Rational Secret Sharing As Extensive Games

Zhifang Zhang

Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China
zfz@amss.ac.cn

Abstract. Some punishments in rational secret sharing schemes turn out to be empty threats. In this paper, we first model 2-out-of-2 rational secret sharing in an extensive game with imperfect information, and then provide a strategy for achieving secret recovery in this game. Moreover, we prove that the strategy is a sequential equilibrium which means after any history of the game no player can benefit from deviations so long as the other players stick to the strategy. Therefor, by considering rational secret sharing as an extensive game, we design a scheme which eliminates empty threats. Except assuming the existence of a simultaneous broadcast channel, our scheme can have dealer off-line and extend to the t-out-of-n rational secret sharing, and also satisfies computational equilibria in some sense.

Keywords rational secret sharing, extensive game, sequential equilibrium

1 Introduction

The well-known t-out-of-n secret sharing problem, first independently studied by Blakley [2] and Shamir [17] in 1979, is that a dealer holding a secret distributes shares among n players such that any group of t or more players can recover the secret from their shares while any group of fewer than t players can not. Most solutions to this problem are based on an implicit assumption that each player is either honest or malicious and the honest players will faithfully execute the protocol. In 2004 Halpern and Teague [8] studied the problem in a game theoretic sense and proposed rational secret sharing which is to fulfill the task among rational players. That is, instead of being totally honest or arbitrarily malicious, rational players only act in their own self-interest. Until now a lot of work has been devoted to bridging game theory and cryptography [3, 9]. Among this, rational secret sharing is an important problem.

Defining a utility function for each player, the process of secret sharing is viewed as a game among n players. But as pointed out in [8] no rational player would deliver his share in a one-shot recovering process, thus the recovery cannot be achieved. Like the repeated prisoner's dilemma [5], this problem can be solved by repeating the recovering process for many times and introducing punishments for deviants. Intuitively, punishment rules act like threats that make rational players would not deviate from the protocol, thus secret recovery can be finally

achieved. But some punishments turn out to be *empty threats*. For example, in 2-out-of-2 rational secret sharing, if a player punishes the deviant by stoping cooperating with him right after detecting cheats, then this punishment also greatly damages the punisher himself, because it makes the punisher forever lose the opportunity of getting the secret. Obviously, a rational player would not execute this punishment. A punishment like this is called an empty threat. Most previous work about rational secret sharing [4, 7, 8, 12, 14] cares little about empty threats.

In game theory, the problem of empty threats is conquered in the model of extensive games. Unlike the strategic game which models a one-shot process where each player chooses his plan of action once and for all, the extensive game explicitly describes the sequential structure of a game where each player can consider their plan of action at any point of time when he is required to move. Thus rationality in extensive games is required to be held after any history of the game. In this paper, we model rational secret sharing in an extensive game with imperfect information and provide a strategy for achieving secret recovery in this game. Moreover, we prove that the strategy is a sequential equilibrium which means after any history no player can benefit from deviations so long as the other players stick to the strategy. In particular, whenever a cheat is detected the corresponding punishment in our scheme will definitely be executed because of the sequential rationality required. Therefor, by considering rational secret sharing as an extensive game, we design a scheme which eliminates empty threats.

1.1 Previous Work and Our Contribution

What kind of rationality should be achieved is a central problem in rational secret sharing. Halpern and Teague [8] proposed the Nash equilibrium surviving iterated deletion of weakly dominated strategies which was later pointed out cannot delete all bad strategies. Kol and Naor proposed the strict Nash equilibrium [12] and then the computational $\mathcal{C}$-resilient equilibrium [11], but these concepts are either too strict or not applicable. Allowing mistakes of the other players, Fuchsbauer et al. [4] proposed computational Nash equilibrium stable with respect to trembles, but they did not explicitly consider the sequential structure of the rational secret sharing game. Maleka et al. [14] studied rational secret sharing in repeated games, but they only discussed the Nash equilibrium in that game instead of considering the more meaningful equilibria, such as the subgame perfect equilibrium. On the other side, some properties similar to sequential rationality were required in [11], but we did not see strict proofs of the related issues. Ong et al. [15] discussed the subgame perfect equilibrium but an honest minority was assumed. Besides, it was written in the conclusion part of some work [8] or in some surveys [3, 10] that there remains much undone concerning subgame perfect equilibria and other solution concepts, especially in the computational setting.

Based on the possible solutions to rational secret sharing, we model the process in an extensive game with imperfect information and simultaneous moves.

This model provides a more precise description of the problem, and rationality in this game is usually captured by the concept of sequential equilibria which is an extension of subgame perfect equilibria. Thus the main contribution of this work is to study rational secret sharing precisely in an extensive game model and provide a scheme which is a sequential equilibrium of the game. Comparing with the schemes considered in a strategic game model, our scheme has the advantage of eliminating empty threats. Related to the scheme, we also provide some immature viewpoints about k-resilience of the sequential equilibrium and definitions in the computational setting.

1.2 Organizations

Section 2 introduces preliminaries needed in this paper, including extensive games and sequential equilibria. Section 3 first builds an extensive game model for 2-out-of-2 rational secret sharing, and then prove a strategy that achieves secret recovery is a sequential equilibrium. Thus a 2-out-of-2 rational secret sharing scheme is given. Section 4 improves the scheme by making the dealer off-line and extends it to the t-out-of-n case. It also discusses issues about simultaneous broadcast and computational equilibria. Section 5 concludes the paper.

2 Preliminaries

2.1 Rational Secret Sharing

Rational secret sharing is to fulfill the task of secret sharing among n rational players. Precisely each player, say P_i, has a utility function $u_i : \{0,1\}^n \to \mathbb{R}$ over the possible outcomes of the recovery. A vector $\mathbf{O} = (o_1, ..., o_n) \in \{0,1\}^n$ denotes an outcome of the recovery where $o_i = 1$ if and only if P_i finally gets the secret. For simplicity, we take the widely adopted assumptions about the utility functions. That is, for $1 \leq i \leq n$, P_i's utility function u_i satisfies

1. For any $\mathbf{O}, \mathbf{O}' \in \{0,1\}^n$, if $o_i > o_i'$ then $u_i(\mathbf{O}) > u_i(\mathbf{O}')$.
2. If $o_i = o_i'$ and $\sum_{i=1}^n o_i < \sum_{i=1}^n o_i'$, then $u_i(\mathbf{O}) > u_i(\mathbf{O}')$.

The above two conditions indicate that P_i always prefers to learn the secret than to not learn it and secondarily, prefers that the fewer of the other players who get it, the better. The aim of rational secret sharing is to design a protocol so that it is in the rational player's interest to provide his share as indicated in the recovering phase. Obviously, it suffices to design a secret sharing protocol such that for every player any deviation from the protocol causes a loss in his utility.

Consider a simple example of 2-out-of-2 rational secret sharing. In the recovering phase when P_i $(i = 1, 2)$ is supposed to provide the share, he chooses one from the two actions: broadcasting share (denoted by B) and keeping silence (denoted by S). On the assumption that all shares can be publicly authenticated [1], the action of delivering a fake share is identified with the action of keeping

[1] This can be realized by associating each share with a signature from the dealer.

silence. For simplicity, we firstly regard the one-shot recovering process in 2-out-of-2 secret sharing as a two-player strategic game in which each player has two actions (i.e., "B" and "S"). By identifying P_1's actions with the rows and P_2's with the columns, the game can be represented by the table in Figure 1, where $a, b, c, d \in \mathbb{R}$ denote player's utility under the corresponding action profile.

	B	S
B	b, b	d, a
S	a, d	c, c

Fig. 1. A strategic game of 2-out-of-2 secret sharing.

Specifically, the upright pair (d, a) means P_1 gets utility d and P_2 gets a under the action profile (B, S) (i.e., P_1 takes the action B, and simultaneously P_2 takes S). Obviously, the action profile (B, S) causes an outcome $(0, 1)$ that means P_2 gets the secret but P_1 does not. Based on our assumptions on the utility functions it evidently holds $a > b > c > d$.

A crucial problem arises in the above strategic game is that for each player the strategy B is *weakly dominated* by the strategy S. That is, no matter what strategy his opponent takes, a player taking the strategy S can get as much as and sometimes even higher utility than taking the strategy B. Hence a rational player has no incentive to broadcast his share in the one-shot recovery. The same problem also arises in the t-out-of-n secret sharing. To cover this problem, an usual way in rational secret sharing is to design a multi-stage process for recovering secret and introduce punishments of deviations. Thus we use the theory of *extensive games* to study the multi-stage secret-recovering process.

2.2 Extensive Game

Unlike strategic games in which all players simultaneously take actions once and for all, extensive games give a detailed description of the situations where players move sequentially. Based on the problem studied in this paper, we focus on the *extensive game with imperfect information and simultaneous moves* (or *extensive game*, in short).

Definition 1. *An* **extensive game** *consists of*

- *A finite set* $N = \{1, 2, ..., |N|\}$. *(the set of* players*)*
- *A set* H *of sequences. (the set of* histories*)*
  - *For any* $h = (a^k)_{k=1}^{L} \in H$, h *is called a* history *of length* L *(*L *might be* ∞*). Each component* a^k *is an action profile taken by the players whose turn it is to move at the* k*-th stage.*

  - *For any* $(a^k)_{k=1}^{L} \in H$ *and* $K < L$*, it holds* $(a^k)_{k=1}^{K} \in H$*. In particular, the empty sequence* $\emptyset \in H$*.*
  - *For any* $h \in H$*, the set of action profiles available after* h *is denoted by* $A(h) = \{a \mid (h, a) \in H\}$*. A history* h *is called* terminal *if* $A(h) = \emptyset$ *or the length of* h *is* ∞*. The set of terminal histories is denoted by* Z*.*
- *A function* $P : H \backslash Z \to 2^N \cup \{\mathfrak{c}\}$ *that assigns to each nonterminal history a subset of* N *or the chance* $\mathfrak{c}$*. (the* player function*)*
  - *Specifically,* $P(h) = A \subseteq N$ *means players in* A *simultaneously move at the stage right after the history* h*, and* $P(h) = c$ *means the chance determines the action taken after* h*.*
- *A function* $f_{\mathfrak{c}}$ *that associates with every history* h *for which* $P(h) = \mathfrak{c}$ *a probability measure* $f_{\mathfrak{c}}(\cdot \mid h)$ *on* $A(h)$*.*
- *For each player* $i \in N$*, a partition* $\mathcal{I}_i$ *of* $\{h \in H \mid i \in P(h)\}$ *with the property that* $A(h) = A(h')$ *whenever* h *and* h' *are in the same member of the partition. (*$\mathcal{I}_i$ *is the* information partition*; a set* $I_i \in \mathcal{I}_i$ *is an* information set*)*
- *For each player* $i \in N$*, a* utility function U_i *on the set of probability distributions over* Z*.*

Denote an extensive game by the tuple $< N, H, P, f_{\mathfrak{c}}, (\mathcal{I}_i), (U_i) >$. To illustrate components of an extensive game, we give a designed extensive game of 2-out-of-2 secret sharing in the following example. It can be used as a sub-protocol of our rational secret sharing scheme described in Section 3.

Example 1. First, with probability p the dealer chooses to share the real secret s between player 1 and 2, and with probability $1 - p$ shares an empty symbol $\perp$. After receiving shares, any single player has no idea whether s or $\perp$ has been shared. At the recovering phase, player 1 is supposed to move first and player 2 moves after observing 1's action. As described earlier, each player chooses from two actions B and S, and his utility may be a, b, c or d, sometimes plus an additional utility $\varepsilon > 0$ which can be regarded as the win of a good reputation by honestly broadcasting the share.

Regarding the dealer as the chance $\mathfrak{c}$, we model the above process by an extensive game as represented in Figure 2, where the game is described as a tree (with a dotted line). Every internal node denotes the chance or the player (sometimes the subset of players, if move simultaneously) taking actions at that stage, and each edge denotes an action. Here for simplicity, we use the probability p and $1-p$ respectively denote the chance $\mathfrak{c}$'s two possible actions *sharing* s and *sharing* $\perp$. Every path from the root to a leaf denotes a terminal history and the pair of numbers labeled below the leaf denotes the corresponding utility profile.

For instance, the path (p, B, S) denotes a history where c first shares s, then player 1 broadcasts his share, and finally player 2 keeps silence. This is a terminal history and causes the utility profile $(d + \varepsilon, a)$.

The dotted line connecting two nodes labeled by 1 means the two histories[2] (p) and $(1 - p)$ are in the same information set of player 1. That is, when

[2] In general, all paths starting from the root and ending at the same dotted line are in the same information set belonging to the player by which the dotted line is labeled.

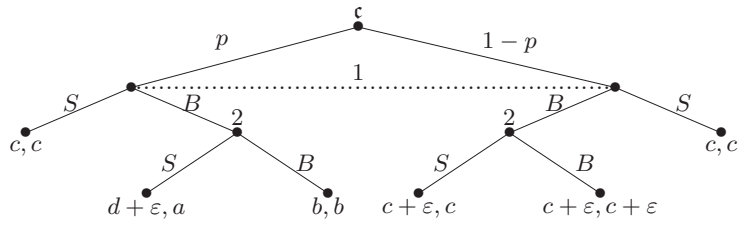

Fig. 2. An extensive game of 2-out-of-2 secret sharing.

the information set $I_1 = \{(p), (1-p)\}$ is reached, player 1 has no idea which history actually happened. For this reason, the extensive game is called the one with imperfect information. To illustrate, we give a complete description of the players' information partition:

$$\mathcal{I}_1 = \{\{(p), (1-p)\}\}, \quad I_2 = \{\{(p, B)\}, \{(1-p, B)\}\} \,. \tag{1}$$

Note that player 1 has one information set and player 2 has two information sets. Moreover, whenever player 2 is supposed to move, he always knows exactly which history has occurred because each of his information set contains only one history.

2.3 Sequential Equilibrium in Extensive Games

To describe players' strategy profiles in an extensive game, we need the concept of *assessment* defined below.

Definition 2. *An* **assessment** *in an extensive game is a pair (β, μ), where*

- $\beta = (\beta_i)_{i \in N}$ *is a profile of* behavior strategies. *Precisely, $\beta_i = (\beta_i(I_i))_{I_i \in \mathcal{I}_i}$ and $\beta_i(I_i)$ is a probability distribution over the set of actions available for player i right after the information set I_i being reached.*
- $\mu = (\mu_i)_{i \in N}$ *is a* belief system. *Precisely, $\mu_i = (\mu_i(I_i))_{I_i \in \mathcal{I}_i}$ and $\mu(I_i)$ is a probability distribution over the histories in I_i.*

Still see Example 1, we denote $\mathcal{I}_1 = \{I_1\}$ and $\mathcal{I}_2 = \{I_{21}, I_{22}\}$ corresponding to Eq.(1). Define an assessment (β, μ) as follows:

- $\beta_1(I_1) = (B : 1; S : 0)$, denoted as $\beta_1(I_1) = B$ for simplicity, i.e. player 1 chooses to take action B at reaching his information set I_1.
- $\beta_2(I_{21}) = S$, i.e. player 2 takes action S at reaching $I_{21} = \{(p, B)\}$.
- $\beta_2(I_{22}) = B$, i.e. player 2 takes action B at reaching $I_{22} = \{(1-p, B)\}$.
- $\mu_1(I_1) = (p, 1-p)$, meaning player 1 believes that the dealer shares s with probability p and shares $\perp$ with probability $1-p$.

– μ_2 is defined trivially.

A main object of game theory is to suggest the most possible outcomes that emerge in classes of games, or equivalently, to provide each player the most *reasonable* strategies. In strategic games, reasonable strategies are usually referred to as Nash Equilibria, correlated Equilibria, etc. In extensive games, a widely used candidate of reasonable strategies is the *sequential equilibrium* which is an extension of the *subgame perfect equilibrium* to the games with imperfect information.

Definition 3. *An assessment (β, μ) is a* **sequential equilibrium** *of an extensive game $< N, H, P, f_c, (\mathcal{I}_i), (U_i) >$, if it satisfies the following two conditions:*

1. *(β, μ) is sequentially rational: For every player $i \in N$ and every information set $I_i \in \mathcal{I}_i$, it holds*

$$U_i(\beta, \mu \mid I_i) \geq U_i((\beta_{-i}, \beta_i'), \mu \mid I_i) \text{ for every strategy } \beta_i' \text{ of player } i \ ,$$

   where (β_{-i}, β_i') is a strategy profile that all players stick to the strategy β except that player i turns to the strategy β_i', and $U_i((\beta_{-i}, \beta_i'), \mu \mid I_i)$ denotes player i's utility induced by this strategy profile and the belief system μ conditional on I_i being reached.
2. *(β, μ) is consistent: There exists a sequence $((\beta^n, \mu^n))_{n=1}^{\infty}$ of assessments that converges to (β, μ) in Euclidian space[3] 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.*

Since the second condition is trivially satisfied in our problem (see Appendix A), we skip this condition here and refer to book chapters (e.g. Chapter 12 of [16]) for its detailed explanations. The first condition is an extension of the requirement in a *subgame perfect equilibrium* that no player can benefit from deviations after any history. As an illustration, let's see Example 1 and the assessment (β, μ) given after Definition 2, i.e. $\beta_1(I_1) = B, \beta_2(I_{21}) = S, \beta_2(I_{22}) = B$ and $\mu_1(I_1) = (p, 1-p)$. For player 1,

$$U_1(\beta, \mu \mid I_1) = U_1((B, \beta_2), \mu \mid I_1) = (d+\varepsilon)p + (c+\varepsilon)(1-p) \ ,$$

$$U_1((S, \beta_2), \mu \mid I_1) = cp + c(1-p) = c \ .$$

It is easy to see if $(d+\varepsilon)p + (c+\varepsilon)(1-p) \geq c$, i.e. $\varepsilon \geq p(c-d)$, then the assessment is sequentially rational for player 1. Sequential rationality for player 2 is straightforward. Since the condition of consistency is trivially satisfied, thus (β, μ) is a sequential equilibrium of the extensive game.

[3] Assume each player's action set is finite and each information set contains finite number of histories, β and μ are probability distributions over finite sets and therefor can be seemed as tuples of nonnegative real numbers.

3 Extensive Game of 2-out-of-2 Rational Secret Sharing

In this section we design an extensive game for 2-out-of-2 rational secret sharing, and then prove a strategy that achieves secret recovery is a sequential equilibrium of this game under the mean payoff criterion.

3.1 The Game Model

Denote the player set by $N = \{1, 2\}$ and assume that the dealer is always honest. Our game model for 2-out-of-2 rational secret sharing consists of three kinds of subgames: $\mathsf{Norm}(k)$, $\mathsf{Puni}(1, t)$ and $\mathsf{Puni}(2, t)$, where the parameters k, t are positive integers. These subgames are explained below.

Subgame $\mathsf{Norm}(k)$, i.e. invocation of the normal recovery process in the k-th subgame, goes along the following steps:

N.1 With probability p the dealer chooses to share the real secret s between players 1 and 2, and with probability $1 - p$ shares an empty symbol $\perp$.
Note: A verifiable 2-out-of-2 secret sharing scheme can be used here. For simplicity, let the dealer secretly selects two random strings $s_1, s_2 \in \{0, 1\}^{|s|}$ such that $s_1 \oplus s_2 = s$ with probability p and $s_1 \oplus s_2 = \perp$ [4] with probability $1-p$. Then the dealer secretly sends to player i the share $(s_i, \mathsf{Sig}(s_i))$, where $\mathsf{Sig}(s_i)$ is the dealer's signature on s_i which is unforgeable.

N.2 When it is time for recovery, player 1 and 2 simultaneously broadcast the share. Then,
- if neither of the broadcast shares passes verification of the signature, then reset the clock and turn to Step N.2.
- if only player i's broadcast share passes verification of the signature, then i broadcasts a complaint that "*j cheats*".
- if both shares pass the verification, then both players compute XOR of the shares.
  - If the XOR is an empty symbol $\perp$, then broadcast a requirement "*once again*".
  - Otherwise, regard the XOR as the secret and broadcast the message "*quit*".

Subgame $\mathsf{Puni}(1, t)$, i.e. punishing player 1 for the t-th time, goes along the following steps:

P.1 With probability p the dealer chooses to share the real secret s and with probability $1 - p$ shares an empty symbol $\perp$, same as Step N.1.

P.2 When it is time for recovery, player 1 firstly broadcasts his share.
- If player 1's broadcast share does not pass verification, then reset the clock and go to Step P.2.

[4] The empty symbol $\perp$ can be regarded as strings in special forms. For example, assume that the secret is started with 1, then all strings started with 0 are identify with $\perp$.

P.3 If player 1's broadcast share passes verification, then player 2 broadcasts his share.
- If player 2 's broadcast share does not pass verification, then player 1 broadcasts a complaint "*2 cheats*".
- Otherwise, both players compute XOR of the shares.
  - If the XOR is an empty symbol $\perp$, then broadcast a requirement "*once again*".
  - Otherwise, regard the XOR as the secret and broadcast the message "*quit*".

Subgame $\mathsf{Puni}(2,t)$, i.e. punishing player 2 for the t-th time, is the same as $\mathsf{Puni}(1,t)$ except interchanging player 1 with player 2.

Note that in any of the three subgames, the dealer is involved only once, and the subgame ends with one of the four broadcast messages "1 cheats", "2 cheats", "once again" and "quit". Specifically, we require that the subgame ends only when at least one player's broadcast share passes the verification, otherwise it keeps asking the player or players broadcast share (i.e. reset the clock and go to Step P.2 or N.2).

The extensive game of 2-out-of-2 rational secret sharing, denoted as EG-$(2,2)\mathsf{RSS}$, consists of sequential invocations of the three subgames described above with a designed transition rule. It begins with repeated invocations of the subgame $\mathsf{Norm}(\cdot)$ where the players are required to simultaneously broadcast the share. Once a player i is complained for cheating, the game immediately turns to L repetitions of the subgame $\mathsf{Puni}(i,\cdot)$, where L is an positive integer to be determined later. During the L-period punishment, if no player deviates in $\mathsf{Puni}(i,\cdot)$, then after L repetitions the game returns to $\mathsf{Norm}(\cdot)$; otherwise, the game immediately turns to the L-period punishment of the deviant. Precisely, the game EG-$(2,2)\mathsf{RSS}$ is described as follows.

Game EG-$(2,2)\mathsf{RSS}$

E.1 Set $k \leftarrow 1$.

E.2 Execute subgame $\mathsf{Norm}(k)$.
- If end with "1 cheats", then set $k \leftarrow k+1$, $t \leftarrow 1$, and go to E.3.
- If end with "2 cheats", then set $k \leftarrow k+1$, $t \leftarrow 1$, and go to E.4.
- If end with "once again", set $k \leftarrow k+1$ and go to E.2.
- If end with "quit", then the game halts.

E.3 Execute subgame $\mathsf{Puni}(1,t)$.
- If end with "2 cheats", then set $k \leftarrow k+1$, $t \leftarrow 1$, and go to E.4.
- If end with "once again",
  - When $t < L$, set $k \leftarrow k+1$, $t \leftarrow t+1$, and go to E.3.
  - When $t = L$, set $k \leftarrow k+1$ and go to E.2.

E.4 Execute subgame $\mathsf{Puni}(2,t)$.
- If end with "1 cheats", then set $k \leftarrow k+1$, $t \leftarrow 1$, and go to E.3.
- If end with "once again",
  - When $t < L$, set $k \leftarrow k+1$, $t \leftarrow t+1$, and go to E.4.
  - When $t = L$, set $k \leftarrow k+1$ and go to E.2.

The game halts as soon as some player quits.

Figure 3 displays a tree representing the extensive game EG-$(2,2)$RSS, where the nodes $\mathfrak{c}, \mathfrak{c}_1$ and $\mathfrak{c}_2$ respectively represent the dealer in the subgames $\mathsf{Norm}(\cdot)$, $\mathsf{Puni}(1,\cdot)$ and $\mathsf{Puni}(2,\cdot)$. Since the game may have infinite length, it cannot be completely represented by a tree with finite length. Therefor, the hollow dots labeled by "$\mathfrak{c}$", "$\mathfrak{c}_1$" and "$\mathfrak{c}_2$" at the leaves correspond to transition to the subgame $\mathsf{Norm}(\cdot)$, $\mathsf{Puni}(1,\cdot)$ and $\mathsf{Puni}(2,\cdot)$ respectively. When the hollow dot is labeled by "$\mathfrak{c}$ or $\mathfrak{c}_1$" (resp. "$\mathfrak{c}$ or $\mathfrak{c}_2$"), it means whether it turns to $\mathsf{Norm}(\cdot)$ or $\mathsf{Puni}(1,\cdot)$ (resp. $\mathsf{Norm}(\cdot)$ or $\mathsf{Puni}(2,\cdot)$) depends on the punishment has been repeated for L periods or not. The hollow dots connected with its ancestor by an arc correspond to the cycles inside the subgames (i.e. players are required to reset the clock and broadcast shares again). The dark nodes at the leaves denote termination of the game.

For simplicity, we make the idleness-avoiding assumption about players:

Idleness-Avoiding Assumption. Assume that each player quits the game as soon as he gets the secret.

This assumption explains the dark dots at the leaves which denote termination of the game.

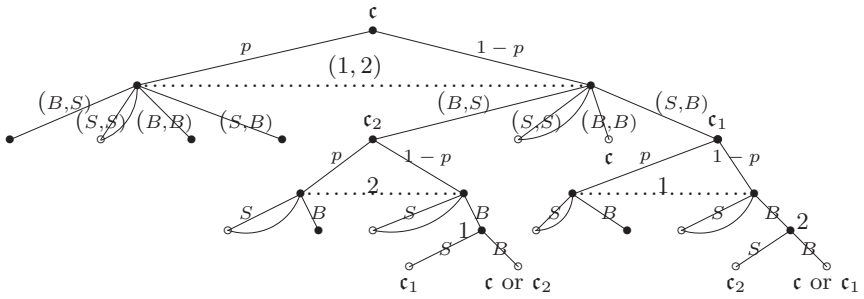

Fig. 3. Extensive game of 2-out-of-2 secret sharing.

According to Definition 1 of an extensive game $< N, H, P, f_{\mathfrak{c}}, (\mathcal{I}_i), (U_i) >$, the above descriptions have defined $N, H, P, f_{\mathfrak{c}}$ and $(\mathcal{I}_i)$ for the game EG-$(2,2)$RSS. In particular, the player function P is defined by the transition rule among the three kinds of subgames. Now it is left to define the utility function (U_i). Given a probability distribution $\mathsf{Prob}(\cdot)$ over the set of terminal histories Z, we define

$$U_i = \sum_{z \in Z} u_i(z)\mathsf{Prob}(z) \ , \tag{2}$$

where $u_i(z)$ denotes player i's utility along the terminal history z. To define $u_i(z)$ precisely, we adopt the methods used in repeated games. Details are as follows.

For any terminal history $z \in Z$ of the game EG-$(2,2)$RSS, let $k(z)$ denote the number of times that one of the three subgames Norm$(\cdot)$, Puni$(1,\cdot)$ and Puni$(2,\cdot)$ is invoked. Without confusion we call each invocation as a subgame. For $1 \leq l \leq k(z)$, let $u_i^l(z)$ denote player i's utility obtained in the l-th subgame. Refer to the utility values used in Section 2.1, we define

- $u_i^l(z) = a$ if only player i gets the secret in the l-th subgame.
- $u_i^l(z) = b$ if both players get the secret.
- $u_i^l(z) = c$ if neither players gets the secret.
- $u_i^l(z) = d$ if only player i does not get the secret.

Concerning mixed strategies that players may take, $u_i^l(z)$ is a convex combination of a, b, c, d, i.e. $u_i^l(z) \in \{\lambda_1 a + \lambda_2 b + \lambda_3 c + \lambda_4 d \mid \lambda_i \in \mathbb{R}_{\geq 0},\ \sum_{i=1}^4 \lambda_i = 1\}$.

By using the mean utility criterion, we define

$$u_i(z) = \frac{\sum_{l=1}^{k(z)} u_i^l(z)}{k(z)},\ \text{for any } z \in Z\ . \tag{3}$$

Combining Equation (2) and Equation (3), it gives a definition for the utility function in the game EG-$(2,2)$RSS.

3.2 A Sequential Equilibrium in EG-$(2,2)$RSS

Next we are to evaluate rationality of a strategy with respect to the concept of sequential equilibrium. According to Definition 3, it needs to compute the utility $U_i(\beta, \mu \mid I_i)$ for any assessment (β, μ) and information set I_i. From Figure 3 it is easy to see that any information set contains at most two histories. Moreover, the two histories in the same information set go through the same sequence of subgames. Thus for any information set I_i, let $k(I_i)$ denote the the number of finished subgames along any history in I_i. Thus $k(I_i)$ equals the current value of the parameter k minus 1 since the last subgame is unfinished at reaching I_i. Additionally, we *always* adopt *the trivial belief system* μ that at each information set containing two histories (denoted by the dotted lines in Figure 3) the player (or players) believes s was shared with probability p and $\perp$ was shared with probability $1-p$. Obviously, this trivial belief system is independent of players' strategies and is fixed in some sense. Therefor we omit the belief system in many places without confusion. In particular, denote $U_i(\beta \mid I_i) = U_i(\beta, \mu \mid I_i)$.

Lemma 1. *Under the mean utility criterion, for any strategy β and information set I_i in the game EG-$(2,2)$RSS,*

$$U_i(\beta \mid I_i) \in [\sum_{l=1}^{\infty} \frac{(l+k(I_i)-1)c+d}{l+k(I_i)}(1-p)^{l-1}, \sum_{l=1}^{\infty} \frac{(l+k(I_i)-1)c+a}{l+k(I_i)}(1-p)^{l-1}]\ .$$

Proof. Conditional on I_i being reached, we only need to consider the terminal histories that contain a history in I_i as a sub-history. Denote such terminal histories by $z : z \ni I_i$. From Equality (2) and (3), it has

$$U_i(\beta \mid I_i) = \sum_{z:z\ni I_i} u_i(z)\mathsf{Prob}_\beta(z|I_i) = \sum_{z:z\ni I_i} \frac{\sum_{l=1}^{k(z)} {u_i}^l(z)}{k(z)}\mathsf{Prob}_\beta(z|I_i) \ ,$$

where $\mathsf{Prob}_\beta(z|I_i)$ is the conditional probability of z induced by the strategy β.

For any terminal history $z : z \ni I_i$, it holds $k(z) \in (k(I_i), \infty)$. Firstly consider the case $k(z) < \infty$. Because of the idleness-avoiding assumption we can conclude that neither player gets the secret in the former $k(z)-1$ subgames. Furthermore, since each subgame ends only when at least one broadcast share passes the verification which means at least one player can recover the value shared by the dealer at that subgame, it must be the case that the dealer shares the empty symbol $\perp$ in the former $k(z) - 1$ subgames and ${u_i}^l(z) = c$ for $1 \le l < k(z)$. In the last subgame, both the case that s is shared and the case that $\perp$ is shared could happen. For example, if $\perp$ is shared, the game may also terminate if some player always chooses the action S taking the last subgame into an infinite cycle. In any case it is a trivial fact that $u_i^{k(z)}(z) \in [d, a]$.

For all the terminal histories $z : z \ni I_i$ with $k(z) < \infty$, we classify them according to the value of $k(z)$. Specifically, for $1 + k(I_i) \le l < \infty$, denote $z_l = \{z \in Z \mid I_i \in z,\ k(z) = l\}$. From analyze in the last paragraph, it follows that for any $z \in z_l$, $u_i(z) \in [\frac{(l-1)c+d}{l}, \frac{(l-1)c+a}{l}]$ and $\mathsf{Prob}_\beta(z_l|I_i) = (1-p)^{l-k(I_i)-1}$. When $k(z) = \infty$, it still has $u_i(z) \in [d, a]$, and $\mathsf{Prob}_\beta(z|I_i) = (1-p)^\infty = 0$. Hence,

$$U_i(\beta \mid I_i) = \sum_{z:z\ni I_i} u_i(z)\mathsf{Prob}_\beta(z|I_i) = \sum_{l=1+k(I_i)}^{\infty} u_i(z_l)\mathsf{Prob}_\beta(z_l|I_i) \ ,$$

and the lemma follows immediately.

Proposition 1. *(The one deviation property) In the game EG-$(2,2)$RSS, an assessment (β, μ) is a sequential equilibrium if and only if it satisfies the one deviation property, that is, for any $i \in N$ and any information set $I_i \in \mathcal{I}_i$, $U_i(\beta_i', \beta_{-i} \mid I_i) \le U_i(\beta_i, \beta_{-i} \mid I_i)$ for any β_i' which is a one-period deviation from β_i at I_i, i.e. $\beta_i'(I_i) \ne \beta_i(I_i)$ and $\beta_i'(I_i') = \beta_i(I_i')$ for any $I_i' \ne I_i$.*

Proof. The necessity is straightforward from Definition 3. Now we prove the sufficiency. Suppose that (β, μ) satisfies the one deviation property. On the contrary, assume that (β, μ) is not a sequential equilibrium. Since the consistency condition is trivially satisfied (see Appendix A), it implies that (β, μ) is not sequentially rational, i.e. there exists a player i and an information set I_i such that

$$U_i(\beta_i', \beta_{-i} \mid I_i) > U_i(\beta_i, \beta_{-i} \mid I_i) \text{ for some } \beta_i' \ne \beta_i \ .$$

By Lemma 1, $U_i(\beta_i', \beta_{-i} \mid I_i) \in [\sum_{l=1}^{\infty} \frac{(l+k(I_i)-1)c+d}{l+k(I_i)}(1-p)^{l-1}, \sum_{l=1}^{\infty} \frac{(l+k(I_i)-1)c+a}{l+k(I_i)}(1-p)^{l-1}]$. Because both $\frac{(l+k(I_i)-1)c+d}{l+k(I_i)}(1-p)^{l-1}$ and $\frac{(l+k(I_i)-1)c+a}{l+k(I_i)}(1-p)^{l-1}$ converge to 0 as l grows to ∞, it follows that when $k(z)$ is sufficiently large the utility

$u_i(z)$ that comes along the history z does not influence the utility $U_i(\beta_i', \beta_{-i} \mid I_i)$ too much. Specifically, for any $\epsilon > 0$, there exists a positive integer T. Define a strategy β_i'' as follows

$$\begin{cases} \beta_i''(I_i') = \beta_i'(I_i') & \text{for any } I_i' \text{ with } k(I_i') \leq T \\ \beta_i''(I_i') = \beta_i(I_i') & \text{for any } I_i' \text{ with } k(I_i') > T \ . \end{cases}$$

Then it holds that $|U_i(\beta_i'', \beta_{-i} \mid I_i) - U_i(\beta_i', \beta_{-i} \mid I_i)| < \epsilon$. By choosing ϵ properly, we can have

$$U_i(\beta_i'', \beta_{-i} \mid I_i) > U_i(\beta_i, \beta_{-i} \mid I_i) \ .$$

Thus β_i'' is also a profitable deviation from β_i and it differs from β_i only before the $(T+2)$-th subgame. Thus $\beta_i''(I_i') \neq \beta_i(I_i')$ for finitely many I_i's. Let β_i'' be such profitable deviation that differs from β_i at the minimal number of I_i's. Let I_i'' be the information set such that $\beta_i''(I_i'') \neq \beta_i(I_i'')$ while $\beta_i''(I_i') = \beta_i(I_i')$ for any I_i' with $k(I_i') > k(I_i'')$. We claim that

$$U_i(\beta_i'', \beta_{-i} \mid I_i'') > U_i(\beta_i, \beta_{-i} \mid I_i'') \ .$$

Otherwise we can modify β_i'' at the information set I_i'' and get a profitable deviation which differs from β_i at fewer information sets than β_i'' does. This contradicts the selection of β_i''.

Finally, since it already has that $\beta_i''(I_i'') \neq \beta_i(I_i'')$ and $\beta_i''(I_i') = \beta_i(I_i')$ for any I_i' with $k(I_i') > k(I_i'')$, we construct a strategy $\tilde{\beta}_i$ such that $\tilde{\beta}_i(I_i'') = \beta_i''(I_i'')$ and $\tilde{\beta}_i(I_i') = \beta_i(I_i')$ for any $I_i' \neq I_i''$. It follows that

$$U_i(\beta_i'', \beta_{-i} \mid I_i'') = U_i(\tilde{\beta}_i, \beta_{-i} \mid I_i'')$$

because the utility conditional on I_i'' being reached is independent of the actions taken at the information set $I_i' \neq I_i''$ with $k(I_i') \leq k(I_i'')$, and for I_i' with $k(I_i') > k(I_i'')$ it holds $\tilde{\beta}_i(I_i') = \beta_i(I_i') = \beta_i''(I_i')$.

Evidently $\tilde{\beta}_i$ is a profitable one-period deviation from β_i at the information set I_i'', which contradicts the hypothesis that (β, μ) satisfies the one deviation property. Hence the assumption is not true and (β, μ) is a sequential equilibrium.

Proposition 1 provides an easy way to check the sequential rationality of a strategy in the game EG-$(2,2)\mathsf{RSS}$. In the following, we describe a strategy (denoted as Strategy A) for the game and then prove it is a sequential equilibrium along with the trivial belief system μ.

Strategy A For $i \in N = \{1, 2\}$,

- whenever player i is supposed to move in a subgame $\mathsf{Norm}(\cdot)$, he always takes the action "B".
- whenever player i is supposed to move in a subgame $\mathsf{Puni}(i, \cdot)$, he always takes the action "B".
- whenever player i is supposed to move in a subgame $\mathsf{Puni}(j, \cdot)$, he first computes the XOR of his share and the share broadcasted by player j that has passed the verification,

- if the XOR is $\perp$, then player i takes the action "B".
- otherwise, player i takes the action "S".

Proposition 2. *For sufficiently large L and sufficiently small p, Strategy A along with the trivial belief system μ is a sequential equilibrium of the game EG-$(2,2)\mathsf{RSS}$ under the mean utility criterion.*

Proof. By Proposition 1, we only need to prove that Strategy A satisfies the one deviation property. Denote Strategy A by β. For any $i \in N$ and any information set $I_i \in \mathcal{I}_i$, conditional on I_i being reached, $k(I_i)$ subgames have been finished with no one getting the secret. The proof is given according to the kind of the $(k(I_i)+1)$-th subgame.

(1) The $(k(I_i)+1)$-th subgame is $\mathsf{Norm}(k(I_i)+1)$.

Suppose that player i sticks to β_i and the other player sticks to β_{-i}, then implementation of the game will continue with $\mathsf{Norm}(k(I_i)+1)$, $\mathsf{Norm}(k(I_i)+2)$,..., and terminate as soon as the dealer shares the real secret at some subgame. In each of these subgames player i gets utility c except that in the last subgame i gets b. By Lemma 1, we have

$$U_i(\beta_i, \beta_{-i} \mid I_i) = \sum_{l=1}^{\infty} \frac{(k(I_i)+l-1)c+b}{k(I_i)+l}(1-p)^{l-1}p\ .$$

suppose that player i turns to a one-period deviation strategy β_i' at I_i while the other player sticks to β_{-i}. Without loss of generality, we may assume that $\beta_i'(I_i) = S$ and $\beta_i'(I_i') = \beta_i(I_i')$ for any $I_i' \neq I_i$. That is, we only need to consider the one-period deviation to the pure strategy. Because utilities under mixed strategies are probability distributions over utilities under pure strategies, and there are only two pure strategies in our game, thus proofs for the mixed strategies can be easily derived from this proof for the pure strategies. By taking the strategy (β_i', β_{-i}), implementation of the game will continue with $\mathsf{Norm}(k(I_i)+1)$, $\mathsf{Puni}(i,1)$,...,$\mathsf{Puni}(i,L)$, $\mathsf{Norm}(k(I_i)+L+2)$,$\mathsf{Norm}(k(I_i)+L+3)$,..., and terminate as soon as the dealer shares the real secret at some subgame. If $\mathsf{Norm}(k(I_i)+1)$ is the termination, i gets a higher utility a in this subgame. If $\mathsf{Puni}(i,\cdot)$ is the termination, i gets a lower utility d. More precisely, we have

$$\begin{aligned} U_i(\beta_i', \beta_{-i} \mid I_i) = \frac{k(I_i)c+a}{k(I_i)+1}p + \sum_{l=2}^{L+1} \frac{(k(I_i)+l-1)c+d}{k(I_i)+l}(1-p)^{l-1}p \\ + \sum_{l=L+2}^{\infty} \frac{(k(I_i)+l-1)c+b}{k(I_i)+l}(1-p)^{l-1}p\ . \end{aligned} \tag{4}$$

For consistency, we write

$$\begin{aligned} U_i(\beta_i, \beta_{-i} \mid I_i) = \frac{k(I_i)c+b}{k(I_i)+1}p + \sum_{l=2}^{L+1} \frac{(k(I_i)+l-1)c+b}{k(I_i)+l}(1-p)^{l-1}p \\ + \sum_{l=L+2}^{\infty} \frac{(k(I_i)+l-1)c+b}{k(I_i)+l}(1-p)^{l-1}p\ . \end{aligned} \tag{5}$$

In order to make β satisfy sequential rationality at I_i, it requires

$$U_i(\beta_i', \beta_{-i} \mid I_i) \leq U_i(\beta_i, \beta_{-i} \mid I_i) \tag{6}$$

By Equality (4) and (5), it is equivalent to require

$$\frac{a-b}{b-d} \leq \sum_{k=1}^{L} \frac{(1-p)^k}{\frac{k}{1+k(I_i)}+1} .$$

Since the inequality (6) is required to hold for any I_i, it is sufficient to require the above inequality hold for $k(I_i) = 0$. That is, it requires $\frac{a-b}{b-d} \leq \sum_{k=1}^{L} \frac{(1-p)^k}{k+1}$. Let L be sufficiently large, it holds $\sum_{k=1}^{L} \frac{(1-p)^k}{k+1} \geq \sum_{k=1}^{\infty} \frac{(1-p)^k}{k+1} - \epsilon$ for some $\epsilon > 0$. Because

$$\sum_{k=1}^{\infty} \frac{(1-p)^k}{k+1} = \frac{1}{1-p}(\sum_{k=1}^{\infty} \frac{(1-p)^k}{k} - 1 + p) = \frac{1}{1-p}(-\ln p - 1 + p) > -\ln p - 1.$$

Thus when $-\ln p - 1 > \frac{a-b}{b-d}$, i.e. $p < e^{-1-\frac{a-b}{b-d}}$, it has $\sum_{k=1}^{\infty} \frac{(1-p)^k}{k+1} > \frac{a-b}{b-d}$. Let $\epsilon = \sum_{k=1}^{\infty} \frac{(1-p)^k}{k+1} - \frac{a-b}{b-d}$ and choose L sufficiently large so that $\sum_{k=1}^{L} \frac{(1-p)^k}{k+1} \geq \sum_{k=1}^{\infty} \frac{(1-p)^k}{k+1} - \epsilon$, the inequality (6) is satisfied.

(2) The $(k(I_i)+1)$-th subgame is $\mathsf{Puni}(i,t)$ for some $1 \leq t \leq L$.

If player i deviates from β_i and turns to take the action S, then it only postpones recovering of the secret and cannot increase i's utility.

(3) The $(k(I_i)+1)$-th subgame is $\mathsf{Puni}(j,t)$ for some $1 \leq t \leq L$.

It is obvious that any one-period deviation from β_i in this case cannot be profitable.

In conclusion, for $p < e^{-1-\frac{a-b}{b-d}}$ and L sufficiently large so that $\sum_{k=1}^{L} \frac{(1-p)^k}{k+1} \geq \sum_{k=1}^{\infty} \frac{(1-p)^k}{k+1} - (\sum_{k=1}^{\infty} \frac{(1-p)^k}{k+1} - \frac{a-b}{b-d})$, strategy A (i.e. β) satisfies the one deviation property and thus is a sequential equilibrium along with the trivial belief system.

It can see that sticking to strategy A makes both players finally get the secret and the expected running time is a constant. Moreover, it has proved the strategy is a sequential equilibrium. Thus the game model EG-$(2,2)\mathsf{RSS}$ along with strategy A turns out to be a 2-out-of-2 rational secret sharing scheme.

4 Some Further Issues

To accomplish this work of rational secret sharing, we need to consider some further issues. Some immature viewpoints are displayed below.

4.1 Dealer Off-line

In the model of EG-$(2,2)\mathsf{RSS}$ described in Section 3.1, it involves the dealer-distributing step in every subgame. That is, it needs a online dealer throughout

the game. But in practice the online dealer assumption is usually unrealistic. In order to make the dealer off-line after the initial phase, we adopt the method proposed in [4] and use one-way trapdoor permutations as primitives.

More precisely, for $i \in N = \{1, 2\}$, let f_i, g_i be one-way trapdoor permutations with the trapdoor held by player i and the dealer. Thus both the dealer and player i can invert the one-way functions f_i and g_i. Let h_{f_i}, h_{g_i} respectively be the hard-core predicates (refer to [6] for definitions) of f_i, g_i. Suppose the secret $s \in \{0, 1\}^l$ and let y be a public element in the domain of f_i, g_i. Then our game model EG-$(2, 2)$RSS is modified as follows.

Add an initial phase where the dealer secretly selects an integer $i^* \in \{1, 2, ...\}$ according to a geometric distribution with parameter p [5]. Then the dealer distributes to P_i the share $s \oplus (f_j^{-(i^*-1)l-1}(y), ..., f_j^{-(i^*-1)l-l}(y))$ and the index message $(g_j^{-(i^*-1)l-1}(y), ..., g_j^{-(i^*-1)l-l}(y))$. Then the dealer leaves the game.

The game still goes along the transition rule among the three kinds of subgames Norm$(\cdot)$, Puni$(1, \cdot)$ and Puni$(2, \cdot)$, except that in each of the subgame, the first step involving dealer distributing shares is deleted and in the k-th subgame player i is required to broadcast the message $(f_i^{-(k-1)l-1}(y), ..., f_i^{-(k-1)l-l}(y))$ and $(g_i^{-(k-1)l-1}(y), ..., g_i^{-(k-1)l-l}(y))$. Verification can be easily done since y is public and the functions f_i, g_i is publicly computable. If the verification is passed, then compare the second broadcast message with the index message distributed at the initial phase. If they are coincide, then $i^* = k$ and the secret can be recovered from the first broadcast message and the initial share; otherwise, it is like that the dealer shares $\perp$ in the k-th subgame and the game continues according to the transition rule.

4.2 Simultaneous Broadcast

Like many previous rational secret sharing schemes [8, 7, 1, 13], our model also relies on the existence of a simultaneous broadcast channel. Because in the subgame Norm$(\cdot)$ both players are required to broadcast share simultaneously, and the player who postpones his broadcast message at this round will be punished in the next subgame. It can see that our punishment rule relies upon the simultaneous broadcast channel. How to build a rational secret sharing scheme in an extensive game model without the simultaneous broadcast channel deserves further research.

4.3 Extension to t-out-of-n Rational Secret Sharing

To consider the t-out-of-n rational secret sharing in an extensive game model, we need first define the *k-resilient* sequential equilibrium. Intuitively, it requires that after any history all players stick to the original strategies except that a group

[5] That is, let p be the probability that the bit 1 is chosen between 0 and 1 in one trial. Execute such trial repeatedly and independently, then the bit 1 is chosen in the i^*-th trial for the first time.

of k players collaborate to deviate, but the utility of any one of the k deviants cannot be increased. To adapt our game model to the t-out-of-n case, the key point is how to make a reasonable punishment rule for the case that there are $k > 1$ players cheat in a subgame. A possible solution is that the $n - k$ players jointly determine a random order on the k deviants and in the next round the k deviants are required to broadcast messages according to this order first. If no one cheats then the rest $n - k$ players are required to broadcast simultaneously, otherwise the game turns to the punishment for the new deviants. Also we should carefully determine the periods L that a punishment lasts for and the probability p with which every subgame results in a real recovery.

4.4 Computational Equilibrium

Another important issue is that we should consider computational equilibria in cryptographic protocols. In our model, verification of the broadcast messages depends on a signature algorithm $\mathsf{Sig}(\cdot)$ and the online dealer is removed by one-way trapdoor permutations. Because of these it is better for us to consider computational issues when defining sequential equilibria. Refer to the concepts of computational equilibria proposed in previous work [4, 11], we can define an efficient strategy to be sequentially rational in the computational setting if *after any history* any efficient deviation of a single player can bring a profit of at most $\epsilon(k)$, where $\epsilon(k)$ is a negligible function. It can see that Strategy A given in Section 3.2 in our game model satisfies this requirement. Katz [10] gave a further consideration for defining subgame perfect equilibrium (or sequential equilibrium) in the computational setting. He proposed that the probability a history happens should be considered in this definition instead of requiring rationality *after any history*. But the rational world is quite complicated and the bounded rationality could frequently give rise to unexpected results, thus defining sequential rationality properly in the computational setting is difficult and still has a long way to go.

5 Conclusion

This paper studies rational secret sharing in an extensive game model and designs a scheme which is proven to be a sequential equilibrium of the game. Discussions of rationality in extensive games are more complicated than that in strategic games. For simplicity, the scheme in this paper is built assuming existence of a simultaneous broadcast channel and we just provides loose considerations about k-resilience and computational equilibria. This is a beginning work in modeling rational secret sharing precisely in extensive games, and there remains much work deserving further research.

References

1. I. Abraham, D. Dolev, R. Gonen, J. Halpern : Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computa-

tion. In: 25th ACM Symposium Annual on Principles of Distributed Computing, pp. 53C62. ACM Press, New York (2006)
2. G.R. Blakley, Safeguarding cryptographic keys, Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies Proceedings 48: 313-317, 1979.
3. Y. Dodis, T. Rabin : Cryptography and game theory. In: Nisan, N., Roughgarden, T., Tardos, E., Vazirani, V. (eds.) Algorithmic Game Theory, pp. 181C207. Cambridge University Press, Cambridge (2007).
4. G. Fuchsbauer, J. Katz, D. Naccache, Efficient Rational Secret Sharing in Standard Communication Networks. TCC 2010, LNCS 5978, pp. 419C436, 2010.
5. D. Fudenberg, J. Tirole. Game Theory. MIT Press, 1992.
6. O. Goldreich, Foundations of Cryptography I: Basic Tools, Cambridge University Press, 2001.
7. S.D. Gordon, J. Katz, Rational secret sharing, revisited. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 229C241. Springer, Heidelberg (2006)
8. J. Halpern and V. Teague. Rational secret sharing and multiparty computation. In Proc. of 36th STOC, pages 623–632. ACM Press, 2004.
9. J. Katz : Bridging game theory and cryptography: Recent results and future directions. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 251C272. Springer, Heidelberg (2008)
10. J. Katz: Ruminations on defining rational MPC. Talk given at SSoRC, Bertinoro, Italy (2008), http://www.daimi.au.dk/ jbn/SSoRC2008/program.
11. G. Kol, M. Naor, Cryptography and game theory: Designing protocols for exchanging information. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 320–339. Springer, Heidelberg (2008)
12. G. Kol, M. Naor, Games for exchanging information. In: STOC 2008, pp. 423C432. ACM, New York.
13. A. Lysyanskaya, N. Triandopoulos: Rationality and adversarial behavior in multi-party computation. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 180–197. Springer, Heidelberg (2006)
14. S. Maleka, A. Shareef, C. Pandu Rangan, Rational secret sharing with repeated games, ISPEC 2008, LNCS 4991, pp. 334C346, 2008.
15. S.J. Ong, D.V. Parkes, A. Rosen, A. Vadhan, Fairness with an honest Minority and a rational majority, TCC 2009, LNCS 5444, pp. 36-53, 2009.
16. M. Osborne, A. Rubinstein, A Course in Game Theory, MIT Press, Cambridge (2004).
17. A. Shamir, How to share a secret, Communications of the ACM, 22(11), pp. 612-613, 1979.

A Appendix: Consistency

An important condition that a sequential equilibrium must hold is about *consistency*: i.e. (β, μ) is consistent if

There exists a sequence $((\beta^n, \mu^n))_{n=1}^{\infty}$ *of assessments that converges to* (β, μ) *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.*

Specifically, a strategy is completely mixed if it assigns each possible action a nonzero probability. Bayes' rule states the relation between posterior probabilities and prior probabilities. Here it defines the consistency between the belief system and the strategies taken previously.

We claim the consistency condition is trivially hold in the extensive games of rational secret sharing we discussed in this paper. The reason is that the nontrivial beliefs are always due to the chance's actions which are taken with a fixed and publicly known probability distribution.

To illustrate this, see Example 1 and the assessment (β, μ) given after Definition 2. Let $\{\epsilon_n\}$ be a sequence of positive real numbers which converge to 0 as n grows to infinity. Define

- $\beta_1^n(I_1) = (B : 1 - \epsilon_n;\ S : \epsilon_n)$.
- $\beta_2^n(I_{21}) = (B : \epsilon_n;\ S : 1 - \epsilon_n)$.
- $\beta_2^n(I_{22}) = (B : 1 - \epsilon_n;\ S : \epsilon_n)$.
- $\mu^n = \mu$.

It is easy to see that the strategy β^n is completely mixed and (β^n, μ^n) converges to (β, μ). Also, β^n and μ^n coincide with Bayes' rule Because the nontrivial beliefs (i.e., beliefs on the information set which contains more than one history) of μ^n are independent of the strategy β^n, and are only caused by the chance's action which is determined by the publicly known probability distribution function f_c (see Definition 1).