China
wjlkt@163.com

Abstract

In the setting of (m,n) *rational secret sharing,* n *rational players wish to share a secret* s*, arbitrarily* m *players can reconstruct it, they always choose the strategies which can bring them more utilities. The security requirement includes privacy, correctness and fairness. Fairness is a central objective of the rational secret sharing scheme, complete fair means either all players get the secret* s *or none of them get it, but most existing schemes do not meet this nature. In this work, a rational secret sharing protocol is proposed, which neither need particular communication channel, nor assume the existence of honest minority, in addition, the scheme can resist the collusion attack with* $k(k<m)$ *players, and can achieve sequential equilibrium. Theoretical analysis shows that the proposed protocol is complete fair.*

Keywords*: rational secret sharing, assessment, sequential equilibrium*

1. Introduction

Secret sharing is an important building block of information security and modern cryptography. Shamir[1] proposed (m,n) secret sharing in 1979 for the first time, in a (m,n) threshold secret sharing scheme, the dealer shares a secret s among n players, and arbitrarily m players can reconstruct it. Traditionally player is assumed to be honest or malicious, honest players follow the protocol, and malicious players try their best to break the protocol. Actually, for some applications, some players may make rational choice for their benefit, if they will obtain more benefit when deviating from the protocol, they have no incentive to obey the protocol. This topic is first introduced by Halpern and Teague[2], they assumed that all players are rational, then they proved that traditional secret sharing protocols would fail, because rational players might refuse to offer their share or give out invalid shares after getting $m-1$ shares in the secret recovery phase, which cause only the malicious player can recover the correct secret, it is unfair for honest players. Since assumption of rational player is more realistic, rational secret sharing has attracted many scholars' attention in recent years, many protocols[3-7] were proposed, but most of them do not satisfy completely fairness, recently some researchers gave some positives results of fairness assume there exists minority honest players in the protocols, how to break the limitation and achieve fairness of the protocol is worthy to study.

1.1 Related Work

In 2004 Halpern and Teague[2] designed the first randomized rational secret sharing protocol, in the protocol all players are motivated to cooperate by control their profits, they suggested the notion of Nash equilibrium surviving iterated deletion of weakly dominated strategies as a standard for capturing the stability of a protocol. Kol and Naor[8] pointed out that many bad strategies could not be ruled out, so they gave the stronger notion of strict Nash equilibrium, in which every player's strategy was a strict

ISSN: 1738-9976 IJSIA

best response, players' utility would strict decrease when they chose to deviate, so players had no incentive to deviate. Fuchsbauer *et al.*[9] and Zhang *et al.*[10] induced $t-1$ -resilient computational strict Nash equilibrium but their protocols relied on cryptographic primitives for authentication, which may be broken after an exponential number of rounds, so their protocols were instability. Ong[11] gave a fair rational secret sharing protocol by considering the mixture of rational players and honest players, but it cannot resist the collusion attack of even two players. Based on the existence of honest players, William[12] designed an efficient protocol tolerating coalitions, which induces a strict Nash equilibrium. However, the assumption of honest players limits the realization of these protocols. Thus, Zhang and Liu[13] got rid of honest players using extensive games, but they can only achieve ε -Nash equilibrium, which cannot ensure the only best response and is weaker than strict Nash equilibrium. Most of these works care about the security of protocol, they don't care the fairness, but the fairness is important for secret sharing, so in this paper, we studied the fair reconstruction problem in rational secret sharing.

All above works are based on the assumption, (1) players want to learn secret, (2) players like fewer players learn it, which is proposed by Halpern and Teague[2], we call it standard assumption. We doubt whether this assumption suitable in every scene, so in this paper time is taken into consideration when players decide their utility.

1.2 Our Contribution

In this paper, we design a rational secret sharing protocol with fairness based on non-interactive publicly verifiable secret sharing, every broadcast message can be verified by others in public, which can eliminate the incredible threat, so the proposed protocol can achieve k -resilient sequential equilibrium. Compared to standard assumption in [2], we give a more practical utility assumption, players care about the time when they can learn the secret, which means if players haven't received message from a player in turn, then they deem he has abort the game, when players' utility is interrelated with time, we can punish the deviator get secret later than follower, so the proposed protocol is complete fair.

1.3 Paper Outline

The rest of this paper is organized as follows. In Section 2, we introduce some preliminaries. In Section 3, we present distribution protocol and reconstruction protocol for our fair rational secret sharing. In Section 4, we analyze the performance of proposed protocol. We present our conclusions in Section 5.

2. Preliminaries

2.1 Game Theory Model and Definition

In the rational secret sharing protocol, each player decides how to move based on all the received messages at each step, so we establish the model with extensive form game, assume all player care about the time when they get the secret, players' utility is interrelated with time, we define the utility for player p_i as follows:

- U^+ player p_i learns the secret earlier than others
- U all players learn secret at the same time
- U^- player p_i learns the secret later than others
- U^{--} all player get nothing

Definition 1. Extensive game with imperfect information $\langle N, H, P, f_c, (I_i), (u_i) \rangle$

(full version of this definition see in [14]).

- *N: the finite set of players*
- *H*: the set of histories. A history $(a^k)_{k=1,..,K} \in H$ is terminal iif it infinite or if there is no a^{K+1} such that $(a^k)_{k=1,..,K} \in H$ .The set of terminal histories is denoted Z
- H: the set of histories. A history $(a^k)_{k=1,..,K} \in H$ is terminal iif it infinite or if there is no a^{K+1} such that $(a^k)_{k=1,..,K} \in H$ .The set of terminal histories is denoted Z.
- P: function assigned to each non-terminal history (each member of $H \setminus Z$)a member of $N \bigcup \{c\}$.
- f_c :function that associates with every history h for which $P(h) = c$ a probability measure $f_c(.|h)$ on $A(h)$,where each such probability measure is independent of every other such measure.
- I_i :the information partition of player i . $I_i \in \mathrm{I}_i$ is an information set of player p_i .
- u_i :the utility function assign to each terminal history a value.

Definition 2. An assessment in an extensive game is a pair (β, μ) , where β is a profile of behavioral strategies, μ is a function that assigns to every information set a probability measure on the set of histories in the information set.

Definition 3. k-resilient sequential equilibrium Let $\Gamma =< N,\ H,\ P,\ f_c,(I_i),(u_i) >$ be a finite extensive game with perfect recall. An assessment (β, μ) is sequential equilibrium if for every player $i \in N$ and every information set $T \in \mathrm{I}_i$, it satisfies:

- **Sequential Rational** $U_i(\beta, \mu \mid I_i) \geq U_i((\beta_{-i}, \beta_{i'}), \mu \mid I_i)$, for every strategy $\beta_{i'}$ of player p_i
- **Consistent** There is a sequence $((\beta^n, \mu^n))_{n=1}^{\infty}$ of assessment that converges to (β, μ) in Euclidian space and has the properties that each strategy profile β^n is completely mixed and that each belief system μ^n is derived from β^n using Bayes' rule.

The biggest difference between Nash equilibrium and Sequential equilibrium is that Nash equilibrium only requires the strategy in decision node on equilibrium path is the best response. However, Sequential equilibrium requires that the equilibrium strategy not only in equilibrium but also in every decision node on non-equilibrium path is the best response, because strategy is a complete description of player's reaction function, and which can tell player how to move at every decision node.Before the formal definition of incredible threat, we give the definition of player's strategy.

Definition 4. A **strategy** of player p_i in an extensive game of imperfect information $< N, H, P, (I_i), (U_i) >$ is a function that assigns an action in $A(I_i)$ to each information set for I_i which $p(I_i) = i$.

If p_j proceeds ahead of p_i before the game, p_i will announce his strategy to p_j , then p_i can announce a threat strategy.

Definition 5. p_i's strategy s_i^* is an **incredible threat** if it satisfies

(i) $s^* = (s_i^*, s_{-i}^*)$ is a Nash equilibrium.

(ii) If p_j takes strategy $s_{j'} \neq s_j^*$, where $s_{-i'} \neq s_{-i}^*$, there exists a strategy $s_{i'} \neq s_i^*$ such that $U_i(s_i^*, s_{-i'}) < U_i(s_{i'}, s_{-i'})$

Above game theory concepts are from reference[15-17]。

2.2 Non-interactive Publicly Verifiable Secret Sharing

In the rational setting, rational players do not trust each other, they may send invalid shares in the reconstruction stage for more profits. Hence, we rely on public verifiable secret sharing to prevent players cheating. The non-interactive publicly verifiable secret sharing can be described as follows.

Step 1. Setup Phase

Select a group G of prime order q and a group G of prime order q, and generators α, β of G, then broadcasted the elements, player p_i generates a secret key $t_i \in Z_q^*$ and broadcasts $y_i = \beta^{t_i}$ as his public key.

Step 2. Distribution Phase

The dealer generates the polynomial $P(x) = a_0 + a_1 + \ldots + a_{m-1}x^{m-1}$ of degree at most $m-1$ over Z_q^* where $a_0 = s$ and $S = \beta^s$, makes public $\alpha_i = \alpha_{a_i} (0 \le i \le m-1)$, then broadcasts the encrypted shares $Y_i = y_i^{P(i)}$, for all $0 \le i \le n$. For demonstrate the correctness of the encrypted shares, the dealer shows a proof of knowledge of the value $P(i)$ such that $X_i = \alpha^{P(i)}$ and $Y_i = y_i^{P(i)}$, where $X_i = \prod_{j=0}^{m-1} \alpha_j^{i^j}$ for all $0 \le i \le n$; more exactly, the dealer broadcasts the concatenation of the non-interactive versions of $DLEQ(\alpha, X_i, y_i, Y_i)$ $(0 \le i \le n)$.

Step 3. Verification Phase

The prover selects $r \in Z_q^*$ and computes $\alpha_{r1} = \alpha^r$, then sends α_{r1}, α_{r2} to the verifier, the verifier selects c ($c \in Z_q^*$) and sends it to the prover, then prover computes $\delta = \gamma - c \cdot x \bmod q$ and sends δ to the verifier, the verifier checks if $\alpha_{r1} = \alpha^{\delta} X_i^c$ and $\alpha_{r2} = y_i^{\delta} Y_i^c$.

Step 4. Reconstruction Phase

The player P_i finds the share $I_i = \beta P(i)$ as $I_i = Y_i^{t_i^{-1}}$ using his private key, then the group A with $|A| = k$ can recover the secret s.

$$s = \prod_{i \in A} I_i^{\frac{j}{j-i}} \quad (1)$$

In our protocol, we let the demonstrator randomly choose it instead of generate by a formula.

3. Fair Rational Secret Sharing Protocol

We assume such channel in the protocol, if a player broadcast his message in his turn, then he is regarded as active, if he is not present in his turn, then he is regarded as abandon.

In order to eliminate "Incredible Threat", we only need punish the player who deviating from the protocol, so we let credible players get secret in the true iteration, but incredible players get it in the following iteration.

3.1 Initialization

Select a group G of prime order q and some generators α, β of G, then broadcasted the elements. P_i generates a secret key $t_i \in Z_q^*$ and broadcasts $y_i = \beta^{t_i}$ as his public key.

3.2 Distribution Phase

The dealer generates the polynomial $P(x) = a_0 + a_1 x + ... + a_{m-1} x^{m-1}$ of degree at most $m-1$ over Z_q^*, where $a_0 = s$, $S = \beta^s$. The dealer broadcasts $\alpha_i = \alpha_{a_i} (0 \le i \le m-1)$ and encrypted shares $Y_i = y_i^{P(i)} (0 \le i \le n)$.

3.3 Player's Protocol

3.3.1 Share Renewal: In this stage, we use the method of PVSS to check whether players are incredible in the random number generation.Players randomly select a number $r_i^{(t)}$ and distribute it to other players. If player P_a sends a consistent share of r_a, then he is incredible, and his r_a is abandon. Without loss of generality, we assume the former $l(n-l < m < l < n)$ players send their random number consistent. Player computes the share $s_i^{(t)} = s_i + \prod r_i$.

Step1. P_i selects a polynomial $P_i(x) = b_0 + b_1 x + ... + b_{m-1} x^{m-1}$ of degree $m-1$ over Z_q^*, where $r_i^{(t)} = b_0$, and broadcasts $\alpha_{ij} = \alpha^{b_i}$ for all $j \in [1, n]$.

Step2. P_i encrypts shares $Y_{ij} = y_j^{P_i(j)}$ for all $j \in [1, n]$.

Step3. P_i broadcasts the concatenation of the non-interactive version $DLEQ(\alpha, X_{ij}, y_j, Y_{ij})$, where $X_{ij} = \alpha^{P_i(j)}, Y_{ij} = y_j^{P_i(j)}$, if the result is false, then the player is a deviator.

Step4. P_i can display the received shares in the blowing matrix after other players distribute a random number.

$$\begin{pmatrix} \beta^{r_{11}^{(t)}} & \beta^{r_{12}^{(t)}} & \cdots & \beta^{r_{1n}^{(t)}} \\ \beta^{r_{21}^{(t)}} & \beta^{r_{22}^{(t)}} & \cdots & \beta^{r_{2n}^{(t)}} \\ \vdots & \vdots & \vdots & \vdots \\ \beta^{r_{n1}^{(t)}} & \beta^{r_{n2}^{(t)}} & \cdots & \beta^{r_{nn}^{(t)}} \end{pmatrix}$$

The $i-th$ row is the share of player P_i sending, and the $i-th$ column is the shares P_i receiving. If someone deviates, then all players give out his shares, since verification progress is publicly, we can easily know who is cheater.

Step5. P_i finds the share $S_i = \beta^{P(i)}$ as $S_i = Y_i^{t_i^{-1}} mod\ q$ using his private key. Then P_i computes $S_{i'} = \beta^{s_i} \cdot \Pi_{j \in A} \beta r_{ji} = \beta^{s_i + \sum_{j \in A} r_{ji}} = \beta^{s_{i'}}$, A is the set of players who follow the protocol.

3.3.2 Secret **Reconstruction:** Players send $S_i^{'}$ synchronously:

$$S^{'} = \prod_i S_i^{'\prod_{j \neq i} \frac{j}{j-i}} \tag{2}$$

In the reconstruction phase, the correctness of the share $S_i^{'}$ can be shown by adding a proof of the knowledge of the value t_i such that $y_i = \beta_{t_i}$ and $Y_i = S_i^{t_i}$.

3.3.3 Secret Verification: Since credible players send the received shares simultaneously, they can verify whether this iteration is true. P_i computes $y_j^{r_{ki}}$ where $j \in A, k \in [1, n]$, since everyone can check whether the received share is true by $DLEQ(\alpha, X_{ij}, y_j, Y_{ij})$, so it's easy to know who is cheater. If P_i is cheater, then he will be punished.

4. Protocol Analysis

4.1 Security Analysis

A (m, n) threshold secret sharing scheme must satisfy the rules, m or more than m players can recover the sharing secret, and $m-1$ or fewer players cannot recover the secret, cannot even get any information of the secret, which is a basic requirement of threshold scheme. In this protocol, players want to reconstruct the secret s, they must reconstruct the Lagrange interpolation polynomials $P(x)$ at first. By the nature of Lagrange interpolation polynomials, we know only more than m players cooperation can reconstruct polynomial $P(x)$ and recover secret s. Since our protocol is based on the assumption of discrete logarithm, player cannot get s from the public message, and may forge his shares by a negligible probability ε.

4.2 Player's Motivation Analysis

1. In Share Renewal phase
   Player will check if someone has aborted (assume x players):

- If $0 \leq x \leq m-1$, then he sends his messages.
- If $x \geq m$, then last iteration is true, then he learns the secret which he received in that iteration, and gives up this iteration also.

2. In Share Reconstruct phase

- Whenever P_i is supposed to move in share reconstruct phase, he always sends secret honestly.

3. In Share Verification phase

- If he is in the credible set, he sends his shares and can check if this iteration is true, if this iteration is true, he would not participant the next iteration.
- If he is in the incredible set, he sends secret honestly.

In this phase, the truth of the iteration is uncertain, players generate a random number in Z_{q^*} ,thus we can obtain that $\Pr[r_i^{(t)}] = \frac{1}{q}$. Then $\Pr[r^{(t)} = 0]$ will be a constant, denotes p . So players' belief μ on the information set is $(p, 1-p)$. So player has the motivation to obey the protocol.

4.3 Sequential Equilibrium *Analysis*

Proposition 1. Strong Discrete Logarithm Assumption: Assume q is a random prime, and g is the generator of Z_q^*, for any polynomial $Q(\cdot)$, and any probabilistic polynomial time (PPT) algorithm A, for all sufficiently large $k's$,

$$\Pr[A(q, g, g^x) = x] < Q(k) \quad (3)$$

Since our protocol is based on the assumption of discrete logarithm, player may forge his shares by a negligible probability ε . Then we can get:

Theorem 1. When $n - m < k < m(\beta, \mu)$ is completely fair in probability $(1-\varepsilon)$, then (β, μ) is completely fair in probability 1 $(p < 1 - \frac{(U^+ - U)}{(1-\varepsilon)(U - U^-)}, L > 1)$.

Proof . We assume that the coalition deviators can forge the shares with a negligible probability ε in the t iteration, then they broadcast the forge number. There will be two situation to discuss:

1. $k > n - m$, that is, the rest players have the correct shares no more than m. Even deviators abort the game, they would not get the right secret. So (β, μ) is completely fair in probability $(1-\varepsilon)$.
2. $k \le n - m$, in this situation players can reconstruct secret even deviator can forge their shares.

Theorem 2. When $k < m \le n - k$, for all $p < 1$, β is k-resilient sequential equilibrium, if the utility assumption satisfies $0 < (1-\varepsilon)(U - U^-) < U^+ - U$, and $p < 1 - \frac{U^+ - U}{(1-\varepsilon)(U - U^-)}, L > 1$, the assessment is a $k-$ resilient sequential equilibrium, where $n - k < m \le n$

Proof. First, we proof that the assessment (β, μ) is consistent. Assume I_i is an information set, and $|I_i| \ge 2$, that means players is uncertain at his action node. Since the uncertain of this game is whether this iteration is true, so we get $\lim_{n\to\infty} \mu^n = \mu = (p, 1-p)$. β is completely mixed. $\lim_{n\to\infty} (\beta^n, \mu^n) = (\beta, \mu)$ then (β, μ) is consistent.

Next, we proof (β, μ) is sequential rational. Because of Theorem 1, we only consider a one-deviation coalition players $C \subseteq N$, that means cheaters only misbehavior once,

and others follow the protocol always. Since our protocol is based on the Strong Discrete Logarithm Assumption, then we can assume coalition can solve it in a negligible probability ε.

If there is no player deviate, then all players' expect utility $U_E = b$, we can write it as form,

$$U_E = \sum_{l=1}^{\infty} p(1-p)^{l-1} b \tag{4}$$

When $n-k \geq m$, even the coalition deviate, players can reconstruct the secret. The utility of $P_i \in C$ is

$$\begin{aligned} U^{'} &= (1-\varepsilon)(pU^{+} + pU^{-}\sum_{l=1}^{L}(1-p)^{l}) + \varepsilon(pU^{+} + pU^{-}\sum_{l=1}^{L}(1-p)^{l}) \\ &= pU^{+} + (1-\varepsilon)pU^{-}\sum_{l=1}^{L}(1-p)^{l} + \varepsilon pU^{-}\sum_{l=1}^{L}(1-p)^{l} \end{aligned} \tag{5}$$

Since $U^{'} < U_E$, so players in coalition will not choose to deviate.

When $n-k < m$, the rest players cannot reconstruct secret without the cheater's correct secret, then the utility of $P_i \in C$ is:

$$\begin{aligned} U^{'} &= (1-\varepsilon)(pU^{+} + pU^{-}\sum_{l=1}^{L}(1-p)^{l}) + \varepsilon(pU^{+} + pU^{-}\sum_{l=1}^{L}(1-p)^{l}) \\ &= pU^{+} + (1-\varepsilon)pU^{-}\sum_{l=1}^{L}(1-p)^{l} + \varepsilon pU^{-}\sum_{l=1}^{L}(1-p)^{l} \end{aligned} \tag{6}$$

Denote $A = p\sum_{l=1}^{L}(1-p)^{l} = (1-p)(1-(1-p)^{L})$, and make $U^{'} < U_E$, then the equation will be:

$$\begin{aligned} & U^{'} = pU^{+} + (1-\varepsilon)U^{-}A + \varepsilon UA < pU + UA \\ & \Leftrightarrow p(U^{+} - U) < A(U - \varepsilon U - (1-\varepsilon)U^{-}) \\ & \Leftrightarrow \frac{p}{A} < \frac{U - \varepsilon U - (1-\varepsilon)U^{-}}{U^{+} - U} \end{aligned} \tag{7}$$

Since $1-p \in [0,1]$, $(1-p)^{l} < 1-p$, when $L > 1$, $\frac{p}{A} < |1-p| < \frac{(1-\varepsilon)(U-U^{-})}{U^{+}-U}$. If the utility assumption satisfies $0 < (1-\varepsilon)(U-U^{-}) < U^{+}-U$, and

$p < 1 - \frac{(U^{+}-U)}{(1-\varepsilon)(U-U^{-})}$, $L > 1$, the assessment is a sequential equilibrium.

5. Conclusion

In this paper, we have studied the fair reconstruction problem when players are rational. Different from before protocols, we modify standard assumption and give a new utility assumption according to time, which leads to a more precise result. At first, we offer the extensive game model for secret sharing, introduce the public verification secret sharing to detect cheaters in each round, then present specific steps of the protocol, at last we analyze the security, players' motivation and the sequential equilibrium, the results show that our protocol guarantees complete fairness compared with others.

Acknowledgements

This work is supported by National Natural Science Foundation(Grant No.61170221). We are indebted to the anonymous reviewers for their numerous useful comments and suggestions. We would like to thank them for their kind efforts to help us improve our work.

References

[1] A. Shamir. "How to share a secret. Communications of the ACM", vol. 22, no. 1, (**1979)**, pp. 612-613 .
[2] J. Halpern, "Teague V. Rational Secret Sharing and Multiparty Computation", "Proceedings of the 36th Annual ACM Symposium on Theory of Computing",(STOC), New York: ACM Press, **(2004)**, pp. 623-632.
[3] I. Abraham , D. Dolev, R Gonen, J Halpern, "Distributed computing meets game theory: robust mechanisms of rational secret sharing and multi-party computation", In Proc 25th ACM symposium on principles of distributed computing (PODC), **(2006),** pp. 53-62.
[4] D. Gordon , J. Kat , "Rational secret sharing, revisited", "Security and Cryptography for Networks", **(2006)**, pp. 229-241.
[5] A. Lysyanskaya, "Triandopoulos N. Rationality and adversarial behavior in multiparty Computation", In CRYPTO2006, LNCS 4117, **(2006)**, pp. 180-197.
[6] Y. Dodis, T. Rabin. "Cryptography and game theory", "Algorithmic Game Theory", Cambridge University Press, **(2007)**, pp.181-207.
[7] S . Maleka, A. Shareef, C. P. Rangan." Rational secret sharing with repeated games", In 4th Information Security Practice and Experience conference, LNCS, 4991, **(2008)**, pp. 334-346.
[8] G .Kol, M . Naor. "Games for exchanging information", The 40th Annual ACM Symposium on Theory of Computing(STOC), New York: ACM Press, **(2008)**, pp. 423-432.
[9] G . Fuchsbauer, J. Katz, D. Naccache. "Efficient Rational secret sharing in standard communication network",. The 7th Theory of Cryptography Conference(TCC), LNCS 5978, (**2010)**, pp. 419-436.
[10] F . Zhang Z, M L Liu, "Unconditionally secure rational secret sharing in standard communication network. Information Security and Cryptology"-ICISC2010, Heidelberg: Springer, **(2011)**, pp. 355-369.
[11] S J Ong, D V Parkes, A Rosen. "Fairness with an honest Minority and a rational majority", The 6th Theory of Cryptography Conference(TCC) , LNCS 5444, **(2009)**, pp. 36-53.
[12] K. William.Mses J, and C P Rangan, "Secret sharing with honest players over an asynchronous channel.", "Advances in Network Security and Applications Communications in Computer and Information Science",vol. 196, no. 1, **(2011)**, pp. 414-426.
[13] Z. Zhang F, M L Liu."Rational secret sharing as extensive games". Science China Information Sciences, no. 42, **(2012)**, pp.32-46
[14] M J Osborne, A. Rubinstein, "A Course in Game Theory. MIT Press", Cambridge University Press, **(1994)** pp. 107-163.
[15] J. Katz . "Bridging game theory and cryptography: Recent results and future directions. In 5th Theory of Cryptography Conference (TCC 2008), LNCS4984, **(2008)**, pp. 251-272.
[16] M J Osborne,"An Introduction to Game Theory". Oxford University Press, **(2004)**, pp. 121-160
[17] Y. Dodis, T. Rabin , "Cryptography and game theory. Algorithmic Game Theory", Cambridge University Press, (**2007)**, pp. 181-207.
[18] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting", Advances in Cryptology-CRYPTO'99, no. 784, (**1999),** pp. 148-164.

Author

Jie Wang, she is an Associate Professor in Shanxi Normal University. Her current research interests include rational secret sharing and rational multiparty computation.