Rational Secret Sharing with Repeated Games

Shaik Maleka, Amjed Shareef, and C. Pandu Rangan*

Department of Computer Science and Engineering,
Indian Institute of Technology Madras, Chennai, India
{maleka.smile, amjedshareef}@gmail.com, rangan@cse.iitm.ernet.in

Abstract. This paper introduces the *Repeated Rational Secret Sharing* problem. We borrow the notion of *rational secret sharing* from Halpern and Teague[1], where players prefer to get the secret than not to get the secret and with lower preference, prefer that as few of the other players get the secret. We introduce the concept of repeated games in the rational secret sharing problem for the first time, which enables the possibility of a deterministic protocol for solving this problem. This is the first approach in this direction to the best of our knowledge. We extend the results for the mixed model (synchronous) where at most t players can be malicious. We also propose the first asynchronous protocol for rational secret sharing.

Keywords: Secret sharing, game theory, repeated games, distributed computing.

1 Introduction

Secret sharing is a widely known primitive in modern cryptography. More formally, in a secret sharing scheme there is a unique player called the *dealer* (player 0) who wants to share a secret s among n players, $p_1, \ldots, p_n$. The dealer sends every player a share of the secret in a way that any group of m (threshold value) or more players can together reconstruct the secret but no group of fewer than m players can. Such a system is called an (m, n)-threshold scheme.

Shamir's Secret Sharing Scheme[2] is based on the fact that, it takes m points to define uniquely a polynomial of degree $(m-1)$. The idea is that the dealer who shares the secret among the players, chooses a random $(m-1)$ degree polynomial f, such that $f(0) = s$, and sends the shares to the players such that every player p_i, $i = 1, \ldots, n$ receives the share $f(i)$. Any m players can recover the secret by reconstructing the polynomial through Lagrange's Interpolation. Any subset of players of size less than m cannot reconstruct the polynomial (even if they have infinite computing power).

1.1 Game Theory in Secret Sharing

Game theory provides a clean and effective tool to study and analyze the situations where decision-makers interact in a competitive manner. Game theoretic

* Work supported by Microsoft Project No. CSE0506075MICOCPAN on Foundation Research in Cryptology.

L. Chen, Y. Mu, and W. Susilo (Eds.): ISPEC 2008, LNCS 4991, pp. 334–346, 2008.

reasoning takes into account, which strategy is the best for a player with respect to every other player's strategy. Thus, the goal is to find a solution that is the best for all the players in the game. Every player's decision is based on the decision of every other player in the game and hence, it is possible to reach the equilibrium state corresponding to the global optima.

In distributed computing or secret sharing or multi-party computation, the players are mostly perceived as either honest or malicious players. An honest player follows the protocol perfectly whereas a malicious player behaves in an arbitrary manner. Halpern and Teague[1] introduced the problem of *secret sharing* assuming that the players are rational, which is known as *rational secret sharing*. In rational secret sharing, player's behavior is selfish. They have their own preferences and utility function (the profit they get). They always try to maximize their profits and behave accordingly.

For any player p_i, let w_1, w_2, w_3, w_4 be the payoffs obtained in the following scenarios.

w_1	–	p_i gets the secret, others do not get the secret
w_2	–	p_i gets the secret, others get the secret
w_3	–	p_i does not get the secret, others do not get the secret
w_4	–	p_i does not get the secret, others get the secret

The preferences of p_i is specified by $w_1 > w_2 > w_3 > w_4$. In brief, every player primarily prefers to get the secret than to not get it and secondarily, prefers that the fewer of the other players that get it, the better. The least preferred scenario for p_i is the situation, where he does not get the secret and others get it. A rational player follows the protocol only if it increases his expected utility.

1.2 Related Work

Consider any arbitrary player, say p_i. He needs $(m-1)$ shares from others to compute the secret. If other players (at least $(m-1)$) send him their shares, then he gets the secret, otherwise he cannot. This does not depend on whether he sends his share to others or not, as all the players are assumed to send their shares simultaneously. So, there is no incentive for any player to send his share. Reasoning in a similar way, no player might send his share. This impossibility result is proved by Halpern and Teague[1]. They show that rational secret sharing is not possible with any mechanism that has a fixed running time by iterated deletion of weakly dominated strategies (the strategy of not sending the share weakly dominates the strategy of sending the share). They also proposed a randomized protocol for $n \geq 3$. All these results apply to multi-party computation. Gordon and Katz[3] improved the original protocol and additionally they proposed a protocol for $n = 2$ for rational secret sharing and rational multi-party computation. Abraham *et.al.* [4] analyzed rational secret sharing and rational multi-party computation in an extended setting where players can form coalitions. They use a trusted third party as mediator. Lysyanskaya and Triandopoulos[5] analyzed multi-party computation in mixed behavior model, where players are rational or malicious using a trusted mediator. The malicious adversary can control at most $(\lceil n/2 \rceil - 2)$ players. Recently, Maleka et al.[6]

proposed a deterministic protocol for rational secret sharing by modifying the existing protocol. They did little variation in the model, where dealer instead of sending shares to the players, sends subshares of the shares.

1.3 Practical Applications and Motivation

Game theory has wide range of applications in Political science, Economics, business, Biology and Computer science (online algorithms). By combining game theory and cryptography, we can solve game theoretic problems as shown by Dodis et. al[7] and cryptography can be understood from a different perceptive. Secret sharing has many applications like, need for the secret to keep in distributed environment (arises if the storage is not reliable and there is a high chance that the secret may be lost). Analogously, if the owner of the secret does not trust any single person, there is a threat that the secret may be misused. Hence, the secret needs to be distributed among the members of a group to achieve shared trust. The secret can provide access to important files or critical resources like bank vault, missile launch pad, source code escrow, etc. In short, to all the applications, which need simultaneously achieving secrecy, availability and group trust.

Rational secret sharing has applications in highly competitive real world scenario, where players are modeled selfish. Suppose by obtaining the secret, players start their firm with it (or run online business activity), then they think that, if many persons learn the secret then they will become competitors to him and finally minimize his profit or payoff. A player gets maximum profit if only he runs the firm having the secret and no one else has the secret. So, every player behaves non-cooperatively, i.e., selfishly. We answer this question affirmatively and provide a solution.

In several practical situations, a group of people may wish to share many number of different secrets. Such scenario generally arises in applications where the key (secret) becomes obsolete after a predefined time limit. We model this as a secret sharing game, which is being played many number of times. Hence, this game can be treated as a *repeated game*. In each game, players share only one secret (not multiple secrets as in *multi-secret sharing*[8]). Thus, applying the game theory concepts (rational behavior and repeated games), we extend the work of Halpern and Teague[1] and introduce the *Repeated Rational Secret Sharing (RRSS)* problem.

1.4 Intuition and Contribution

Our intuition is that, the rational players have an incentive to send their share in repeated games by means of punishment strategy. If a player does not cooperate by not sending a share in the current game, then other players adopt the punishment strategy and do not send him the share in the further games. Hence, every player because of the fear of not receiving any share from other players in the further games will cooperate in the current game. Thus, the punishment strategy acts as an incentive for a player to cooperate. The major contribution of our work is that we present the first deterministic protocol for rational secret

sharing with repeated games. In an infinitely played repeated game or finitely played repeated game (where players do not know how many times the game will be repeated), we propose a deterministic protocol in both synchronous and asynchronous models. We prove that secret sharing is not possible for finitely played repeated games, where players know how many times the game will be repeated. We extend these results to mixed model (synchronous) where there can be few malicious players.

1.5 Model and Assumptions

We model the secret sharing as a game, denoted by Γ. The players of the game are rational and the game will be repeated for several times. We consider the scenario where m players come together and share the secrets repeatedly. That is, we solve the problem when m players come together to play the secret sharing game Γ repeatedly (the same set of m players). We do not consider the case where every time a new (different) set of players come and repeatedly play the game. Unlike the game defined by Halpern and Teague[1], our model considers both synchronous and asynchronous rational secret sharing and proposes a deterministic protocol. In the synchronous model, the game is finite with respect to time and the starting and ending points are precisely defined. The game proceeds in the following manner. The game starts when the dealer distributes the shares and the players send their shares simultaneously at a predefined synchronized point of time and ends in finite time at another synchronized point of time. Thus, the game has two possible outcomes, either players learn the secret or do not. In short, the game has only one round. On the contrary, in the asynchronous model, the game does not start and end at predefined points of time and has only two possible outcomes as that of the synchronous model.

We assume that all players are connected to each other through secure private channels independently, which ensures that a player can send his share to a selected number of players. Initially, we make an assumption that the underlying network is synchronous and the messages will be delivered in fixed amount of time. Later we consider the asynchronous model. Here, the message delivery time is indefinite. But, in both cases, the communication is guaranteed. In synchronous model, all the players are synchronized with respect to a global clock. Hence, all the players start and end the game at the same time whereas in asynchronous model, there does not exist a global clock. The dealer authenticates the shares, and therefore a player cannot send incorrect value as a share to other players. All the players are assumed to be computationally bounded. There is no trusted mediator and the dealer is assumed to be honest (so, he will not send different messages to different players). We also assume that the players are patient enough and care for their future payoff, hence we assume that the discount factor δ is sufficiently large and closer to 1.

1.6 Paper Outline

In the next section, we briefly explain the basics of Game Theory. Section 3 presents the protocol for the RRSS game, played both infinitely and finitely.

Section 4 discusses the mixed model where few malicious players are also present. Section 5 proposes a protocol for Asynchronous repeated rational secret sharing. Finally, Section 6 concludes the paper and gives an insight on open problems in further direction.

2 Basics of Game Theory

We define some basic terminology of game theory in this section [9].

A *strategy* can be defined as a complete algorithm for playing the game, implicitly listing all moves and counter-moves for every possible situation throughout the game. And a *strategy profile* is a set of strategies for each player which fully specifies all actions in a game. A strategy profile must include one and only one strategy for every player.

Let $\Gamma(N, L, U)$ represents an n persons game, where N is a finite set of n players $(p_1, \ldots p_n)$, $L = \{L_1, \ldots, L_n\}$ is a set of actions for each player p_i, $i \in \{1, \ldots, n\}$ and $U = \{u_1, \ldots, u_n\}$ is a utility function for each player, where $u_i : L{->}\mathrm{R}$

Let a_{-i} be a strategy profile of all players except for the player p_i. When each player p_i, $i \in \{1, \ldots, n\}$ chooses strategy $a_i \in L$ resulting in strategy profile $a = \{a_1, \ldots, a_n\}$, then player p_i obtains payoff $u_i(a)$. Note that, the payoff depends on the strategy profile chosen, i.e., on the strategy chosen by player p_i as well as the strategies chosen by all the other players.

Definition 1. (Strict Domination): In a strategic game with ordinal preferences, player p_i's action $a'' \in L_i$ strictly dominates his action $a' \in L_i$ if

$u_i(a'', a_{-i}) > u_i(a', a_{-i})$ for every list L_{-i} of the other players' actions.

We say that the action $a^{'}$ is strictly dominated.

Definition 2. (Nash Equilibrium - NE): A strategy profile $a^* \in L$ is a Nash equilibrium (NE) if no unilateral deviation in strategy by any single player is profitable, that is

$$\forall i, u_i(a_i^*, a_{-i}^*) \geq u_i(a_i, a_{-i}^*).$$

2.1 Repeated Games

Repeated games capture the idea that a player can condition his future game's move based on the previous game's outcome. In repeated games, the players interact several number of times $(\Gamma_1, \Gamma_2, \cdots)$. We assume that the players make their moves simultaneously in each game. The set of the past moves of all the players is commonly referred to as the history H of the game. History is uniquely defined at the beginning of each game ($h_1, h_2, \ldots$ and $h_1 = 0$) and the future move depends on the history. In repeated games, the users typically want to maximize their payoff for all the game they play. Hence, every player p_i tries to maximize his payoff function u_i. But for repeated games, we cannot simply

add up the payoffs received at each stage. There is a discount factor $\delta \in (0, 1)$ such that the future discounted payoff of player p_i is given by

$$u_i + \delta^1 u_i + \delta^2 u_i + \delta^3 u_i + \cdots$$

In some cases, the objective of the player can be to maximize their payoff only for the current game (which is equivalent to a game, which is played only once). Such game is known as shortsighted game. If the players try to maximize their payoff throughout the repeated game, then it is a long-sighted game. If the game is played finite number of times, then it is a finite repeated game. Otherwise, it is an infinite repeated game.

Definition 3. (Feasible payoff): A payoff profile (payoff vector of n players), say y, is feasible if there exist rational, non-negative values α_a such that for all p_i, we can express y_i (payoff corresponding to p_i) as $\sum_{a \in L} \alpha_a u_i(a)$ with $\sum_{a \in L} \alpha_a = 1$.

Definition 4. (Friedman or Nash folk theorem for infinitely repeated games) [10]: Let Γ be a strategic game in which each player has finitely many actions and $(y_1, y_2, \ldots y_n)$ be a feasible payoff profile of Γ and $(e_1, e_2, \ldots e_n)$ denotes the payoff from a Nash equilibrium of Γ. If $y_i > e_i$ for every player i and if δ is sufficiently close to one, then there exists a Nash equilibrium of infinitely repeated game Γ that achieves $(y_1, y_2, \ldots y_n)$ as the payoff.

3 Protocol for Synchronous Repeated Rational Secret Sharing

We denote our game by $\Gamma(n, m)$, where n is the number of players participating in the game and m is the threshold value of the number of shares to obtain the secret. We consider the scenario where m players come together and share the secrets repeatedly. That is, we solve the problem when m players come together to play the secret sharing game Γ repeatedly (the same set of m players). We do not consider the case where every time a new (different) set of players come and repeatedly play the game. So, exchange of shares is between these m players group, i.e., when a player sends his share to this set (selected players), they intern send their shares, reasoning to this is given below.

For every player, we have two actions namely, sending and not sending. Let us denote the action of sending the share to other $(m-1)$ players by 'A' and not sending by 'B'. Then, the strategy of a player for always not sending is $\{B, B, \ldots\}$ and for always sending is $\{A, A, \ldots\}$. In every game, the strategy profile, strategies chosen by the all players is denoted by n-tuple $(c_1, c_2, \ldots, c_n)$, where $c_i = A$ or $B, i \in \{1, \ldots, n\}$. The Repeated Rational Secret Sharing (RRSS) is similar to the Repeated prisoners' dilemma in many aspects [9].

In the modeled secret sharing game, the strategy which chooses not sending benefits one player and losses the players. We introduce one more punishment strategy known as Limited punishment strategy, which is explained in detail

in the section 3.1. We first discuss the strategies of the players, then analyze the cases for both the infinitely and finitely repeated rational secret sharing game.

3.1 Punishment Strategies

1. Grim trigger strategy

- choose A as long as the other players choose A.
- In any game some player chooses not sending (i.e., chooses B), then choose B in every subsequent game.

The grim trigger strategy for a repeated rational secret sharing game is defined as:

$s_i(\phi) = A$ (player p_i chooses A at the start of the game, ϕ denotes initial history), and

$$s_i(h_1, \ldots, h_q) = \begin{cases} A & \text{if } (h_{j1}, \ldots, h_{jq}) = (A, \ldots, A) \\ & \text{for every other player } p_j \\ B & \text{otherwise.} \end{cases}$$

That is, player p_i chooses A after any history in which every previous action of every player was A, and B after any other history. Even though the grim trigger strategy is effective in achieving the Nash equilibrium, the cooperating players are also getting the punishment. We propose one more strategy, which punishes only the player who did not send his share and not the other players.

2. Limited Punishment Strategy

- choose A as long as the other players choose A.
- In any game some player chooses not sending (i.e., chooses B), then choose B for k subsequent games.

The intention of this strategy is to punish only the player who did not send his share. If a player p_j does not send his share to a player p_i, then p_i chooses B for k consequent games. p_i will choose A only if p_j keeps sending his share for k consecutive games, even p_i does not send his share. Otherwise p_i will not send share to p_j. This is equivalent to outcast the player who does not send the data from the game for k number of games. The value of k should be such that, the gain obtained by not sending share should be less than loss that occurs in the next k games (as he cannot obtain the secret and others get his share).

In general, both of the strategies discussed here work effectively. But, for the sake of analysis we use only grim trigger strategy.

3.2 Infinitely Repeated Rational Secret Sharing Game

We make an assumption that players are patient enough and care for their future. In other words, the discount factor δ is sufficiently large and close to 1. We first analyze the game and then discuss the Nash equilibrium.

Suppose, a particular player p_j does not send his share to a player p_i, then the player p_i does not get the secret in that particular game. So, the player p_i uses the grim trigger strategy and does not send his share to p_j in further games. Thus, the player p_j will not get the secret from next game onwards. The player p_j realizes that he can no more obtain the secret and so there is no motivation to send his share to other players. Thus, no player learns the secret in further games. Hence, every player, because of the fear of not receiving any share from other players in further games, will cooperate in the current game. This punishment strategy acts as an incentive for a player to cooperate. Therefore, a player p_i's strategy is to always send his share to other players. He stops sending only when he does not receive a share from any other player. In this way every player receives m shares and can get the secret.

Suppose, in k^{th} game a player p_i does not send his share to a player p_j. Then, player p_j chooses grim trigger strategy and henceforth never sends his share to p_i. Thus, player p_i cannot obtain secret from $(k+1)^{th}$ game onwards and his payoff will be $(w_1, w_3, w_3, \ldots)$. If the player p_i always sends his share, then his payoff would be $(w_2, w_2, w_2, \ldots)$. So, for any player the payoff is high if he chooses always sending rather than not sending in any particular game. And every player primarily prefers to get the secret than not to get the secret (players care about future). Hence, every player always chooses to send his share.

But for infinitely repeated games, we cannot simply add up the payoffs received at each stage. The payoff is discounted by a factor, $\delta \in (0,1)$ such that the future discounted payoff of player p_i is given by $\sum_{j=0}^{\infty} \delta^j u_i(\Gamma_j)$. If δ is closer to 0, then the player does not care about his future payoff and concentrates more on the current payoff where as if δ is closer to 1, then the player is very patient and cares much about his future payoff.

Suppose if the player chooses the strategy always send $(A, A, \ldots)$, with payoff $u_i(A) = w_2$, then the overall discounted payoff will be $\sum_{j=0}^{\infty} \delta^j w_2 = \frac{w_2}{(1-\delta)}$.

If the player finks at r^{th} round, then till $(r-1)^{th}$ round the player gets payoff of w_2, at r^{th} round payoff of w_1 and from $(r+1)^{th}$ onwards payoff of w_3.

$$\begin{aligned}\sum_{j=0}^{\infty} \delta^j u_i(\Gamma_j) &= w_2 + \delta w_2 + \delta^2 w_2 + \ldots + \delta^{r-1} w_2 + \delta^r w_1 + \delta^{r+1} w_3 + \delta^{r+2} w_3 + \\ &\quad \delta^{r+3} w_3 + \ldots . \\ &= w_2(1 + \delta + \delta^2 + \ldots + \delta^{r-1}) + \delta^r w_1 + \delta^{r+1} w_3 (1 + \delta + \delta^2 + \ldots) \\ &= w_2() \tfrac{1-\delta^r}{1-\delta} + \delta^r w_1 + \tfrac{\delta^{r+1} w_3}{1-\delta} \\ &= \tfrac{w_2(1-\delta^r) + \delta^r w_1 + (\delta^{r+1} w_3)}{1-\delta}\end{aligned}$$

As δ is close to one,

$$\frac{w_2(1-\delta^r) + \delta^r w_1 + (\delta^{r+1} w_3)}{1-\delta} < \frac{w_2}{1-\delta}$$

So, every player chooses the strategy of always sending $(A, A, \ldots)$.

Theorem 1: *Infinitely Repeated Rational Secret Sharing (RRSS) game, $\Gamma(n, m)$ has a deterministic protocol when a group of m players come together, where n is the number of players and m is the threshold of shares.*

Proof: Given, a player sends his share to $(m-1)$ players and in-turn receives their shares, his payoff would be $(w_2, w_2, \ldots)$. The strategy profile $(A, A, \ldots)$ is a feasible payoff profile of the game and $(B, B, \ldots)$ be the Nash equilibrium of the single game Γ. As the players are patient enough and care for their future payoff, δ is sufficiently closer to one. As payoff corresponding to the strategy A, w_2 is greater than the minmax value, w_3 $(u_i(A) > u_i(B))$, from Nash folk theorem (Definition 4), the strategy profile $(A, A, \ldots)$ is a Nash equilibrium of infinitely repeated game $\Gamma(n, m)$ and the strategy, A is the best strategy for a player provided that every other player also plays his best strategy. In this way, all the players send their shares and thus obtain the secret. Hence, there exists a deterministic protocol for the RRSS game $\Gamma(n, m)$. □

Nash Equilibrium
The strategy $(A, A, \ldots)$ is a Nash equilibrium. Similarly, $(B, B, \ldots)$ is also a Nash equilibrium. But a player prefers to get the secret rather than not getting the secret. Hence, every player prefers to be in the state $(A, A, \ldots)$.

3.3 Finitely Repeated Rational Secret Sharing Game

First we discuss the issue what if the RRSS game is played only once ? Next we propose, in a finitely repeated rational secret sharing game, we have a deterministic protocol if the players are not aware of the last game. If the last game is known in advance, we do not have a solution for the game, $\Gamma(n, m)$.

3.3.1 What if the RRSS Game Is Played only Once?

Before analyzing the cases of infinitely and finitely repeated rational secret sharing game, we make an insight to the RRSS game when played only once (equivalent to a static game). Here, the players do not have a threat of not getting the secret in future games. So, the incentive of sending the share is lost. Lemma 1 proves the impossibility of secret sharing in such a game.

Lemma 1: *Secret Sharing is not possible in an RRSS game $\Gamma(n, m)$ if the game is played only once, where n is the number of players and m is the threshold of shares (considering our model and game $\Gamma(n, m)$).*

Proof: There is no punishment involved in the game, $\Gamma(n, m)$ as it is played only once. If the player p_i gets the secret and everyone else does not get the secret, then the payoff is w_1. If everyone (including p_i) gets the secret, then the payoff is w_2. Thus player p_i can obtain the payoff w_1 by not sending his share and w_2 by sending. As $w_1 > w_2$, the strategy B (not sending) strictly dominates the strategy A (sending). So, every player chooses strictly dominating strategy and no player sends his share. Hence, secret sharing is not possible in an RRSS game $\Gamma(n, m)$ if the game is played only once. □

3.3.2 Players Are Not Aware of the End of the Game

A finitely repeated game can be modeled as an infinitely repeated game, if the players are not aware of the end of the game. Therefore, we can always obtain a solution in this case, which is illustrated in the theorem 2.

Theorem 2: *Finitely Repeated Rational Secret sharing (RRSS) game, $\Gamma(n, m)$ has a deterministic protocol, if the players are not aware of the last game.*

Proof: As players do not know the last game, in every i^{th} game, players are not sure about whether they play the $(i+1)^{th}$ game or not. If a player does not send his share in i^{th} game, he might loss the chance of getting the secret in $(i+1)^{th}$ game onwards (if the game is going to be repeated). The punishment strategy acts as incentive for the players to send their shares. This scenario is similar to that of the infinitely repeated rational secret sharing game. Hence, from theorem 1, every player gets the secret. □

3.3.3 Players Are Aware of the Last Game

When players are aware of the end of the game, we can apply the concept of backward induction because, the game is of complete information (players know the number of times the game will be played). Let us consider the last game. Every player concludes that their dominant strategy is not to send the share of secret to others (i.e., to play 'B'). Given this argument, the best strategy is to play 'B' in the penultimate game. Following the same argument, this technique of backward induction dictates that every player should choose the strategy 'B' in every game. Thus, secret sharing is not possible for the finitely repeated game, given the players are aware of the end of the game. More formal proof is given by the lemma 2 and theorem 3.

Lemma 2: *If the players know that r^{th} game is the last game of finite RRSS game $\Gamma(n, m)$, then secret sharing is not possible in the r^{th} game.*

Proof: Given, the game is going to be played r number of times. As there is no punishment involved for the r^{th} game, there is no incentive for a player to send his share. Thus, this game is equivalent to a game, which is played only once. Hence, from lemma 1, there is no solution for the r^{th} game. □

Theorem 3: *Secret sharing is not possible for the RRSS game $\Gamma(n, m)$, if the players are aware of last game.*

Proof: We prove it by backward induction. Suppose, the game is being played r number of times. Given, the players are aware of the value of r, from the lemma 2, there is no solution for the r^{th} game. That is, no player sends his share in r^{th} game. So, in $(r-1)^{th}$ game, there is no effective punishment strategy, hence there is no incentive for a player to send their share. Hence $(r-1)^{th}$ game is equivalent to a single game. From Lemma 1, there is no solution for the $(r-1)^{th}$ game. Same reasoning applies to $(r-2)^{th}, (r-3)^{th} \ldots 1^{st}$ game. Therefore, in a finitely repeated game where players know the end of the game, repeated rational secret sharing $\Gamma(n, m)$ is not possible. □

Theorem 4: *Repeated Rational Secret Sharing game, $\Gamma(n, m)$ has a deterministic protocol for infinitely repeated games and finite repeated games (where players are not aware of number of times the game is going to be played), where n is the number of players and m is the threshold of shares.*

Proof: Easy observation from theorems 1 and theorem 3. □

3.3.4 Nash Equilibrium

For the finitely repeated rational secret sharing game, we have two cases. One, when players do not know the end of the game. In this case the Nash equilibrium is same as that of an Infinitely repeated game$(A, A, \ldots, A)$. Another, when the players are aware of the last game. In this case the Nash equilibrium is not to send the share, that is $(B, B, \ldots, B)$.

4 Mixed Model

We assume there are at most 't' computationally bounded malicious players. So the malicious players cannot send the wrong shares to other players. According to the protocol, every player distributes his shares to $(m-1)$ players and in-turn obtains their shares. If malicious players are present, then they choose not to send their shares to other players so that, no player learns the secret (even though they do not get the secret). To solve this problem, every player sends his share to $(m+t-1)$ players and in-turn obtains at least $(m-1)$ shares (as at least $(m-1)$ players are honest). If a player p_i did not receive the share of p_j, then player p_i considers p_j as a malicious player and stops sending the shares to p_j alone (sends to every one else).

Theorem 5: *In the presence of at most t malicious players, Repeated Rational Secret Sharing (RRSS) game $\Gamma(n, m)$ has a deterministic protocol for infinitely repeated games and finite repeated games (where players are not aware of number of times the game is going to be played), where n is the number of players and m is the threshold of shares.*

Proof: In mixed model, at most t players can be malicious and every player obtains at least $(m-1)$ shares. Hence, from theorem 4, repeated rational secret sharing (RRSS) game, $\Gamma(n, m)$ with at most t malicious players has a deterministic protocol. □

5 Asynchronous Repeated Rational Secret Sharing

We consider the Asynchronous model of the RRSS game. Here, we do not have a global clock and messages can be indefinitely delayed. For the dealer to know the end of the game and distribute new shares, the players are asked to send a message whenever they obtain the secret. If the dealer receives such messages from all the players, then he will distribute the shares of next secret, thus starting the next game. This protocol followed by the dealer acts as a punishment strategy (players wait indefinitely until every player gets the secret) and creates an incentive for every player to send his share.

Protocol for the Dealer and the Players
1. Protocol for player p_i

1. p_i sends his share to other $(m-1)$ players.

2. In every game, after receiving $(m-1)$ players' shares, calculate the secret and send a message to the dealer that the secret has been obtained mentioning the game.
   For e.g., $msg_i =$ " secret obtained in k^{th} game ".

2. Protocol for dealer

1. In the first game, send the shares to all the players $(p_1, p_2, \ldots, p_n)$.
2. After distributing shares in k^{th} game, $k \geq 1$ wait until n number of messages are received, $(msg_1, msg_2, \ldots msg_n)$. If all the messages are received, then distribute the new shares of $(k+1)^{th}$ game to all the players.

Lemma 3: *In Asynchronous model, a player has an incentive to send his share (in every game) to the* $(m-1)$ *players, in an infinite RRSS game and a finite RRSS game (where players are not aware of the last game).*

Proof: We prove this by contradiction. Assume that there is no incentive for a player p_i to send his share in k^{th} game. So, p_i will not send his share to any player in k^{th} game and no one gets the secret. Now, as per the protocol, the dealer waits indefinitely for the messages from the players and the next game never starts. So, the payoff of p_i from k^{th} game onwards will be $(w_1, w_3, \ldots)$. But, if he sends his share, the payoff would have been $(w_2, w_2, \ldots)$. Given the player does not know about the last game, he prefers $(w_2, w_2, \ldots)$ than $(w_1, w_3, \ldots)$, which is a contradiction. So, there is an incentive for a player to send his share in any given k^{th} game. □

Theorem 6: *Asynchronous Repeated Rational Secret Sharing (RRSS) game,* $\Gamma(n, m)$ *has a deterministic protocol for infinitely repeated game and finitely repeated game (where players are not aware of the last game), where* n *is the number of players and* m *is the threshold of shares.*

Proof: We prove this by contradiction. Assume that there is no incentive for a player p_i to send his share in k^{th} game. So, p_i will not send his share to any player in k^{th} game and no one gets the secret. Now, as per the protocol, the dealer waits indefinitely for the messages from the players and the next game never starts. So, the payoff of p_i from k^{th} game onwards will be $(w_1, w_3, \ldots)$. But, if he sends his share, the payoff would have been $(w_2, w_2, \ldots)$. Given the player does not know about the last game, he prefers $(w_2, w_2, \ldots)$ than $(w_1, w_3, \ldots)$, which is a contradiction. So, there is an incentive for a player to send his share in any given k^{th} game. So, every player sends his share. By considering Theorem 2, it can be observe that the game $\Gamma(n, m)$ finitely repeated games (where players are not aware of last game) is similar to infinitely repeated game. Hence, RRSS game has a deterministic protocol for infinitely repeated games and finitely repeated games (where players are not aware of last game). □

6 Conclusions and Open Problems

We have modeled the secret sharing as a repeated game (the game is played for some r number of times). We analyzed the repeated secret sharing game when

r is both finite and infinite. We propose a deterministic protocol for the infinite repeated game ($r->\infty$) and the finite repeated game (r is a finite number and the players do not know the value of r) in both synchronous and asynchronous models. We proved the impossibility for the finite repeated game when players know the value of r. We extended these results to the mixed model where at most t players are malicious, considering the synchronous model. The main advantage of introducing repeated games is that the players choose the strategy, which is mutually beneficial in terms of long-term gain rather than the one, which gives instantaneous benefit. We expect that the concept of repeated games can be introduced into various other problems of distributed computing (where the players are rational) and the scope for problem solving strategies in asynchronous model can be enhanced.

References

1. Halpern, J., Teague, V.: Rational secret sharing and multiparty computation: extended abstract. In: STOC 2004: Proceedings of the 36th annual ACM Symposium on Theory of Computing, pp. 623–632. ACM, New York, USA (2004)
2. Shamir, A.: How to share a secret. Commun. ACM 22, 612–613 (1979)
3. Gordon, S.D., Katz, J.: Rational secret sharing, revisited. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 229–241. Springer, Heidelberg (2006)
4. Abraham, I., Dolev, D., Gonen, R., Halpern, J.: Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In: PODC 2006: Proceedings of the 25th annual ACM symposium on Principles of distributed computing, pp. 53–62. ACM, New York, USA (2006)
5. Lysyanskaya, A., Triandopoulos, N.: Rationality and adversarial behaviour in multi-party computation (extended abstract). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 180–197. Springer, Heidelberg (2006)
6. Maleka, S., Amjed, S., Pandu Rangan, C.: The deterministic protocol for rational secret sharing. In: SSN 2008: The 4th International Workshop on Security in Systems and Networks (to be published, 2008)
7. Dodis, Y., Halevi, S., Rabin, T.: A cryptographic solution to a game theoretic problem. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 112–130. Springer, Heidelberg (2000)
8. Franklin, M., Yung, M.: Communication complexity of secure computation. In: 24th ACM Symposium on Theory of Computing (STOC), pp. 699–710 (1992)
9. Osborne, M.: An Introduction to Game Theory. Oxford University Press, Oxford (2004)
10. Friedman, J.W.: A non-cooperative equilibrium for supergames. Review of Economic Studies 38(113), 1–12 (1971)