SCIENCE CHINA
Information Sciences

• **RESEARCH PAPER** •

May 2015, Vol. 58 052109:1–052109:13
doi: 10.1007/s11432-014-5275-5

Bayesian mechanism for rational secret sharing scheme

TIAN YouLiang[1,2,3], PENG ChangGen[2*], LIN DongDai[1], MA JianFeng[3], JIANG Qi[3] & JI WenJiang[3]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*College of Science, Guizhou University, Guiyang* 550025*, China;*
[3]*School of Computer Science and Technology, Xidian University, Xi'an* 710071*, China*

Received September 5, 2014; accepted October 28, 2014; published online January 9, 2015

Abstract We consider the cooperation of rational parties in secret sharing. We present a new methodology for rational secret sharing both in two-party and multi-party settings based on Bayesian game. Our approach can resolve the impossible solutions to a rational secret sharing model. First, we analyze the 2-out-of-2 rational secret sharing using Bayesian game, which makes us able to consider different classes of the protocol player (for "good" and "bad" players) and model attributes such as any other parties' preferences and beliefs that may affect the outcome of the game. Thus, the new model makes us able to reason rational secret sharing from the perspective of Bayesian rationality, a notion that may be in some scenarios more appropriate than that defined as per pure rational. According to these analyses, we propose a Bayesian rational protocol of 2-out-of-2 secret sharing. Also, our techniques can be extended to the case of t-out-of-n Bayesian rational secret sharing easily. Our protocol is adopted only by the parties in their decision-making according to beliefs and Bayes rule, without requiring simultaneous channels and can be run over asynchronous networks.

Keywords rational secret sharing, game theory, Bayesian game, perfect Bayesian equilibrium, Bayesian rationality

Citation Tian Y L, Peng C G, Lin D D, et al. Bayesian mechanism for rational secret sharing scheme. Sci China Inf Sci, 2015, 58: 052109(13), doi: 10.1007/s11432-014-5275-5

1 Introduction

The well-known t-out-of-n secret sharing problem which was studied by Blakey [1] and Shamir [2] in 1979 independently is that a dealer who holds a secret distributes shares among n players such that any group of size larger than t can recover the secret from their shares, while any group of size smaller than t can not. The implicit assumption in the original primitive of the secret sharing is that each player is either "good" or "bad", and "good" players are all willing to cooperate when reconstruction of the secret is desired. However, the "bad" players always cheat others in an arbitrary manner. No matter how "smart" the "bad" parties are, they must pay a "price" to reach their deception purposes. Sometimes the price is "high". Starting from the work of Halpern and Teague [3], secret sharing schemes and other cryptographic tasks were first revaluated in a game-theoretic perspective (see [4,5]). In this setting, none of players is honest or corrupted, but the players are viewed as rational and are assumed (only) to act in their own self-interest.

* Corresponding author (email: sci.cgpeng@gzu.edu.cn)

1.1 Motivation

We will naturally pose the question as to how the introduction of rationality into secret sharing protocols affects the analysis of these protocols based on the traditional assumptions. By defining a payoff function for each rational party, the process of secret sharing is considered as a game among n players. Unfortunately, as pointed out in [3], there is no rational party who would like to deliver his/her share in a one-shot recovering process. Thus the reconstruction of the secret cannot be completed. By repeating the recovering process many times and introducing punishments for deviants, this problem can be solved [6]. Intuitively, punishment rules serve as threats that make rational players not deviate from the protocol, and thus the secret recovery can be finally achieved. However, some punishments turn out to be empty threats [7]. So, every player behaves noncooperatively, that is, selfishly.

A group of people wishes to share the secrets in some practical situations in which some parties may cooperate while others may not cooperate. Sometimes the noncooperative people may cooperate with their opponents to maximize their utility. Therefore, their behavior is limited to always cooperate. It would be informative to take beliefs about their behavior into consideration. This would allow us to distinguish between a "good" party with highly "honest degree" (e.g., a 90% "good" party properly cooperate) and a "bad" party with highly "dishonest degree".

How should we deal with such a scenario generally arising in applications? Recently, game theory has found a wide range of applications in economics, political science, biology, business, and computer science. Certainly, it also provides us with a solid body of knowledge which is able to model features such as those discussed above. In particular, the so-called games of Bayesian games are those in which some parties do not know some parameters of the game they are playing. In this type of games, party's beliefs over other parties' real nature, past experiences, reputation factors, and so on can be taken into account when the optimal decision is made at any given point during the recovery phase of secret sharing. We model this as a secret sharing game using Bayesian games. Thus, applying the Bayesian games (Bayes rational action and Bayes rule), we extend the works of Halpern and Teague [3] and Maleka et al. [8] and introduce the Bayesian rational secret sharing (BRSS) problem.

1.2 Related work

In their frequently quoted paper, Halpern and Teague [3] studied the Nash equilibrium in secret sharing and secure multiparty computation, such as the Nash equilibrium surviving iterated deletion of weakly dominated strategies. Later, it was pointed out that it cannot delete all bad strategies. Lysyanskaya and Triandopoulos [9] studied a model with a mix parties between rational and malicious behaviors with simultaneous broadcast channels and implementation type. Kol and Naor raised problems of the strict Nash equilibrium [10] and the computational C-resilient equilibrium [11]. Allowing mistakes of the other parties, Fuchsbauer et al. [12] presented computational Nash equilibrium stable with respect to trembles. Maleka et al. [8] studied rational secret sharing scheme using repeated games. Some sequential rationalities were required in [11]. Ong et al. [13] presented the subgame perfect equilibrium but with an honest minority assumed.

Besides, it can be found in the conclusion part of some work [3] or in some surveys [5][1)] that there remains much undone concerning subgame perfect equilibria and other solution concepts, especially in the computational setting. Zhang and Liu [7] proposed the 2-out-of-2 rational secret sharing as an extensive game with imperfect information, provided a strategy for achieving secret recovery in this game, and proved the strategy is a sequential equilibrium. Then, in standard communication networks, they presented information-theoretic secure rational secret sharing scheme [14]. Tian et al. [15] reviewed the classical secure communication issues, which are always described as a set of interactive rules following a specified sequence in the perspective of game theory. By introducing rational communication participants, they model the secure communication process in the manner of game theory to capture the interactions of distrusted communication parties.

1) Katz J. Ruminations on defining rational MPC. Talk given at SSoRC, Bertinoro, 2008.

1.3 Intuition and contribution

Our intuition is that every party has a type which depends on its belief system. The type of an honest party is a probability which is greater than 1/2. That is to say, for an honest party, the cooperative probability could be greater than the noncooperative probability. The rational party has an incentive to cooperate by sending its share in Bayesian game to get a maximizing expected utility and a good reputation (denoted by prior probability). If a party does not cooperate by sending an invalid share or not sending her/his share in the current round, other parties take the punishment strategy which updates their "reputation" (certainly a"bad" reputation) according to the Bayes rules and do not cooperate with him/her in the further rounds. Note that the reputation is by prior probability. For fear of not receiving any share from others in the further rounds and having a bad reputation, a party will cooperate in the current round. At the beginning of the game, we assume that parties expect to cooperate with each other in order to get the secret and a good reputation, and they behave this way in every round. Thus, these rules act as an incentive for a player to cooperate.

In the game-theoretic setting, simple secret sharing has been shown to be impossible. Meanwhile, Maleka et al. [8] show that secret sharing is impossible if the secret sharing game is played only once and secret sharing is possible in the finitely repeated rational secret sharing only if players are not aware of the end of the game. To solve these problems, we introduce a Bayesian rational model for multiparty protocols and give protocols for secret sharing. Our major work is that the Bayesian view introduces a probability with which a player cooperates. Our contributions are as follows:

1. We present the first formal framework for BRSS with Bayesian dynamic game. We extend previous results of rational secret sharing to mixed model where there can be different classes of protocol parties. A BRSS is defined based on the perfect Bayesian equilibrium (PBE) with incomplete information.
2. In the framework, we propose the two-party or multiparty BRSS in nonsimultaneous channels and prove the condition for reaching PBE. In the game (played only once or repeated multiple times), all parties cooperate with each other using Bayes rule and obtain the maximizing expected utility. It also naturally solves the fairness problem of secret sharing.
3. In our Bayesian schemes, a "bad" dealer (or party) will be detected since the signcryption scheme is used among the dealer and each party. That is to say, we can also consider a rational dealer in this scheme. This scheme does not require the availability of secure channels between the dealer and each party individually.

1.4 Paper outline

The rest of the paper is organized in the following way. In Section 2, we give a brief introduction to the rational secret sharing and the basics of dynamic game of incomplete information. In Section 3, we analyze the 2-out-of-2 secret sharing using Bayesian game and prove that (C, C) is a PBE when there exists a complete honest party. In Section 4, we propose a Bayesian protocol for the 2-out-of-2 secret sharing. Section 5 extends the 2-out-of-2 Bayesian protocol to the case of t-out-of-n BRSS. Section 6 discusses some issues. In Section 7, we conclude the paper and give an insight on open problems in future.

2 Preliminaries

This section briefly reviews the concepts of rational secret sharing and Bayesian game.

2.1 Rational secret sharing protocol

Rational secret sharing protocol is to achieve the task of secret sharing a secret among n rational parties (denoted by $\mathcal{P}$). Each party $P_i \in \mathcal{P}$ has a payoff function $u_i : \{0,1\}^n \rightarrow \mathbb{R}$, which is the possible outcome of the reconstruction process. A outcome vector $O = (o_1; \cdots ; o_n) \in \{0,1\}^n$ represents an outcome of the recovery, where $o_i = 1$ iff P_i finally obtains the secret. Here, for $1 \leqslant i \leqslant n$, P_i's payoff function u_i satisfies:

Table 1 A strategic game of 2-out-of-2 secret sharing

$P_1 \setminus P_2$	C	D
C	(U, U)	(U^{--}, U^{+})
D	(U^{+}, U^{--})	(U^{-}, U^{-})

(a) For $\forall\ O, O' \in \{0,1\}^n$, if $o_i > o'_i$ then $u_i(O) > u_i(O')$.

(b) If $o_i = o'_i$ and $\sum_{i=1}^{n} o_i < \sum_{i=1}^{n} o'_i$, then $u_i(O) > u_i(O')$.

The above conditions (a) and (b) indicate that, on the one hand, party P_i always prefers to get the secret in the recovering phase than not getting it; on the other hand, it prefers the fewer of the other parties learning it, which would be better. The functionality of rational secret sharing is to achieve a scheme so that it is in the rational party's payoff to provide his/her share as indicated in the recovering process, and such that any deviation for every party must cause a loss in his/her payoff.

Here, we give a simple example of case of 2-out-of-2 rational secret sharing, which regards the one-shot recovering process and two-player strategic game. In this game, each party has two actions between Cooperate(C) and Defect(D), where Cooperate(C) denotes sending share and Defect(D) stands for doing nothing. This game can be stood for the table in Table 1 where P_1's actions are represented by rows and P_2's by columns, where $U^{+}, U, U^{-}, U^{--} \in \mathbb{R}$ represents party's payoff under the corresponding action profile. The action profile (C, D) produces a game outcome $(0, 1)$, which means party P_2 obtains the secret but party P_1 does not. Based on these assumptions of the payoff functions, the definition $U^{+} > U > U^{-} > U^{--}$ obviously holds.

Like the Prisoner's dilemma, there is a crucial problem that arises in the above game, that is. no matter what action his/her opponent adopts, a party adopting action D can obtains as much as possible and sometimes even higher payoff than choosing action C. Thus, none of rational parties have incentive to sending his/her share in such game with one-shot recovery. There also exists the same problem in the t-out-of-n secret sharing. Here, we will use the theory of Bayesian games to resolve this problem.

2.2 Bayesion game

This section briefly introduces some concepts of player's type, player's beliefs, and PBE in Bayesian games [6].

Definition 1 (Party's type and type space). Assume that party $P_i \in \mathcal{P}$ has a type $T_i \in \mathcal{T}_i$ with $\mathcal{T}_i$ being the type space for party P_i.

Definition 2 (Type profile). A type profile is a tuple of types $T = (T_1, \ldots, T_n)$, one for each party, which univocally determines the type of every party involved in a specific game. Note that $\mathcal{T} = \mathcal{T}_1 \times \cdots \times \mathcal{T}_n$.

Here, we can assign a type $T_i \in [0, 1]$ to each party P_i , which can be counted as his/her reputation.

We formalize the following definition of the party's belief system. Let $\Delta(X)$ be the space of probability distribution over the set X.

Definition 3 (Belief system). The belief that a party has the type of $P_j \in \mathcal{P}$ is denoted by a probability distribution over party P_j's type-space $\Delta(\mathcal{T}_j)$. Let each belief be denoted by Greek letters $\alpha(\cdot), \beta(\cdot), \ldots,$ and ρ denotes the set of all beliefs.

Fudenberg and Tirole [16] formally defined the notion of PBE for Bayesian games in 1991, which is defined as pairing of strategy–believe profile $(S; \rho)$ such that:

(1) The profile $(S; \rho)$ is not only a Bayesian Nash equilibrium in each of the continuation subgames, but also a Bayesian Nash equilibrium in the whole game. In other words, from every information set, the moving party's strategy maximizes its expected utility of the remainder of the game, taking into account his/her beliefs and all party's strategies.

(2) On-the-equilibrium path, believes are determined by the Bayes rule and equilibrium strategies. An information set will be attained with positive probability if and only if the game is played based on the equilibrium strategies. That is, this information set is on-the-equilibrium path.

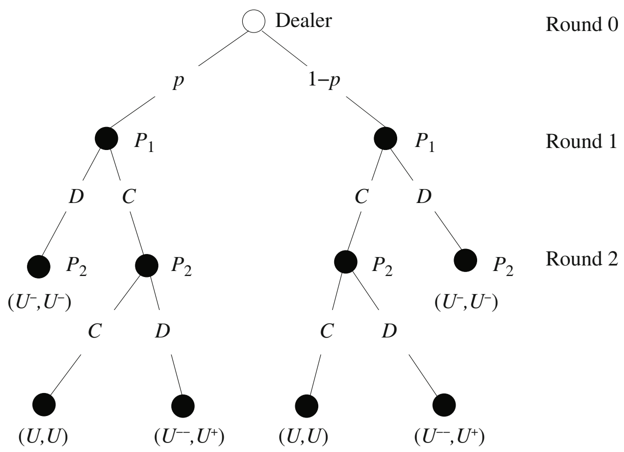

Figure 1 A game tree of 2-out-of-2 secret sharing.

(3) Off-the-equilibrium path, beliefs where possible are determined by the Bayes rule and equilibrium strategies. A defection from the equilibrium path, dose not increase the chance that others will play irrationally.

The profile $(S;\rho)$ would interpret a set of strategies such that given his/her beliefs in set $\mathcal{I}_i$, P_i's strategy is his/her best response for each party $P_i \in \mathcal{P}$ and each information set $I_i \in \mathcal{I}_i$. Before we formally give the notion of the PBE, it is necessary that we define a series of requirements.

Definition 4 (Bayes requirement 1)**.** Given S (i.e., a strategy profile), it is required that, for $\forall P_i \in \mathcal{P}$ and at each for $I_i \in \mathcal{I}_i$, P_i has beliefs $\rho(I_i) \in \Delta(I_i)$ about the node at which he/she is located, conditional upon being notified that party has attained I_i.

Definition 5 (Bayes requirement 2)**.** Assume that the continuation game is defined by $I_i \in \mathcal{I}_i$ of some party P_i and $\rho_i(I_i)$. The constraint for $(S;\rho)$ must be a Nash equilibrium of this game beginning with I_i.

Definition 6 (Bayes requirement 3)**.** The strategy profile based on Bayes' rule determines the beliefs at any on-the-equilibrium path information sets. That is to say, if $I_i \in \mathcal{I}_i$ is an information set of party P_i which achieved with positive probability following the strategy profile S, then S according to Bayes rule must compute $\rho(I_i) \in \Delta(I_i)$.

Definition 7 (Bayes requirement 4)**.** The strategy profile S in terms of Bayes rule whenever possible must determine the beliefs at any off-the-equilibrium path information set.

Definition 8 (PBE)**.** Given S and ρ (i.e., strategy profile and a set of beliefs), $(S;\rho)$ forms a PBE if and only if the strategy–belief profile $(S;\rho)$ satisfies Bayes requirements 1–4.

3 Bayesian analysis of 2-out-of-2 secret sharing

This section analyzes 2-out-of-2 secret sharing in a richer set of environmental hypotheses and only considers the simplest scenario: let party P_1 be either "good" or "bad", but P_2 is always "good". The game is shown in Figure 1.

3.1 Player and types

Assume that the player set $\mathcal{P} = \{P_1, P_2\}$ and the dealer is always "good". Denote $\mathcal{T} = \mathcal{T}_{P_1} \times \mathcal{T}_{P_2}$ by the type–profile space with $\mathcal{T}_{P_1} = \{P_1^h, P_1^d\}$ and $\mathcal{T}_{P_2} = \{P_2^h\}$ being the type spaces of parties P_1 and P_2. Superscript h represents a "good" party, while d denotes a "bad" one. Assume that the dealer is always honest ("good").

We consider the following probability distributions θ_{P_1} and θ_{P_2} over $\mathcal{T}_{P_1}$ and $\mathcal{T}_{P_2}$, respectively:

$$\theta_{P_1}^h = \Pr(P_1^h|P_2), \quad \theta_{P_1}^d = \Pr(P_1^d|P_2), \quad \text{s.t.} \quad \theta_{P_1}^h + \theta_{P_1}^d = 1, \tag{1}$$

and

$$\theta^h_{P_2} = \Pr(P^h_2|P_1) = 1, \ \ \theta^d_{P_2} = \Pr(P^d_2|P_1) = 0. \tag{2}$$

3.2 Strategies and beliefs

Every player can adopt a special action *quit* at anytime. Hence, the set of actions that are available to parties is $A = A_{P_1} \cup A_{P_2}$, where $A_{P_1} = \{C, D, quit_{P_1}\}$ and $A_{P_2} = \{C, quit_{P_2}\}$ are the sets of actions for players P_1 and P_2, respectively. So, players P_1 has three possible pure strategies and P_2 has two.

There are two possible pure strategies for player P_2. A pure strategy for player P_2 is $s_{P_2} \in S_{P_2} = \{(s_1, s_3)\}$. Alternatively, a pure strategy for player P_1 is a tuple: $s_{P_1} \in S_{P_1} = \{(s_1, s_3)_h, (s_2, s_3)_d\}$, where $s_1 \in \{C\}$, $s_2 \in \{D\}$, and $s_3 \in \{quit_{P_1}, quit_{P_2}\}$. The first component stands for a strategy for type P_1 "good" and the second one for P_1 "bad".

In the new Bayesian game, a strategy profile of one for each party is a vector $s = (s_{P_1}, s_{P_2})$ of individual strategies. The outcome of the game is univocally determined by a strategy profile. The following probability distributions denote, at each particular stage of the protocol, the set of beliefs which each party holds over the opponent's set of actions.

At round 2 of the Bayesion game, let the following probability distribution functions, over party P_2's set of actions, denote party P_2's beliefs:

$$\alpha_h, \alpha_d : \mathcal{T}_{P_1} \longrightarrow \Delta(A_{P_1}), \ \ \text{s.t.} \ \ \alpha_h(C) + \alpha_h(D) + \alpha_h(quit_{P_1}) = 1, \ \ \alpha_d(C) + \alpha_d(D) + \alpha_d(quit_{P_1}) = 1, \tag{3}$$

and P_2 believes that

$$\Pr_{P_2}[quit_{P_1}|P^h_1] + \Pr_{P_2}[C|P^h_1] = 1, \ \Pr_{P_2}[D|P^h_1] = 0, \tag{4}$$
$$\Pr_{P_2}[quit_{P_1}|P^d_1] + \Pr_{P_2}[D|P^d_1] = 1, \ \Pr_{P_2}[C|P^d_1] = 0. \tag{5}$$

Note that party P_2 also has the following beliefs which represent the fact that when party P_1 has defected, she/he will always take the action $quit_{P_1}$ or D in this game. Therefore, we have

$$\Pr_{P_2}[quit_{P_1}|P^h_2] + \Pr_{P_2}[D|P^h_2] = 1, \ \Pr_{P_2}[C|P^h_2] = 0, \tag{6}$$
$$\Pr_{P_2}[quit_{P_1}|P^d_2] + \Pr_{P_2}[D|P^d_2] = 1, \ \Pr_{P_2}[C|P^h_2] = 0. \tag{7}$$

By contrast, in round 1 of the game, P_1 has analog results.

$$\beta : \mathcal{T}_{P_2} \longrightarrow \Delta(A_{P_2}), \ \ \text{s.t.} \ \ \beta(C) + \beta(quit_{P_2}) = 1. \tag{8}$$

3.3 Utility functions

One of the crucial points for a game is each type of party being associated with a possibly different utility function. Definition of payoff functions is as follows:

$$U_i : \Pi_{i\in\{P_1,P_2\}}\mathcal{T}_i \times \Pi_{i\in\{P_1,P_2\}}A_i \longrightarrow \mathbb{R}. \tag{9}$$

So, for every branch in the game tree, we define a utility value as the total outcome parties P_1 and P_2 obtained, when selecting such a game path (see Figure 1). Obviously, $U_i \in \{\lambda_1 U^+ + \lambda_2 U + \lambda_3 U^- \lambda_4 U^{--} | \lambda_i \geqslant 0 \wedge \sum_{i=1}^4 \lambda_i = 1\}$.

3.4 Expected utilities

We denote the expected payoff for player P_i as $\mathrm{EU}(P_i, s_{P_i})$ with following the strategy s_{P_i}. We first discuss the expected utilities when parties take pure strategies. For each strategy profile $s_{P_1} = ((s_2, s_3)_d, (s_1, s_3)_h)$ of party P_1, the expected payoff value is

$$\mathrm{EU}({P_1}^h, s_{P_1}) = \beta(C)[U_{P_1}((s_1, s_3)_h, s_1) + (1 - \beta(C))[U_{P_1}((s_1, s_3)_h, s_3), \tag{10}$$
$$\mathrm{EU}({P_1}^d, s_{P_1}) = \beta(C)[U_{P_1}((s_2, s_3)_d, s_1) + (1 - \beta(C))[U_{P_1}((s_2, s_3)_h, s_3). \tag{11}$$

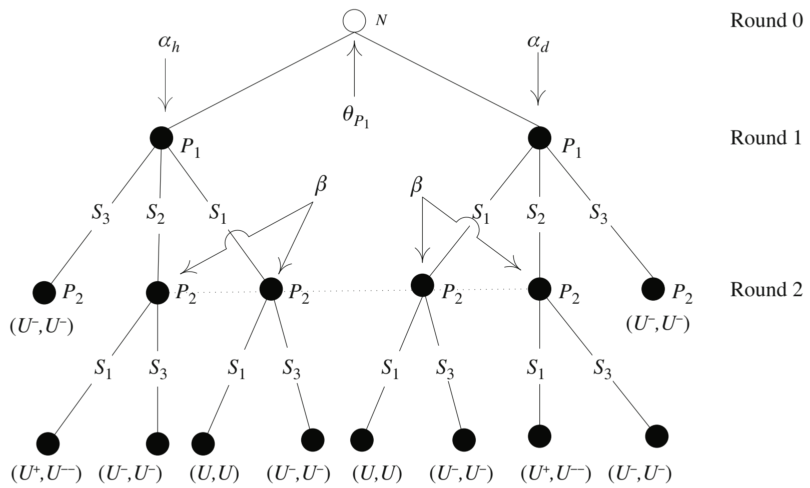

Figure 2 Bayesian game of 2-out-of-2 secret sharing.

In the case, if P_2 selects the action: $s_3 \in \{quit_{P_2}\}$, then P_2 has the following expected utility value:

$$\mathrm{EU}(P_2, s_3) = U^-. \tag{12}$$

Otherwise, the expected utility is

$$\begin{aligned}\mathrm{EU}(P_2, s_1) &= \theta^h_{P_1}[\alpha_h(s_1)\cdot U + \alpha_h(s_3)\cdot U^-] + (1-\theta^h_{P_1})[\alpha_d(s_2)\cdot U^{--} + \alpha_d(s_3)\cdot U^-]\\ &= \theta^h_{P_1}[\alpha_h(s_1)\cdot U - \alpha_d(s_2)\cdot U^{--} + (\alpha_h(s_3)-\alpha_d(s_3))\cdot U^-] + \alpha_d(s_2)\cdot U^{--} + \alpha_d(s_3)\cdot U^-\\ &= L_1\cdot\theta^h_{P_1} + L_2,\end{aligned} \tag{13}$$

where

$$L_1 = \alpha_h(s_1)\cdot U - \alpha_d(s_2)\cdot U^{--} + (\alpha_h(s_3)-\alpha_d(s_3))\cdot U^-, \quad L_2 = \alpha_d(s_2)\cdot U^{--} + \alpha_d(s_3)\cdot U^-. \tag{14}$$

Proposition 1. Under the mean utility criterion in the game, if $\theta^h_{P_1} \geqslant (U^- - L_2)/L_1$, then party P_2 always selects the action $s_1(C)$. Otherwise, he will select the action $s_3(quit_{P_2})$.

Proof. For an honest party P_2, according to (12) and (13), if $\theta^h_{P_1} \geqslant (U^- - L_2)/L_1$, then $\mathrm{EU}(P_2, s_3) \geqslant \mathrm{EU}(P_2, s_1)$. Thus, P_2 prefers s_1 to s_3. Otherwise, the action s_3 is the best strategy of P_2.

3.5 PBE candidates

Candidates to be PBE in the 2-out-of-2 secret sharing game will be $(S;\rho)$ with $S = (s_{P_1}, s_{P_2})$, $s_{P_1} \in S_{P_1}$, $s_{P_2} \in S_{P_2}$ and $\rho = (\theta_{P_1}, \theta_{P_2}, \alpha_h, \alpha_d, \beta)$ is a tuple which has the probability distribution functions denoting the set of beliefs depicted above. A given strategy–believe profile $(S^*;\rho^*)$ represents a PBE if it defines a strategy set such that, for $\forall P_i$ and $\forall I_i$, the strategy of P_i is his/her best response to the opponent's action strategy, given his/her belifs in the information set $\mathcal{I}_i$.

We will give the following $(S^*;\rho^*)$ as the first candidate to PBE of the Bayesian game in Figure 2.

$(S^*;\rho^*) = (\{(s_1)_h, (s_1)_d\}, \{(s_1)\}; (\theta^*_{P_1}, \theta^*_{P_2}, \alpha^*_h, \alpha^*_d, \beta^*))$, with $\theta^{h^*}_{P_1} \geqslant (U^- - L^*_2)/L^*_1$, where Eq. (14) contains the definitions of L^*_1 and L^*_2. Note that the PBE candidate interprets the party P_1's intention to succeed in recovery phase.

The next candidate for PBE to be considered stands for the set of P_1's strategies and P_2's strategies when P_2 thinks that P_1 is wants to noncooperation at round 1. Then, P_2's strategy for the best response is to quit the game:

$(S^o;\rho^o) = (\{(s_3)_h, (s_2)_d\}, \{(s_3)\}; (\theta^o_{P_1}, \theta^o_{P_2}, \alpha^o_h, \alpha^o_d, \beta^o))$, with $\theta^{h^o}_{P_1} < (U^- - L^o_2)/L^o_1$, where L^o_1 and L^o_2 will be defined as in (14).

Next, we commence with the case of $(S^*;\rho^*)$ which is a PBE of the secret sharing game of the 2-out-of-2 case, as $(S^o;\rho^o)$ can be inferred from the following steps trivially.

Theorem 1. The profile $(S^*;\rho^*)$ is a PBE in 2-out-of-2 secret sharing game.

Proof. A PBE requires that $(S^*;\rho^*)$ should satisfy Bayes requirements 1–4.

First, we show that the profile $(S^*;\rho^*)$ satisfies Bayes requirement 1. Requirement 1 requests that each player for P_1 and P_2 allocates a distribution of probability over each of nodes in every information set $I_i \in \mathcal{I}_i$. At the first round of the Bayesion game, player P_1 learns his/her type and $\theta^h_{P_1}+\theta^d_{P_1}=1$ (see (1)). At round 2, regarding ρ^*, player P_2 defines the probability distributions α^*_h, as well as α^*_d satisfy $\alpha^*_h(s_1)+\alpha^*_h(s_3)=1$ $\alpha^*_d(s_2)+\alpha^*_d(s_3)=1$ according to (3)–(5). Then, we have $\theta_h^{P_1{}^*}\cdot\alpha^*_h(s_1)+\theta_h^{P_1{}^*}\cdot\alpha^*_h(s_3)+\theta_d^{P_1{}^*}\cdot\alpha^*_d(s_2)+\theta_d^{P_1{}^*}\cdot\alpha^*_d(s_3)=1$. Therefore, $(S^*;\rho^*)$ satisfies Bayes requirement 1.

Second, rational P_2 behaves based on his/her beliefs. Once the Bayesion game is over, player P_2 achieved the information set I_{P_2}. Assume that SG is the continuation game beginning with the same $I_{P_2}\in\mathcal{I}_{P_2}$, as well as $\rho^*(I_{P_1})$ are the assumption belief at I_{P_1}. Then, we know that $(S^*;\rho^*(I_{P_1}))$ is an equilibrium of the SG.

In the light of $\theta^{h^*}_{P_1}\geqslant(U^- - L^*_2)/L^*_1$ and Proposition 1, we have $\mathrm{EU}(P_2,s_3,SG)\leqslant\mathrm{EU}(P_2,s_1,SG)$. Hence, a rational party P_2 cannot deviate from the rule based on its belief system.

Therefore, $(S^*;\rho^*)$ satisfies Bayes Requirement 2 since the profile strategy, given by $(S^*;\rho^*(I_{P_2}))$, forms an equilibrium in this SG.

Third, at the on-equilibrium path information set I_{P_2}, requirement 3 requests P_2 for establishing sensible beliefs. The strategy profile based on the Bayes rule can determine these sets of beliefs. Thus, party P_2 has to find distributions α^*_h, as well as α^*_d according to the different action strategies that party P_1 can adopt at the first round of the game.

According to (3)–(5), if P_2 believes that a "good" player P_1 would take the action s_1 with probability γ_h, the action s_2 with δ_h as well as the action s_3 with $(1-\gamma_h-\delta_h)$, then $\alpha^*_h(s_1)$ and $\alpha^*_h(s_3)$ must take the following values:

$$\alpha^*_h(s_1)=\frac{\gamma_h}{\gamma_h+\delta_h},\quad \alpha^*_h(s_3)=\frac{\delta_h}{\gamma_h+\delta_h}.$$

Likewise, as for a "bad" player P_1, player P_2 is demanded to define

$$\alpha^*_d(s_2)=\frac{\gamma_d}{\gamma_d+\delta_d},\quad \alpha^*_d(s_3)=\frac{\delta_d}{\gamma_d+\delta_d}.$$

Finally, at any off-the-equilibrium path information set, requirement 4 claims P_2 to establish sensible beliefs. Requirement 4 is trivially satisfied for there being no information sets off the Nash equilibrium path.

So, $(S^*;\rho^*)$ is a PBE in 2-out-of-2 secret sharing game by Definition 8.

3.6 A numerical instance

Note that Theorem 1 shows that the strategy S^* is an equilibrium depending on the condition of $\theta^{h^*}_{P_1}\geqslant(U^- - L^*_2)/L^*_1$ and beliefs of each party. Next, we give an example in which a set of parameter values reached equilibrium when both parties behave rationally, as well as achieve a successful reconstruction protocol in the secret sharing scheme (see Table 2).

Let us suppose the payoffs $U^+=5$, $U=3$, $U^-=1$, and $U^{--}=0$ in the game. Assume that party P_1 can make sure that P_2 is always honest by past experience and reputation, and that party P_2 has reasons to think that P_1 is not always "good". P_2 evaluates P_1 to be "good" with probability $\theta^h_{P_1}=0.6$. Assume that party P_2 does also have enough evidence to evaluate that when P_1 is "good", his/her misbehaving probability at the step of this game is very low, where $\alpha_h(C)=0.6$, $\alpha_h(D)=0.1$, and $\alpha_h(quit_{P_1})=0.3$. Likewise, $\alpha_d(C)=0.1$, $\alpha_d(D)=0.7$, and $\alpha_d(quit_{P_1})=0.2$. According to the results in Table 2, we know that P_2 had better respond to s_1 (i.e., P_2 had better choose cooperation). By contrast, P_2 will quit the game since $\theta^h_{P_1}\geqslant L$ when $U^-=2.05$. In general, we here assume that $U\geqslant(U^+ + U^-)/2$.

Table 2 A numerical example

	$U^+ = 5$	$U = 3$	$U^- = 1$	$U^{--} = 0$
Beliefs	$\theta^h_{P_1} = 0.6$	$\alpha_h(C) = 0.6$	$\alpha_h(D) = 0.1$	$\alpha_h(quit_{P_1}) = 0.3$
	$\theta^d_{P_1} = 0.4$	$\alpha_d(C) = 0.1$	$\alpha_d(D) = 0.7$	$\alpha_d(quit_{P_1}) = 0.2$
Results	$L_1 = 1.8$	$L_2 = 0.2$	$L = \frac{U^- - L_2}{L_1} = -4.5$	$\theta^h_{P_1} \geqslant L$

Table 3 The 2-out-of-2 secret sharing protocol $\prod_{2,2}$

Bayesian secret sharing $\prod_{2,2}$

Let $(\mathrm{Gen}, \mathrm{SC}, \mathrm{UNSC})$ be signcryption scheme. Assume that the player set is $N = \{P_1; P_2\}$ and there exists a dealer distributing shares in the sharing phase. Let s denote the secret and $s = s_1 \oplus s_2$ for simplicity. Protocol $\prod_{2,2}$ is defined as follows:

Sharing phase

The phase consists of three steps:
1. The dealer first computes $(pk_d, sk_d) \leftarrow \mathrm{Gen}(1^k)$. Next party P_1 and P_2 do $(pk_1, sk_1) \leftarrow \mathrm{Gen}(1^k)$ and $(pk_2, sk_2) \leftarrow \mathrm{Gen}(1^k)$, respectively.
2. Then the dealer computes: $C_0 := C(s)$, $share_1 := \mathrm{SC}_{sp_d, pk_1}(s_1)$, and $share_2 := \mathrm{SC}_{sp_d, pk_2}(s_2)$, where $C(\cdot)$ is a public one-way function.
3. Finally, the dealer gives P_1 the $share_1$ and C_0, gives P_2 the $share_2$ and C_0. When P_1 and P_2 receive the $share_1$ and $share_2$, respectively, every P_i can verify valid share and get the s_i by $\mathrm{UNSC}_{pk_d, sk_i}(share_i)$.

Reconstruction phase

When it is time for recovery, player P_1 and P_2, with P_i's type being $\theta_i \in [0, 1]$, simultaneously choose the actions $s_{P_1} \in \{C, D, quit_{P_1}\}$, as well as $s_{P_2} \in \{C, D, quit_{P_2}\}$ in terms of their beliefs as well as Bayes rules, respectively. In each round of the game $r = 1, 2, \ldots$, the players do as followings:

P_i **sends message to** $P_j (\neq P_i)$**:** P_i
1. estimates $\theta_j^{h^{(r)}} := \mathrm{Pr}_{P_i}(\theta_i^{(r-1)} | \theta_j)$, $\theta_j^{d^{(r)}} := 1 - \theta_j^{h^{(r)}}$. (we assume that $\theta_j^{h^{(0)}} > 1/2$).
2. computes $\alpha_h^{(r)}(C) := \mathrm{Pr}_{P_j}(C | \theta_j^{h^{(r)}})$, $\alpha_h^{(r)}(D) := \mathrm{Pr}_{P_j}(D | \theta_j^{h^{(r)}})$, and $\alpha_h^{(r)}(quit_{P_j}) := \mathrm{Pr}_{P_j}(quit_{P_j} | \theta_j^{h^{(r)}})$. Likewise, $\alpha_d^{(r)}(C)$, $\alpha_d^{(r)}(D)$, and $\alpha_d^{(r)}(quit_{P_j})$.
3. computes its expected utility maximization using results of the above steps, where denoted the optimal strategy by $os_i^{(r)} \in \{C, D, quit_i\}$.
4. If $os_i^{(r)} = C$, then P_i sends $\mathrm{SC}_i^{(r)} := \mathrm{SC}^{(r)}_{pk_j, sk_i}(s_i)$ to P_j. Else if $os_i^{(r)} = D$, then P_i sends $\mathrm{SC}_i^{(r)} := \mathrm{SC}^{(r)}_{pk_j, sk_i}(s_i')$ to P_j, where $s_i' (\neq s_i)$ is an invalid share. Otherwise, P_i quit the game.

P_i **receives message from** $P_j (\neq P_i)$**:**P_i
1. receives $\mathrm{SC}_j^{(r)}$ from P_j. If share $\mathrm{SC}_j^{(r)}$ passes verification of the $\mathrm{UNSC}_{pk_j, sk_i}(\mathrm{SC}_j^{(r)})$ whether $C_0 = C(s_i \oplus s_j)$, then P_i updates the P_j's reputation $\theta_j^{(r)} := \mathrm{Pr}_{P_j}(\theta_j^{(r)} | C)$ and halts. Else $\theta_j^{(r)} := \mathrm{Pr}_{P_j}(\theta_j^{(r)} | D)$ and halts.
2. updates the P_j's reputation $\theta_j^{(r)} := \mathrm{Pr}_{P_j}(\theta_j^{(r)} | quit_j)$ and halts without P_j sending anything.

4 Bayesian 2-out-of-2 secret sharing

This section describes Bayesian secret sharing protocol of the 2-out-of-2 case based on the above analysis. We give the formal specification in Table 3. Our protocol has two phases: the sharing phase and the reconstruction phase.

Sharing phase. In this phase, a dealer distributes shares to both parties. We assume that the dealer is also rational rather than honest or dishonest, and the dealer can distribute the shares successfully. We do not discuss the rational dealer problem in this paper. The rational dealer case is shown in [17]. The dealer first commits the secret s using a public one-way function $C(\cdot)$ and then generates a ciphertext σ_i using the algorithm SC, which signcrypts s_i with dealer's private key as well as P_i's public key. Following the dealer sends the ciphertext σ_i to party P_i and broadcasts C. Finally, by receiving σ_i, P_i can verify the validity of the share and get s_i by the algorithm UNSC.

Reconstruction phase. The recovery phase is done in a series of rounds, each round constituting one message which is sent by each player. No private channel is needed between two parties since the message is signcrypted by each sender using a signcryption scheme. There is no need to assume simultaneous communication, although messages could be simultaneously sent, since every party makes decision based on his/her beliefs and types.

Theorem 2. The protocol in Table 3 induces a PBE (C, C) if there exists a completely honest player (i.e., $\exists P_i$, s.t. $\theta_i^h = 1$), and if there exists a completely dishonest player (i.e., $\exists P_j$, s.t. $\theta_j^d = 1$), no rational player will cooperate with each other.

Proof. A complete honest player P_i always adopts either the action C or the special action $quit_{P_i}$. For the other party P_j, according to Table 3, it is best to respond to action C by the expected payoff maximization rules. Otherwise, his/her payoff will be less. When he/she chooses C, the best action of a complete honest player is also the action C by Proposition 1. Hence, the rational entities will cooperate with each other. According to Theorem 1, the strategic profile (C, C) is a PBE in this case.

On the other hand, for a completely dishonest player, then (D, D) is a PBE too. So, they will not cooperate.

5 Bayesian *t*-out-of-*n* secret sharing

This section will describe extensions of the above protocol to the t-out-of-n case, denoted by $\prod_{t,n}$. Assumping that t parties being active during the recovery, the protocol $\prod_{t,n}$ can be resilient to coalitions of up to $t-1$ players. Assume that communication can be over a synchronous peer-to-peer network without simultaneity. The formal specification is given in Table 4.

As in the 2-out-of-2 case, the protocol $\prod_{t,n}$ has two phases: the sharing phase as well as the reconstruction phase. In the sharing phase, the dealer chooses a random polynomial $F(x)$ of $(t-1)$-degree subject to the restraint $F(0) = s$, as well as gives the signcryption $share_i$ of $F(i)$ combined with the public information C to player P_i (for $i = 1, \ldots, n$). In the reconstruction phase, every party P_i makes decision in terms of its beliefs and the reputation of its opponents P_{-i} to maximize its expected utility. Any party P_i who has t valid shares can recover $F(x)$ (and hence s) by interpolating the polynomial. Furthermore, a party who gets fewer than t shares cannot deduce any information about s. See Table 4 for details.

Theorem 3. Under the protocol $\prod_{t,n}$ in Table 4, all active rational parties cooperate together if they believe that there exist at least $(t^* - t + 1)$ parties whose $\theta_j^h > 1/2$, and they will not cooperate if there are $(t^* - t + 1)$ parties whose $\theta_j^h < 1/2$, where t^* stands for the number of the active parties during the reconstruction phase.

Proofs are omitted due to space limitations, as well as the proof is exactly analogous to the proof of Theorem 2.

6 Discussion

In this section, some further issues will be considered to fulfill this work of secret sharing from Bayesian rationality in game theory setting.

6.1 Asynchronous networks

Many previous rational secret sharing schemes [3,7,9,18,19] rely on the existence of simultaneous broadcast channel. The proposed protocol $\prod_{t,n}$ can be used even when players communicate over an asynchronous point-to-point network. Under the circumstances, players cannot make out an abortion which derives from a delayed message. Therefore, the protocol is modified as follows: each player continues doing the next round as soon as he/she gets $t-1$ valid messages which are derived from the previous round, as well as only quits if he/she receives an invalid message derived from someone as in the case of [12]. Every party easily verifies the share validity by signcryption scheme in our protocol. Our protocols in Tables 3 and 4 can run over asynchronous networks if every party makes decision according to its expected utility maximization and Bayes rule.

Table 4 The t-out-of-n secret sharing protocol $\prod_{t,n}$

Bayesian secret sharing $\prod_{t,n}$

The protocol of secret sharing for the t-out-of-n case consists of two phases: sharing phase and reconstruction phase.

Sharing phase

In order to share a secret $s \in \{0,1\}^l$ among $\mathcal{P} = \{P_1, \ldots, P_n\}$, the dealer and all parties do the following:
1. Dealer generates $(pk_d, sk_d) \leftarrow \text{Gen}(1^k)$ and party P_i do $(pk_i, sk_i) \leftarrow \text{Gen}(1^k)$, for all $P_i \in \mathcal{P}$.
2. Dealer chooses random $(t-1)$-degree polynomials $F \in \mathbb{F}_{2^l}[x]$ subject to $F(0) = s$.
3. Dealer computes $s_i := F(i)$,$C_i = C(s_i)$, for all $i \in \{1, \ldots, n\}$ and $C_0 = C(s)$, where $C(\cdot)$ is the one-way function, denoted by $C = \{C_0, C_1, \ldots, C_n\}$.
4. Dealer sends $share_i$ and C to P_i, where $share_i := \text{SC}_{sp_d,pk_i}(s_i)$, for all $P_i \in \mathcal{P}$.
5. When every P_i receives $share_i$ and C from dealer, it can verify valid share and get the s_i by $\text{UNSC}_{pk_d,sk_i}(share_i)$.

Reconstruction phase

When it is time for recovery, assume that I is the indices of the t active parties, party P_i selects actions $s_{P_i} \in \{C, D, quit_{P_i}\}$ at the same time, according to their beliefs and Bayes rules, with P_i's type being $\theta_i \in [0,1]$ for $i \in I$. denoted by $P_{-i} = P_{(i\in I)} \backslash P_i$. In each round $r = 1, 2, \ldots$, the players do:

P_i **sends message to** P_{-i}**:** For all $P_j \in P_{-i}$, P_i
1. estimates $\theta_j^{h^{(r)}} := \Pr_{P_i}(\theta_i^{(r-1)}|\theta_j), \theta_j^{d^{(r)}} := 1 - \theta_j^{h^{(r)}}$. (assume that $\theta_j^{h^{(0)}} > 1/2$).
2. computes $\alpha_h^{(r)}(C) := \Pr_{P_j}(C|\theta_j^{h^{(r)}}), \alpha_h^{(r)}(D) := \Pr_{P_j}(D|\theta_j^{h^{(r)}})$ and $\alpha_h^{(r)}(quit_{P_j}) := \Pr_{P_j}(quit_{P_j}|\theta_j^{h^{(r)}})$. Likewise, $\alpha_d^{(r)}(C)$, $\alpha_d^{(r)}(D)$ and $\alpha_d^{(r)}(quit_{P_j})$.
3. computes its expected utility maximization using results of the above steps, where the optimal strategy is denoted by $os_i^{(r)} \in \{C, D, quit_i\}$.
4. If $os_i^{(r)} = C$, then P_i sends $\text{SC}_i^{(r)} := \text{SC}_{pk_j,sk_i}^{(r)}(s_i)$ to P_j. Else if $os_i^{(r)} = D$, then P_i sends $\text{SC}_i^{(r)} := \text{SC}_{pk_j,sk_i}^{(r)}(s'_i)$ to P_j, where $s'_i(\neq s_i)$ is a invalid share. Otherwise, P_i quits the game.

P_i **receives message from** $P_j(\neq P_i)$**:**
1. P_i receives $\text{SC}_j^{(r)}$ from P_j. If share $\text{SC}_j^{(r)}$ passes verification of the $\text{UNSC}_{pk_j,sk_i}(\text{SC}_j^{(r)})$ whether $C_j = C(s_j)$, then P_i updates the P_j's reputation $\theta_j^{(r)} := \Pr_{P_j}(\theta_j^{(r)}|C)$ and halts. Else $\theta_j^{(r)} := \Pr_{P_j}(\theta_j^{(r)}|D)$ and halts.
2. If P_j does not send anything, then P_i updates the P_j's reputation $\theta_j^{(r)} := \Pr_{P_j}(\theta_j^{(r)}|quit_j)$ and halts.

6.2 Computational PBE

An important issue is that we should consider computational Perfect Bayesian Equilibrium (CPBE) in cryptographic protocols. Since verification of the receiving messages, in our model depends on a signcryption algorithm SC$(\cdot)$ and the one-way function $C(\cdot)$, we had better consider computational issues when defining PBE. Based on the concepts of computational equilibria proposed in the quote references, we can define an efficient strategy to be Bayes rationality in the computational setting. That is, if after any information sets, any resultful defections of a single party can produce a earnings of at most $\epsilon(k)$, with $\epsilon(k)$ being a negligible function. It is required that these strategies satisfy Bayes requirements 1–4. In the computational setting, Katz[1)] gave the further consideration for the definition of subgame perfect equilibrium. He presented that the probability, a history happens, should be contained in this definition, while the required rationality after any history. Zhang [7] believes that the rational setting is very complicated, as well as the bounded rationality maybe frequently results in unexpected outcomes. It is difficult to define the Bayes rationality of rational secret sharing properly in the computational setting, as well as there is still a long way to go.

Another important issue is that we need to define the k-resilient PBE to take into account the rational secret sharing for the t-out-of-n case in Bayesian game. In Section 5, we only designed a very simple Bayesian t-out-of-n secret sharing scheme without further considering k-resilient PBE. Intuitively, after any information sets all parties should persist in the original strategies except that a group of k parties collaborate to defect, but the payoff of any one of the k defectors cannot be increased. To use our proposed t-out-of-n game model, a possible solution is that all parties jointly decide a random order on the k bad reputation parties, as well as in the next round, the k parties are asked for sending messages based on this order first. If none of these parties defects, then the remainder of parties are demanded to send their share simultaneously, otherwise the rest of parties quit this game or select action D. Here, referring to the concepts of k-resilient equilibria which are proposed in previous work [14], we can analogously define k-resilient PBE. In fact, both Table 3 and Table 4 are 1-resilient. When there exists a bad reputation party who chooses action D, other parties will select the action D or *quit* according to its maximizing expected utility.

7 Conclusion

We have modeled the secret sharing as a dynamic game of incomplete information (or Bayesian dynamic game). We first analyze the 2-out-of-2 secret sharing with Bayesian game and prove that both parties cooperate in the presence of a complete honest party, which is a PBE. Based on these results, we propose the two-party and the multiparty setting Bayesian secret sharing. The main advantage of introducing the Bayesian games is that the parties will select the strategy, which is mutually beneficial according to party's beliefs and type. Thus, a long-term cooperative relation would be maintained among the parties to gain more benefits. Our techniques can certainly be extended to the multi-party secure computation. We hope that the notion of Bayesian games can be introduced to other cryptographic primitives as well as distributed computing problems, where these parties are of different types (for honest or malicious parties). We should enhance the scope for problem–solving strategies in asynchronous networks.

Acknowledgements

This work was supported by Program for Changjiang Scholars and Innovative Research Team in University (Grant No. IRT1078), Key Program of NSFC-Guangdong Union Foundation (Grant No. U1135002), Major National S&T Program (Grant No. 2011ZX03005-002), National Natural Science Foundation of China (Grant Nos. 61170280, 61272398, 61262073, 61363068), China Postdoctoral Science Foundation (Grant No. 2013M530705), Natural Science Foundation of Guizhou of China (Grant No. 20132112), Doctor Foundation of the Guizhou University (Grant No. 2012-024), and Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No. XDA06010701).

References

1 Blakley G R. Safeguarding cryptographic keys. In: Proceedings of the 1979 AFIPS National Computer Conference. Monval: AFIPS Press, 1979. 313–317
2 Shamir A. How to share a secret. Commun ACM, 1979, 22: 612–613
3 Halpern J, Teague V. Rational secret sharing and multiparty computation: extended abstract. In: Proceedings of 36th Annual ACM Symposium on Theory of Computing (STOC). New York: ACM, 2004. 623–632
4 Dodis Y, Rabin T. Cryptography and game theory. In: Nisan N, Roughgarden T, Tardos E, et al., eds. Algorithmic Game Theory. Cambridge: Cambridge University Press, 2007. 181–207
5 Katz J. Bridging game theory and cryptography: recent results and future directions. In: Proceedings of 5th Theory of Cryptography Conference. Heidelberg: Springer, 2008. 251–272
6 Fudenberg D, Tirole J. Game Theory. Cambridge: MIT Press, 1992
7 Zhang Z F, Liu M L. Rational secret sharing as extensive games. Sci China Inf Sci, 2013, 56: 032107
8 Maleka S, Shareef A, Pandu Rangan C. Rational secret sharing with repeated games. In: Proceedings of 4th Information Security Practice and Experience Conference. Heidelberg: Springer, 2008. 334–346
9 Lysyanskaya A, Triandopoulos N. Rationality and adversarial behavior in multiparty computation. In: Dwork C, ed. In: Proceedings of 26th Annual International Cryptology Conference. Heidelberg: Springer, 2006. 180–197
10 Kol G, Naor M. Games for exchanging information. In: Proceedings of 40th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2008. 423–432
11 Kol G, Naor M. Cryptography and game theory: designing protocols for exchanging information. In: Proceedings of 5th Theory of Cryptography Conference. Heidelberg: Springer, 2008. 320–339
12 Fuchsbauer G, Katz J, Naccache D. Efficient rational secret sharing in standard communication networks. In: Proceedings of 7th Theory of Cryptography Conference. Heidelberg: Springer, 2010. 419–436
13 Ong S J, Parkes D V, Rosen A, et al. Fairness with an honest Minority and a rational majority. In: Proceedings of 6th Theory of Cryptography Conference. Heidelberg: Springer, 2009. 36–53
14 Zhang Z F, Liu M L. Unconditionally secure rational secret sharing in standard communication networks. In: Proceeding of 13th International Conference on Information Security and Cryptology. Heidelberg: Springer, 2011. 355–369

15 Tian Y L, Ma J F, Peng C G, et al. A rational framework for secure communication. Inf Sci, 2013, 250: 215–226
16 Fudenberg D, Tirole J. Perfect Bayesian equilibrium and sequential equilibrium. J Econ Theory, 1991, 53: 236–260
17 Tian Y L, Ma J F, Peng C G, et al. Game-theoretic analysis for the secret sharing scheme (in Chinese). Acta Electron Sin, 2011, 39: 2790–2795
18 Abraham I, Dolev D, Gonen R, et al. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In: Proceedings of 25th ACM Symposium Annual on Principles of Distributed Computing. New York: ACM Press, 2006. 53–62
19 Gordon S D, Katz J. Rational secret sharing, revisited. In: Proceedings of 5th Conference on Security and Cryptography for Networks. Heidelberg: Springer, 2006. 229–241