Socio-Rational Secret Sharing as a New Direction in Rational Cryptography

Mehrdad Nojoumian[1,⋆] and Douglas R. Stinson[2,⋆⋆]

[1] Department of Computer Science,
Southern Illinois University, Carbondale, Illinois, USA
nojoumian@cs.siu.edu
[2] David R. Cheriton School of Computer Science,
University of Waterloo, Waterloo, Ontario, Canada
dstinson@math.uwaterloo.ca

Abstract. Rational secret sharing was proposed by Halpern and Teague in [8]. The authors show that, in a setting with rational players, secret sharing and multiparty computation are only possible if the actual secret reconstruction round remains unknown to the players. All the subsequent works use a similar approach with different assumptions.

We change the direction by bridging cryptography, game theory, and reputation systems, and propose a "social model" for repeated rational secret sharing. We provide a novel scheme, named *socio-rational secret sharing*, in which players are invited to each game based on their reputations in the community. The players run secret sharing protocols while founding and sustaining a public trust network. As a result, new concepts such as a *rational foresighted player*, *social game*, and *social Nash equilibrium* are introduced.

To motivate our approach, consider a repeated secret sharing game such as "secure auctions", where the auctioneers receive sealed-bids from the bidders to compute the auction outcome without revealing the losing bids. If we assume each party has a reputation value, we can then penalize (or reward) the players who are selfish (or unselfish) from game to game. This social reinforcement stimulates the players to be cooperative.

Keywords: cryptography, game theory, reputation systems.

1 Introduction

The classical (t, n)-*secret sharing scheme* was proposed in [24,3], where a *dealer* distributes shares of a secret α among n players $P_1, \ldots, P_n$ for a subsequent secret recovery. In a Shamir secret sharing [24], the dealer first generates a random polynomial $f(x) \in \mathbb{Z}_q[x]$ of degree $t-1$ such that $f(0) = \alpha$ is the secret. He then sends shares $f(i)$ to player P_i for $1 \leq i \leq n$. As a result, any group of t or more players can reconstruct the secret by Lagrange interpolation whereas any group

⋆ Research supported by NSERC CGS - MSFSS Supplements Program.
⋆⋆ Research supported by NSERC Discovery Grant 203114-12.

J. Grossklags and J. Walrand (Eds.): GameSec 2012, LNCS 7638, pp. 18–37, 2012.

of size less than t cannot gain any information about the secret. The standard assumption in traditional secret sharing is that each player is either *honest* (i.e., he follows protocols) or *malicious* (i.e., he deviates from protocols) where (1) at least t honest parties cooperate in order to recover the secret, and (2) the total number of malicious players is less than t.

A new research direction was initiated by Halpern and Teague [8] in the area of secret sharing and multiparty computation in a game-theoretic setting. In this new scheme, players are *rational* rather than being honest or malicious. This means each player selects his action (i.e., revealing his share or not revealing it) based on the utility that he can gain. As illustrated by the authors, classical secret sharing fails in this setting due to the failure of the secret reconstruction round. We should highlight that, in the context of rational secret sharing, "deviation" means that a player has not revealed his share during the reconstruction phase. Sending incorrect shares is another issue which can be prevented by having the dealer sign the shares. For a simple example of such an authentication method, see [13]. We now provide a high-level description of the problem.

If players are primarily incentivized to learn the secret, and secondly, they prefer that fewer of the other parties learn it, then it is not reasonable for each player to reveal his share in the "recovery phase". For instance, suppose players P_1, P_2, and P_3 receive shares $6, 11$, and 18 from a dealer respectively, where $f(x) = 3 + 2x + x^2 \in \mathbb{Z}_{19}[x]$ is the secret sharing polynomial. If only two players reveal their shares in the recovery phase, then the third selfish player (who has not revealed his share) can reconstruct the secret using two revealed shares and his own private share. Obviously, the other two cooperative players who have revealed their shares do not learn the secret. This justifies why the players do not reveal their shares in a rational setting, i.e., each player waits to receive shares of the other parties (see [5,11] for an overview in this direction).

To generalize this, consider the following scenario for a player P_j where the degree of the secret sharing polynomial is $t-1$. If P_i (for i less than $t-1$ or i more than $t-1$) reveal their shares, nothing changes whether P_j reveals his share or not. In the former case, no one learns the secret. In the latter case, everyone learns the secret. On the other hand, if exactly $t-1$ players P_i reveal their shares, then P_j can not only learn the secret with his own private share (i.e., t shares are sufficient to use Lagrange interpolation) but also can prevent the other players from learning the secret by not revealing his share, i.e., achieving the second preference of a self-interested player in rational secret sharing. In other words, for each P_i, revealing the share is *weakly dominated* by not revealing the share. As a result, no one reveals his share and the secret is never reconstructed.

We briefly introduce the notion of *social secret sharing* [21,22] in which players are either honest or malicious. In this protocol, weights of the players, i.e., the number of shares each player can hold, are periodically updated such that the players who cooperate receive more shares than those who defect. Although this scheme addresses a different issue compared to the secret recovery problem in a rational setting, we use its trust function in order to construct a new solution concept in rational cryptography.

1.1 Our Solution in Nutshell

In our "socio-rational" setting, the players are "selfish" similar to standard rational secret sharing. In addition, they have "concerns" about future gain or loss since our secret sharing game is repeated an unknown number of times. We term this new type of the player, a *rational foresighted player*. In the proposed scheme, each player has a reputation value which is updated according to his behavior each time the game is played. The initial reputation value is zero and its computation is public. For instance, if a player cooperates (he reveals his share), his trust value is increased, otherwise, it is decreased. A long-term utility (used by each player for action selection) and an actual utility (used for the real payment at the end of each game) are computed based on the following parameters:

1. Estimation of future gain or loss due to trust adjustment (virtual utility).
2. Learning the secret at the current time (real utility).
3. The number of other players learning the secret at the moment (real utility).

All these factors are used by each player to estimate his long-term utility and consequently to select his action, whereas only the last two items are used to compute the real payment at the end of each game. To estimate future impact, the following scenario is considered: whenever a player cooperates (or defects), we assume he can potentially gain (or lose) some extra units of utility, i.e., he has a greater (or lesser) chance to be "invited" to the future games and consequently he gains (or loses) more utility. In other words, if the reputation of P_i is decreased, he will have less chance to be invited to the future secret sharing games. Otherwise, P_i is going to be invited to more secret sharing games. To realize this scenario, in each game, the dealer selects the players based on their reputations, e.g., 50% from *reputable* players, 30% from *newcomers*, and 20% from *non-reputable* parties, where the number of players in each category varies.

This gain or loss is "virtual" at the current time but will be "realized" in the future. As an example of "future impact", consider the following statements, where U $\gg$ u and V $\gg$ v:

1. As a consumer, if you buy something today (*cooperate*: lose \$u), you receive a significant discount from the producer (*rewarded* \$U) on your next purchase.
2. As a producer, if you use low-grade materials to save money (*defect*: gain \$v), you lose many of your consumers (*penalized* \$V) in the coming years.

In other words, if we construct a socio-rational model where the players can gain (or lose) more utility in the future games than the current game, depending on their behavior, we can then incentivize them to be foresighted and cooperative.

1.2 Our Motivation

In *secure multiparty computation* [7,2,4], various players cooperate to jointly compute a function based on the private data they each provide. As stated in the literature, secret sharing is a fundamental method that is used by the players

to inject their private data into a multiparty computation protocol. At the end of a multiparty computation protocol, each player has a share of the function value. Therefore, they can collaborate to reveal this value to everyone.

We refer to *sealed-bid auctions* [9] as an application of multiparty computation. In a secure auction, auctioneers receive many sealed-bids from bidders and the goal is to compute the auction outcome (i.e., the winner and selling price) without revealing the losing bids. The main reason for using sealed-bids is the fact that, if bids are not kept private, they can be used in the future auctions and negotiations by different parties, say auctioneers, to maximize their revenues, or competitors, to win a later auction. To motivate our concept of "socio-rational secret sharing", consider the following repeated game, as shown in Figure 1:

1. The bidders select a subset of auctioneers based on a non-uniform probability distribution over the auctioneers' types, i.e., reputable auctioneers have a greater chance to be selected.
2. Each bidder then acts as an independent dealer to distribute the shares of his sealed-bid among the selected auctioneers.
3. Subsequently, the auctioneers compute the selling price and determine the winner by using a multiparty computation protocol.
4. In the last phase of the multiparty computation, the auctioneers reconstruct the selling price α and report it to the seller.

In this setting, only the auctioneers who have learned and reported α to the seller, are each paid $\$\Omega$, i.e., there exists a "competition" for learning the secret. In addition, $\$\Omega$ are divided among the auctioneers who have learned the secret; each of them can therefore earn more money if fewer of them learn α. If we repeat this game an unknown number of times and choose an appropriate invitation mechanism based on the players' reputation, we can incentivize the auctioneers to be cooperative, that is, they will reveal the shares of α in the recovery phase.

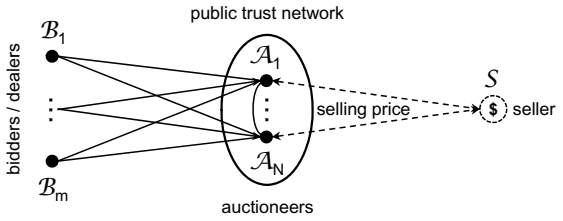

Fig. 1. Sealed-Bid Auction as a Repeated Secret Sharing Game

1.3 Our Contribution

We provide a new solution concept to the rational secret sharing problem by considering a social setting in which the players enter into a long-term interaction for executing an unknown number of independent secret sharing protocols.

In our model, a public trust network is constructed in order to incentivize the players to be cooperative. This incentive is sustained from game to game

since the players are motivated to enhance their reputations and consequently gain extra utility. In other words, they avoid a selfish behavior due to the social reinforcement of the trust network. Constructing a "social model" and inviting the players to a repeated game based on their "reputations" in the community, is a new contribution not only in rational cryptography but also in the existing game-theoretic solution concepts. We refer the reader to [17] for other discussions in this direction. Our scheme has the following desirable properties:

- It has a single secret recovery round, despite the existing solutions.
- It provides a game-theoretic solution that is always a Nash equilibrium.
- It is immune to rushing attack; it is not advantageous for players to wait.
- It prevents players from aborting the game; the case in some solutions.

The rest of this paper is organized as follows. Section 2 provides the relevant background. Section 3 reviews the literature of rational cryptography. Section 4 present our construction. Section 5 compares our solution with the existing schemes and techniques. Finally, Section 6 provides concluding remarks.

2 Preliminaries

2.1 Game-Theoretic Concepts

A *game* consists of a set of *players*, a set of *actions* and *strategies* (i.e., the way of choosing actions), and finally a *pay-off function* which is used by each participant to compute his utility. In *cooperative games*, players collaborate and split the total utility among themselves, i.e., cooperation is enforced by agreements. In *non-cooperative games*, players can not form agreements to coordinate their behavior, i.e., any cooperation must be self-enforcing. We now briefly review some game-theoretic definitions [8] for further technical discussions.

Definition 1. *Let* $\mathcal{A} \stackrel{\text{def}}{=} \mathcal{A}_1 \times \cdots \times \mathcal{A}_n$ *be an action profile for* n *players, where* $\mathcal{A}_i$ *denotes the set of possible actions of player* P_i*. A* game $\Gamma = (\mathcal{A}_i, u_i)$ *for* $1 \leq i \leq n$*, consists of* $\mathcal{A}_i$ *and a utility function* $u_i : \mathcal{A} \mapsto \mathbb{R}$ *for each player* P_i*. We refer to a vector of actions* $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathcal{A}$ *as an* outcome of the game.

Definition 2. *The* utility function u_i *illustrates the preferences of player* P_i *over different outcomes. We say* P_i prefers *outcome* $\boldsymbol{a}$ *to* $\boldsymbol{a}'$ *iff* $u_i(\boldsymbol{a}) > u_i(\boldsymbol{a}')$*, and he* weakly prefers *outcome* $\boldsymbol{a}$ *to* $\boldsymbol{a}'$ *if* $u_i(\boldsymbol{a}) \geq u_i(\boldsymbol{a}')$*.*

In order to allow the players to follow randomized strategies (where the strategy is the way of choosing actions), we define σ_i as a probability distribution over $\mathcal{A}_i$ for a player P_i. This means that he samples $a_i \in \mathcal{A}_i$ according to σ_i. A strategy is said to be a *pure-strategy* if each σ_i assigns probability 1 to a certain action, otherwise, it is said to be a *mixed-strategy*. Let $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ be the vector of players' strategies, and let $(\sigma_i', \boldsymbol{\sigma}_{-i}) \stackrel{\text{def}}{=} (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i', \sigma_{i+1}, \ldots, \sigma_n)$, where P_i replaces σ_i by σ_i' and all the other players' strategies remain unchanged.

Therefore, $u_i(\boldsymbol{\sigma})$ denotes the expected utility of P_i under the strategy vector $\boldsymbol{\sigma}$. A player's goal is to maximize $u_i(\boldsymbol{\sigma})$. In the following definitions, one can substitute an action $a_i \in \mathcal{A}_i$ with its probability distribution $\sigma_i \in \mathcal{S}_i$ or vice versa.

Definition 3. *A vector of strategies $\boldsymbol{\sigma}$ is a* Nash equilibrium *if, for all i and any $\sigma_i' \neq \sigma_i$, it holds that $u_i(\sigma_i', \boldsymbol{\sigma}_{-i}) \leq u_i(\boldsymbol{\sigma})$. This means no one gains any advantage by deviating from the protocol as long as the others follow the protocol.*

Definition 4. *Let $\mathcal{S}_{-i} \stackrel{\text{def}}{=} \mathcal{S}_1 \times \cdots \times \mathcal{S}_{i-1} \times \mathcal{S}_{i+1} \times \cdots \times \mathcal{S}_n$. A strategy $\sigma_i \in \mathcal{S}_i$ (or an action) is* weakly dominated *by a strategy $\sigma_i' \in \mathcal{S}_i$ (or another action) with respect to $\mathcal{S}_{-i}$ if:*

1. *For all $\boldsymbol{\sigma}_{-i} \in \mathcal{S}_{-i}$, it holds that $u_i(\sigma_i, \boldsymbol{\sigma}_{-i}) \leq u_i(\sigma_i', \boldsymbol{\sigma}_{-i})$.*
2. *There exists a $\boldsymbol{\sigma}_{-i} \in \mathcal{S}_{-i}$ such that $u_i(\sigma_i, \boldsymbol{\sigma}_{-i}) < u_i(\sigma_i', \boldsymbol{\sigma}_{-i})$.*

This means that P_i can never improve its utility by playing σ_i, and he can sometimes improve it by not playing σ_i. A strategy $\sigma_i \in \mathcal{S}_i$ is strictly dominated *if player P_i can always improve its utility by not playing σ_i.*

2.2 Rational Secret Sharing

We briefly review *rational secret sharing*, which was initiated by Halpern and Teague [8]. The scheme consists of a dealer D, who creates a secret sharing scheme with threshold t, and n players $P_1, \ldots, P_n$.

The protocol proceeds in a sequence of iterations where only one iteration is the "real" secret recovery phase (i.e., the last iteration) and the rest are just "fake" iterations for trapping selfish players. At the end of each iteration, the protocol either terminates (due to the observation of selfish behavior or cooperation for secret recovery) or it proceeds to the next iteration. Indeed, in any given round, players do not know whether the current iteration is the real recovery phase (where a player may gain more utility by being silent and not sending his share to the other players), or just a test round.

As we just stated, certain assumptions regarding the players' utility function are required for rational secret sharing to be achievable. Let $u_i(\boldsymbol{a})$ denotes the utility of P_i in a specific outcome $\boldsymbol{a}$ of the protocol. Suppose $l_i(\boldsymbol{a})$ is a bit defining whether P_i has learned the secret or not in $\boldsymbol{a}$. We then define $\delta(\boldsymbol{a}) = \sum_i l_i(\boldsymbol{a})$, which denotes the number of players who have learned the secret. The generalized assumptions of rational secret sharing are as follows:

- $l_i(\boldsymbol{a}) > l_i(\boldsymbol{a}') \Rightarrow u_i(\boldsymbol{a}) > u_i(\boldsymbol{a}')$.
- $l_i(\boldsymbol{a}) = l_i(\boldsymbol{a}')$ and $\delta(\boldsymbol{a}) < \delta(\boldsymbol{a}') \Rightarrow u_i(\boldsymbol{a}) > u_i(\boldsymbol{a}')$.

The first assumption means P_i prefers an outcome in which he learns the secret, i.e., since $l_i(\boldsymbol{a}) = 1$ and $l_i(\boldsymbol{a}') = 0$, he therefore prefers $\boldsymbol{a}$. The second assumption means P_i prefers an outcome in which the fewest number of other players learn the secret, given that P_i learns (or does not learn) the secret in both outcomes.

2.3 Social Secret Sharing

We now review *social secret sharing*, introduced by Nojoumian et al. [21], where the shares are allocated based on a player's reputation and the way she interacts with other parties. In other words, weights of players are adjusted such that participants who cooperate receive more shares compared to non-cooperative parties. This is similar to human social life where people share more secrets with whom they really trust and vice versa. In the context of social secret sharing, the players are either honest or malicious.

To quantify the reputation of each player in a social secret sharing scheme, the trust calculation method proposed in [20] is applied. In this approach, as shown in Table 1, three "types" of players (that is, $\mathcal{B}$: bad; $\mathcal{N}$: new; and $\mathcal{G}$: good) with six possible outcomes are defined, where α and β determine boundaries on the trust values used to define the different sets of players. This approach then applies functions $\mu(x)$ and $\mu'(x)$ to update the reputation $\mathcal{T}_i(p)$ of each P_i, as shown in Figure 2.

Table 1. Six Possible Actions for the Trust Management

Current Trust Value	Cooperation	Defection
$P_i \in \mathcal{B} \quad if \quad \mathcal{T}_i(p) \in [-1, \beta)$	Encourage	Penalize
$P_i \in \mathcal{N} \quad if \quad \mathcal{T}_i(p) \in [\beta, \alpha]$	Give a Chance	Take a Chance
$P_i \in \mathcal{G} \quad if \quad \mathcal{T}_i(p) \in (\alpha, +1]$	Reward	Discourage

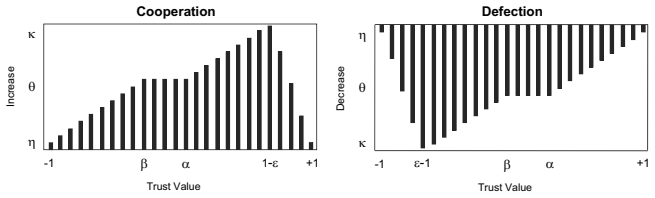

Fig. 2. Trust Adjustment by $\mu(x)$ and $\mu'(x)$ Functions

Let $\ell_i \in \{0, 1\}$ where $\ell_i = 1$ denotes that player P_i has cooperated in the current period and $\ell_i = 0$ denotes that he has defected. The proposed trust function is as follows, where $x = \mathcal{T}_i(p-1)$ (i.e., x is the previous trust value):

$$\ell_i = 1 \quad \Rightarrow \quad \mathcal{T}_i(p) = \mathcal{T}_i(p-1) + \mu(x), \text{ where}$$

$$\mu(x) = \begin{cases} \dfrac{\theta - \eta}{\beta + 1}(x+1) + \eta & P_i \in \mathcal{B} \\ \theta & P_i \in \mathcal{N} \\ \dfrac{\kappa - \theta}{1 - \epsilon - \alpha}(x - \alpha) + \theta & P_i \in \mathcal{G}, \mathcal{T}_i(p) \leq 1 - \epsilon \\ \dfrac{\kappa}{\epsilon}(1 - x - \epsilon) + \kappa & \mathcal{T}_i(p) > 1 - \epsilon \end{cases}$$

$$\ell_i = 0 \quad \Rightarrow \quad \mathcal{T}_i(p) = \mathcal{T}_i(p-1) - \mu'(x), \text{ where}$$

$$\mu'(x) = \begin{cases} \frac{\kappa}{\epsilon}(x+1) & \mathcal{T}_i(p) < \epsilon - 1 \\ \frac{\theta - \kappa}{\beta - \epsilon + 1}(x - \epsilon + 1) + \kappa & P_i \in \mathcal{B}, \mathcal{T}_i(p) \geq \epsilon - 1 \\ \theta & P_i \in \mathcal{N} \\ \frac{\eta - \theta}{1 - \alpha}(x - \alpha) + \theta & P_i \in \mathcal{G} \end{cases}$$

3 Literature Review

As we mentioned, the notion of *rational secret sharing* was introduced by Halpern and Teague [8]. Assuming the same game-theoretic model, Lysyanskaya and Triandopoulos [16] provide a solutions in a *mixed-behavior* setting in which players are either rational or malicious. Abraham et al. [1] define a notion of resistance to coalitions and present a *coalition-resistant* protocol. All these constructions use simultaneous channels (either a broadcast channel or secure private channels) that means each player must decide on the value he wants to broadcast before observing the values broadcasted by the other players; this is known as a *strategic game*.

The proposed protocols in [14,15,10] rely on *physical assumptions* such as secure envelopes and ballot boxes, which might be impossible or difficult to implement. In the same model, [19] provided a purely rational secret sharing scheme using a verifiable trusted channel. They showed that all the existing solutions not only rely on the players' rationality, but also on their beliefs. As a result, they cannot guarantee that all rational players learn the secret. For instance, suppose P_i believes that equilibrium (a, b) is played whereas P_j believes (a', b') is played, but the game leads to (a, b'), which may not be an equilibrium.

Kol and Naor [13] introduced an equilibrium notion, termed *strict Nash equilibrium*, in an information-theoretic secure setting. In a Nash equilibrium, no deviations are advantageous (i.e., there is no incentive to deviate). In its strict counterpart, all deviations are disadvantageous (i.e., there is an incentive not to deviate). They first considered both simultaneous and non-simultaneous broadcast channels and provided a new solution to avoid the simultaneous channel at the cost of increasing the round complexity.

Kol and Naor later [12] showed that all the existing computational-based protocols are susceptible to backward induction because of the cryptographic primitives used in the beginning of those protocols. That is, they can surely be broken after an exponential number of rounds. The authors then illustrate a new cryptographic coalition-resilient approach that is *immune to backward induction* by considering simultaneous as well as non-simultaneous broadcast channels.

The notion of *computational strict Nash equilibrium* was introduced in [6]. This dealer-free scheme can tolerate a coalition of size $t-1$ without using simultaneous channels. It can even be run over asynchronous point-to-point networks. Finally, it is efficient in terms of computation, share size, and round complexity.

Maleka et al. [18] presented *repeated rational secret sharing*, with the same approach proposed in [23], by considering two punishment strategies. In the former, each player reveals his share as long as the other players cooperate. As soon as the first defection is observed, the players do not reveal their shares in every subsequent game. In the latter, the players do not send their shares to the deviant for k subsequent games after observing the first defection. In the first scheme, each player not only punishes the deviant but also the other players including himself. In the second method, a player may deviate in an *expensive* secret recovery without having concern for k subsequent *cheap* recoveries.

4 Socio-Rational Secret Sharing

We first provide formal definitions of a *social game*, a *social Nash equilibrium*, and *socio-rational secret sharing*. In our model, each P_i has a public reputation value $\mathcal{T}_i$, where $\mathcal{T}_i(0) = 0$ and $-1 \leq \mathcal{T}_i(p) \leq +1$; $p = 0, 1, 2, \ldots$ denote the time periods of the games. The construction of this function is independent of our protocol, therefore, we use the existing function presented in Section 2.3. We assume each player's action $a_i \in \{\mathcal{C}, \mathcal{D}, \perp\}$, where $\mathcal{C}$ and $\mathcal{D}$ denote "cooperation" and "defection" respectively, and $\perp$ denotes P_i has not been chosen by the dealer to participate in the current game.

Definition 5. *In a society of size N, a* social game *$\Gamma = (\mathcal{A}_i, \mathcal{T}_i, u_i, u'_i)$, where $1 \leq i \leq N$, is repeatedly played an unbounded number of times among different subsets of players. Each P_i has a set of* actions *$\mathcal{A}_i$, a* reputation value *$\mathcal{T}_i$, a* long-term utility function *u_i, and an* actual utility function *u'_i. Let $\mathcal{A} \stackrel{\text{def}}{=} \mathcal{A}_1 \times \cdots \times \mathcal{A}_N$ be the action profile. In each game:*

- *A subset of $n \leq N$ players is chosen by the dealer for each new secret sharing game based on their reputation values $\mathcal{T}_i$, where more reputable players have a greater chance to be selected.*
- *Each P_i estimates his long-term utility by $u_i : \mathcal{A} \times \mathcal{T}_i \mapsto \mathbb{R}$ based on his gain in the current game and future games. Player P_i then selects his action a_i according to u_i.*
- *Let $\boldsymbol{a} = (a_1, \ldots, a_N) \in \mathcal{A}$ be the current game's outcome. The actual utility of each P_i is computed based on a function $u'_i : \mathcal{A} \mapsto \mathbb{R}$ at the end of the current game.*
- *Each player's reputation value $\mathcal{T}_i$ is publicly updated by a trust function based on each player's action in the current game, as shown in Section 2.3, except that $\mathcal{T}_i(p) = \mathcal{T}_i(p-1)$ if $a_i = \perp$.*

The *long-term utility function* u_i is used for action selection and the *actual utility function* u'_i is used to compute the "real gain" at the end of the current game.

Definition 6. *A vector of strategies $\boldsymbol{\sigma}$ is said to be a* social Nash equilibrium *in each game of a social game Γ if for all i and any $\sigma'_i \neq \sigma_i$ it holds that $u_i(\sigma'_i, \boldsymbol{\sigma}_{-i}) \leq u_i(\boldsymbol{\sigma})$. Accordingly, if $u_i(\sigma'_i, \boldsymbol{\sigma}_{-i}) < u_i(\boldsymbol{\sigma})$, it is said to be a* strict social Nash equilibrium. *That is, considering future games, a player cannot gain any benefit by deviating from the protocol in the current game.*

4.1 Utility Assumption

Let $u_i(\boldsymbol{a})$ denotes P_i's utility resulting from a list of players' actions $\boldsymbol{a}$ by considering future games, let $u'_i(\boldsymbol{a})$ denotes P_i's utility resulting from the current game, let $l_i(\boldsymbol{a}) \in \{0, 1\}$ denote if P_i has learned the secret during a given time period, and define $\delta(\boldsymbol{a}) = \sum_i l_i(\boldsymbol{a})$. Also, let $\mathcal{T}_i^{\boldsymbol{a}}(p)$ denote the reputation of P_i after outcome $\boldsymbol{a}$ in period p; each game of a social game is played in a single period. The generalized assumptions of socio-rational secret sharing are as follows:

A. $l_i(\boldsymbol{a}) = l_i(\boldsymbol{a}')$ and $\mathcal{T}_i^{\boldsymbol{a}}(p) > \mathcal{T}_i^{\boldsymbol{a}'}(p) \Rightarrow u_i(\boldsymbol{a}) > u_i(\boldsymbol{a}')$.
B. $l_i(\boldsymbol{a}) > l_i(\boldsymbol{a}') \Rightarrow u'_i(\boldsymbol{a}) > u'_i(\boldsymbol{a}')$.
C. $l_i(\boldsymbol{a}) = l_i(\boldsymbol{a}')$ and $\delta(\boldsymbol{a}) < \delta(\boldsymbol{a}') \Rightarrow u'_i(\boldsymbol{a}) > u'_i(\boldsymbol{a}')$.

The preference "*A*" illustrates that, whether player P_i learns the secret or not, P_i prefers to maintain a high reputation. The preferences "*B*" and "*C*" are the standard assumptions of rational secret sharing.

Definition 7. *In a social game, a* rational foresighted player *has prioritized assumptions: "A" (greediness) is strictly preferred to "B" and has an impact factor ρ_1, "B" (selfishness) is at least as good as "C" and has an impact factor ρ_2, and "C" (selfishness) has an impact factor ρ_3. We denote this using the notation $A^{\rho_1} \succ B^{\rho_2} \succeq C^{\rho_3}$, where $\rho_1 \gg \rho_2 \geq \rho_3 \geq 1$.*

The above definition reflects the fact that a rational foresighted player has a "long-term" vision and firstly prefers to achieve the highest level of trustworthiness. Only in this case, he will be involved in the future games and consequently gain more profits. He secondly prefers an outcome in which he learns the secret. Finally, he desires the fewest number of other players learn the secret. We next propose a long-term utility function that satisfies all three preferences.

4.2 Utility Computation

Our long-term utility function $u_i : \mathcal{A} \times \mathcal{T}_i \mapsto \mathbb{R}$ computes the utility that each player P_i potentially gains or loses by considering future games, based on assumptions "*A*", "*B*", "*C*", whereas the actual utility function $u'_i : \mathcal{A} \mapsto \mathbb{R}$ only computes the current gain or loss, based on assumptions "*B*" and "*C*".

Sample Function. We define two functions $\omega_i(\boldsymbol{a})$ and $\tau_i(\boldsymbol{a})$ for the n participating players of the current game:

$$\omega_i(\boldsymbol{a}) = \frac{3}{2 - \mathcal{T}_i^{\boldsymbol{a}}(p)} \tag{1}$$

$$\tau_i(\boldsymbol{a}) = \mathcal{T}_i^{\boldsymbol{a}}(p) - \mathcal{T}_i^{\boldsymbol{a}}(p-1). \tag{2}$$

Since $-1 \leq \mathcal{T}_i^{\boldsymbol{a}}(p) \leq +1$, then $+1 \leq \omega_i(\boldsymbol{a}) \leq +3$. Let $\Omega > 0$ be a "unit of utility", for instance, \$100. To satisfy our assumptions in Section 4.1, we define:

$$A : \frac{|\tau_i(\boldsymbol{a})|}{\tau_i(\boldsymbol{a})} \times \omega_i(\boldsymbol{a}) \times \Omega \quad \text{where} \quad \frac{|\tau_i(\boldsymbol{a})|}{\tau_i(\boldsymbol{a})} = \begin{cases} +1 \text{ if } a_i = \mathcal{C} \\ -1 \text{ if } a_i = \mathcal{D} \end{cases} \tag{3}$$

$$B : l_i(\boldsymbol{a}) \times \Omega \quad \text{where} \quad l_i(\boldsymbol{a}) \in \{0, 1\} \tag{4}$$

$$C : \frac{l_i(\boldsymbol{a})}{\delta(\boldsymbol{a}) + 1} \times \Omega \quad \text{where} \quad \delta(\boldsymbol{a}) = \sum_{i=1}^{N} l_i(\boldsymbol{a}). \tag{5}$$

- (3) will evaluate to $+\omega_i(\boldsymbol{a})\Omega$ if P_i cooperates and it will evaluate to $-\omega_i(\boldsymbol{a})\Omega$, otherwise. This means that P_i gains or loses at least 1Ω and at most 3Ω (depending on his reputation value, as reflected in ω_i) units of utility in the future games due to his current behavior.
- (4) illustrates that a player gains one unit of utility if he learns the secret in the current game and he loses this opportunity, otherwise.
- (5) results in "almost" one unit of utility being divided among all the players P_i who have learned the secret in the current game; to avoid a division by 0 when $\delta(\boldsymbol{a}) = 0$, we use $\delta(\boldsymbol{a}) + 1$ in the denominator.

We combine these three terms, weighted with their corresponding impact factors:

$$u'_i(\boldsymbol{a}) = \rho_2\Big(l_i(\boldsymbol{a}) \times \Omega\Big) + \rho_3\Big(\frac{l_i(\boldsymbol{a})}{\delta(\boldsymbol{a}) + 1} \times \Omega\Big), \text{ and} \tag{6}$$

$$\begin{aligned} u_i(\boldsymbol{a}) &= \rho_1\Big(\frac{|\tau_i(\boldsymbol{a})|}{\tau_i(\boldsymbol{a})} \times \omega_i(\boldsymbol{a}) \times \Omega\Big) + u'_i(\boldsymbol{a}) \\ &= \Omega \times \Big(\rho_1\Big(\frac{|\tau_i(\boldsymbol{a})|}{\tau_i(\boldsymbol{a})} \times \omega_i(\boldsymbol{a})\Big) + \rho_2\Big(l_i(\boldsymbol{a})\Big) + \rho_3\Big(\frac{l_i(\boldsymbol{a})}{\delta(\boldsymbol{a}) + 1}\Big)\Big). \end{aligned} \tag{7}$$

The function $u_i(\boldsymbol{a})$ shows that if player P_i, with preference factors $\rho_1 \gg \rho_2 \geq \rho_3 \geq 1$, defects (or cooperates), he may gain (or lose) $\rho_2\Omega + (\rho_3\Omega)/(\delta(\boldsymbol{a}) + 1)$ utility in the current game, but he will lose (or gain) "x" units of utility in the future games, where $\rho_1\Omega \leq x \leq 3\rho_1\Omega$. That is, future loss or gain is more important than the current loss or gain. We later show that the dealer gives a lesser (or a greater) chance of contribution to non-reputable (or reputable) players in the future games, that is, reputation remains with a player as a characteristic which continuously affects his utility.

4.3 Proposed Protocol

We now discuss our socio-rational secret sharing scheme, the details are presented in Figure 3. Suppose the public trust network has already been created. Assume we have a dealer who initiates a (t, n)-threshold secret sharing scheme. Also, assume all the players use a "pure-strategy". A *socio-rational secret sharing* game $\Gamma = (\mathcal{A}_i, \mathcal{T}_i, u_i, u'_i)$ is a social game that is played among rational foresighted players and it is based on the following elements:

Secret Sharing

1. Let ϕ be the current probability distribution over players' types $\mathcal{B}, \mathcal{N}, \mathcal{G}$, as defined in Section 2.3. The dealer D selects n out of N players, where $n \leq N$, based on this non-uniform probability distribution.
2. D then initiates a (t, n)-secret sharing scheme by selecting $f(x) \in \mathbb{Z}_q[x]$ of degree $t-1$, where $f(0) = \alpha$ is the secret. Subsequently, he sends shares $f(i)$ to P_i for the n chosen players, and leaves the scheme.

Secret Recovery

1. Each chosen player P_i computes his long-term utility function $u_i : \mathcal{A} \times \mathcal{T}_i \mapsto \mathbb{R}$, and then selects an action, i.e., revealing or not revealing his share $f(i)$.
2. If enough shares are revealed, the polynomial $f(x)$ is reconstructed through Lagrange interpolation and the secret $f(0) = \alpha$ is recovered.
3. Each chosen player P_i receives his utility $u_i' : \mathcal{A} \mapsto \mathbb{R}$ (i.e., the real payment) at the end of the reconstruction phase according to the outcome.
4. Finally, the reputation values $\mathcal{T}_i$ of all the chosen players are publicly updated according to each player's behavior and the trust function.

Fig. 3. Socio-Rational Secret Sharing Protocol

1. Set of possible actions $\mathcal{A}_i = \{\mathcal{C}, \mathcal{D}, \perp\}$, defined in Section 4.
2. Function $\mathcal{T}_i$, except that $\mathcal{T}_i(p) = \mathcal{T}_i(p-1)$ if $a_i = \perp$, defined in Section 2.3.
3. Long-term utility function $u_i : \mathcal{A} \times \mathcal{T}_i \mapsto \mathbb{R}$, defined in Section 4.2.
4. Actual utility function $u_i' : \mathcal{A} \mapsto \mathbb{R}$, defined in Section 4.2.

The *sharing phase* is similar to that of standard secret sharing. The only difference is the way that the dealer selects n out of N players for secret sharing. In other words, the dealer gives more chance to reputable players compared to unreliable parties. Although a natural approach is to invite only the reputable players, it is not fair if the dealer does not provide any opportunity for newcomers, or if he completely ignores the bad players. Once in a while, he should give a chance to the bad players so they can compensate for their past behavior. This is a realistic approach even in human society; it can be interpreted as a "forgiveness factor". The *secret recovery phase* is also similar to that of the standard secret sharing but with some extra components.

Note that since the players' reputations and the trust function are public information. Therefore, all computations associated with the reputation system can be done by any authority or a committee of the players. It is also worth mentioning that it is not required to consider unknown number of iterations for secret recovery, which is the case in all the existing rational secret sharing schemes. In fact, in a "socio-rational secret sharing" game, we have an unknown number of independent secret sharing games, whereas in "rational secret sharing", we only have one secret with an unknown number iterations for secret recovery.

Theorem 1. *In a $(2,2)$-socio-rational secret sharing, $\mathcal{C}$ strictly dominates $\mathcal{D}$, considering a long-term utility function , shown in Equation (7), which satisfies the preferences of rational foresighted players, shown in Definition 7. In other words, $\mathcal{D}$ is strictly dominated by $\mathcal{C}$. As a result, $(\mathcal{C},\mathcal{C})$ is a strict social Nash equilibrium that is a unique solution.*

Proof. We compute the utility of each outcome for P_i. Let P_j be the other player.

1. If both players cooperate, denoted by $(\mathcal{C},\mathcal{C})$, then τ_i is positive, $l_i = 1$ since P_i has learned the secret, and $\delta = 2$ because both players have learned the secret. We have:
$$\big(\tau_i > 0, l_i = 1, \delta = 2\big) \Rightarrow u_i^{(\mathcal{C},\mathcal{C})}(\boldsymbol{a}) = \Omega\Big(\rho_1\omega_i + \rho_2 + \frac{\rho_3}{3}\Big).$$
2. If only P_i cooperates, denoted by $(\mathcal{C},\mathcal{D})$, then τ_i is positive, $l_i = 0$ since P_i has not learned the secret, and $\delta = 1$ because only player P_j has learned the secret. We have:
$$\big(\tau_i > 0, l_i = 0, \delta = 1\big) \Rightarrow u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a}) = \Omega\Big(\rho_1\omega_i\Big).$$
3. If only P_j cooperates, denoted by $(\mathcal{D},\mathcal{C})$, then τ_i is negative, $l_i = 1$ since P_i has learned the secret, and $\delta = 1$ because only player P_i has learned the secret. We have:
$$\big(\tau_i < 0, l_i = 1, \delta = 1\big) \Rightarrow u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a}) = \Omega\Big(-\rho_1\omega_i + \rho_2 + \frac{\rho_3}{2}\Big).$$
4. If both players defect, denoted by $(\mathcal{D},\mathcal{D})$, then τ_i is negative, $l_i = 0$ since P_i has not learned the secret, and $\delta = 0$ because no one has learned the secret. We have:
$$\big(\tau_i < 0, l_i = 0, \delta = 0\big) \Rightarrow u_i^{(\mathcal{D},\mathcal{D})}(\boldsymbol{a}) = \Omega\Big(-\rho_1\omega_i\Big).$$

We ignore the common factor Ω. We know $1 \leq \omega_i(\boldsymbol{a}) \leq 3$ and $\rho_1 \gg \rho_2 \geq \rho_3 \geq 1$.

- First, we have:
$$u_i^{(\mathcal{C},\mathcal{C})}(\boldsymbol{a}) = \rho_1\omega_i + \rho_2 + \frac{\rho_3}{3} > \rho_1\omega_i = u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a}). \tag{8}$$
- Next, it is easy to see that
$$u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a}) = \rho_1\omega_i > -\rho_1\omega_i + \rho_2 + \frac{\rho_3}{2} = u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a}) \tag{9}$$
if and only if $2\rho_1\omega_i > \rho_2 + \frac{\rho_3}{2}$. We have:
$$\begin{aligned} 2\rho_1\omega_i &\geq 2\rho_1 \\ &> \rho_2 + \rho_3 \\ &> \rho_2 + \frac{\rho_3}{2}, \end{aligned}$$
so the desired conclusion follows.

- Finally,

$$u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a}) = -\rho_1\omega_i + \rho_2 + \frac{\rho_3}{2} > -\rho_1\omega_i = u_i^{(\mathcal{D},\mathcal{D})}(\boldsymbol{a}). \tag{10}$$

Therefore, we have the following payoff inequalities which proves the theorem:

$$\overbrace{u_i^{(\mathcal{C},\mathcal{C})}(\boldsymbol{a}) > u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a})}^{P_i \text{ cooperates}} > \overbrace{u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a}) > u_i^{(\mathcal{D},\mathcal{D})}(\boldsymbol{a})}^{P_i \text{ defects}}.$$

□

The interesting observation is the difference between the utilities $u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a})$ and $u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a})$. This means that it is better for player P_i to cooperate, even though he might not learn the secret and the other party might learn it. On the other hand, even if P_i learns the secret by deviating at a given period (using the share of the other party), he will gain less utility in the long-term. This is due to future gain or loss and the significance of being reputable, which is incorporated in our long-term utility function by considering an impact factor ρ_1. We should also note that, as ρ_1 is increased, the difference between $u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a})$ and $u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a})$ also increases, i.e., the enforcement for cooperation would be greater.

In a secret sharing scheme with selfish players, the outcome $(\mathcal{U}^-,\mathcal{U}^-)$ is a Nash equilibrium, as shown in Table 2, where $\mathcal{U}^+ > \mathcal{U} > \mathcal{U}^- > \mathcal{U}^{--}$. Rational secret sharing solves this problem by using a randomized mechanism, as presented in Section 2.2. The payoff matrix associated with socio-rational secret sharing is illustrated in Table 3. In this payoff matrix, the outcome $(\mathcal{U}^+,\mathcal{U}^+)$ is a *strict social Nash equilibrium.*

Table 2. $(2,2)$-SS with Selfish Players

P_1 \ P_2	$\mathcal{C}$ooperation	$\mathcal{D}$efection
$\mathcal{C}$ooperation	$\mathcal{U},\mathcal{U}$	$\mathcal{U}^{--},\mathcal{U}^{+}$
$\mathcal{D}$efection	$\mathcal{U}^{+},\mathcal{U}^{--}$	$\mathcal{U}^{-},\mathcal{U}^{-}$

Table 3. $(2,2)$-Socio-Rational SS

P_1 \ P_2	$\mathcal{C}$ooperation	$\mathcal{D}$efection
$\mathcal{C}$ooperation	$\mathcal{U}^{+},\mathcal{U}^{+}$	$\mathcal{U},\mathcal{U}^{-}$
$\mathcal{D}$efection	$\mathcal{U}^{-},\mathcal{U}$	$\mathcal{U}^{--},\mathcal{U}^{--}$

We should note that our socio-rational game is a non-cooperative game. In fact, cooperation is self-enforcing due to the importance of reputation as well as future concerns of a rational foresighted player. In a cooperative game, this enforcement is provided by a third party and players do not really compete. Moreover, this payoff matrix does not mean that the players never deviate. As an example, consider a scenario in which a player is involved in many independent social games. If he simultaneously receives many requests for secret recovery of various schemes, he will select the one in which he can gain more utility. This is discussed later, in Section 4.4. We now analyze our scheme for $n > 2$.

Theorem 2. *In a socio-rational secret sharing scheme with n participants and $t = 2$, $\mathcal{C}$ strictly dominates $\mathcal{D}$ for all P_i, assuming the preferences of rational foresighted parties. Consequently, the vector $\boldsymbol{a}^{\mathcal{C}} = (a_1^{\mathcal{C}}, \ldots, a_n^{\mathcal{C}})$ is a strict social Nash equilibrium that is a unique solution.*

Proof. Let $\mathcal{C}_i$ (or $\mathcal{D}_i$) denote that player P_i cooperates (or defects), and let $\mathcal{C}_{-i}$ (or $\mathcal{D}_{-i}$) denote that, excluding P_i, all the other players cooperate (or defect), and finally let $\mathcal{M}_{-i}$ denotes that, excluding P_i, some players cooperate and some of them defect. We compute the utility of each outcome based on Equation (7) for the least possible threshold $t = 2$ when $n > 2$.

1. If all the players cooperate, denoted by $(\mathcal{C}_i, \mathcal{C}_{-i})$, then τ_i is positive, $l_i = 1$ since player P_i has learned the secret, and $\delta = n$ because all the players have learned the secret. We have:
$$\big(\tau_i > 0, l_i = 1, \delta = n\big) \Rightarrow u_i^{(\mathcal{C}_i, \mathcal{C}_{-i})}(\boldsymbol{a}) = \Omega\Big(\rho_1\omega_i + \rho_2 + \frac{\rho_3}{n+1}\Big).$$
2. If player P_i cooperates but some of the other parties cooperate and some defect, denoted by $(\mathcal{C}_i, \mathcal{M}_{-i})$, then τ_i is positive, $l_i = 1$, and $\delta = n$ because all the players have learned the secret. We have:
$$\big(\tau_i > 0, l_i = 1, \delta = n\big) \Rightarrow u_i^{(\mathcal{C}_i, \mathcal{M}_{-i})}(\boldsymbol{a}) = \Omega\Big(\rho_1\omega_i + \rho_2 + \frac{\rho_3}{n+1}\Big).$$
3. If only P_i cooperates, denoted by $(\mathcal{C}_i, \mathcal{D}_{-i})$, then τ_i is positive, $l_i = 0$, and $\delta = n - 1$ since all the players, except P_i, have learned the secret. We have:
$$\big(\tau_i > 0, l_i = 0, \delta = n-1\big) \Rightarrow u_i^{(\mathcal{C}_i, \mathcal{D}_{-i})}(\boldsymbol{a}) = \Omega\Big(\rho_1\omega_i\Big).$$
4. If only P_i defects, denoted by $(\mathcal{D}_i, \mathcal{C}_{-i})$, then τ_i is negative, $l_i = 1$, and $\delta = n$ because all the players have learned the secret. We have:
$$\big(\tau_i < 0, l_i = 1, \delta = n\big) \Rightarrow u_i^{(\mathcal{D}_i, \mathcal{C}_{-i})}(\boldsymbol{a}) = \Omega\Big(-\rho_1\omega_i + \rho_2 + \frac{\rho_3}{n+1}\Big).$$
5. If P_i defects but some of the other parties cooperate and some defect, denoted by $(\mathcal{D}_i, \mathcal{M}_{-i})$, τ_i is negative, $l_i = 1$, and $\delta = n - 1$ if only one player reveals his share, or $\delta = n$ if at least two players reveal their shares. We have:
$$\big(\tau_i < 0, l_i = 1, \delta\big) \Rightarrow u_i^{(\mathcal{D}_i, \mathcal{M}_{-i})}(\boldsymbol{a}) = \Omega\Big(-\rho_1\omega_i + \rho_2 + \frac{\rho_3}{\delta+1}\Big), \delta \in \{n-1, n\}.$$
6. If all the players defect, denoted by $(\mathcal{D}_i, \mathcal{D}_{-i})$, then τ_i is negative, $l_i = 0$, and $\delta = 0$ because no one has learned the secret. We have:
$$\big(\tau_i < 0, l_i = 0, \delta = 0\big) \Rightarrow u_i^{(\mathcal{D}_i, \mathcal{D}_{-i})}(\boldsymbol{a}) = \Omega\Big(-\rho_1\omega_i\Big).$$

We now analyze these six scenarios:

- If player P_i cooperates (cases $1-3$), regardless of whether the other players cooperate or defect, then
$$u_i^{\mathcal{C}}(\boldsymbol{a}) \geq \rho_1\omega_i. \tag{11}$$
- If P_i defects (cases $4-6$), regardless of whether the other players cooperate or defect, then
$$u_i^{\mathcal{D}}(\boldsymbol{a}) \leq -\rho_1\omega_i + \rho_2 + \frac{\rho_3}{n}. \tag{12}$$

It is easy to prove that $\rho_1\omega_i > -\rho_1\omega_i + \rho_2 + \frac{\rho_3}{n}$; the proof is the same as the proof of (9) in Theorem 1. As a result, it is always in P_i's best interest to cooperate:

$$u_i^{\mathcal{C}}(\boldsymbol{a}) > u_i^{\mathcal{D}}(\boldsymbol{a}).$$

□

Remark 1. A similar analysis can be given for any threshold $t > 2$ when $n > 2$.

4.4 Expected Utility

We now illustrate how each P_i can compute his expected utility when he participates in different independent social games. Note that the *utility value* shows the connection between actions and their consequences for a player, whereas the *expected utility* of P_i is an estimation of gain or loss when he plays with P_j.

We initially show how to compute the expected utilities in a $(2,2)$-game for "cooperation" and "defection". An expected utility is computed as a linear combination of utility values and the probability of P_j's cooperation, where $\epsilon_j \in [0,1]$ denotes the probability that the opponent P_j may cooperate and $\mathcal{U}^+ > \mathcal{U} > \mathcal{U}^- > \mathcal{U}^{--}$ are the utility values from Table 3. We have:

$$\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}) = \epsilon_j\,\mathcal{U}^+ + (1-\epsilon_j)\,\mathcal{U} \tag{13}$$

$$\mathcal{EU}_i^{\mathcal{D}}(\boldsymbol{a}) = \epsilon_j\,\mathcal{U}^- + (1-\epsilon_j)\,\mathcal{U}^{--} \tag{14}$$

Theorem 3. *In a socio-rational secret sharing game with two players P_i and P_j, the expected utility of cooperation is greater than the expected utility of defection, i.e., $\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}) - \mathcal{EU}_i^{\mathcal{D}}(\boldsymbol{a}) > 0$, where ϵ_j is the probability of opponent's cooperation.*

Proof.

$$\begin{aligned}\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}) - \mathcal{EU}_i^{\mathcal{D}}(\boldsymbol{a}) &= \big(\epsilon_j\,\mathcal{U}^+ + (1-\epsilon_j)\,\mathcal{U}\big) - \big(\epsilon_j\,\mathcal{U}^- + (1-\epsilon_j)\,\mathcal{U}^{--}\big) \text{ by (13,14)}\\ &= \epsilon_j\,(\mathcal{U}^+ - \mathcal{U}^-) + (1-\epsilon_j)\,(\mathcal{U} - \mathcal{U}^{--})\\ &> 0.\end{aligned}$$

□

We now consider the expected utilities in two independent $(2,2)$-games. Let us define $\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}_{ij})$ and $\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}_{ik})$ as the expected utilities of the two games, when player P_i cooperates with players P_j and P_k respectively.

Theorem 4. *Suppose P_i plays with P_j and P_k in two independent $(2,2)$-games. Player P_i then gains more utility if he collaborates with the most reputable player.*

Proof. Let P_j and P_k have different reputation values computed with the same trust function. For instance, $\epsilon_j > \epsilon_k$, which means P_j is more reputable than P_k. Suppose P_i receives the same unit of utility Ω in both games, and let $\boldsymbol{a}_{ij}, \boldsymbol{a}_{ik}$ be the outcomes of the two games. We have:

$$\begin{aligned}\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}_{ij}) - \mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}_{ik}) &= \big(\epsilon_j\,\mathcal{U}^+ + (1-\epsilon_j)\,\mathcal{U}\big) - \big(\epsilon_k\,\mathcal{U}^+ + (1-\epsilon_k)\,\mathcal{U}\big) \quad \text{by (13)} \\ &= \epsilon_j\,\mathcal{U}^+ - \epsilon_k\,\mathcal{U}^+ + (1-\epsilon_j)\,\mathcal{U} - (1-\epsilon_k)\,\mathcal{U} \\ &= (\epsilon_j - \epsilon_k)\,\mathcal{U}^+ + (\epsilon_j - \epsilon_k)\,\mathcal{U} \\ &> 0,\end{aligned}$$

since $\epsilon_j > \epsilon_k$. As a result, $\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}_{ij}) > \mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}_{ik})$. This means that player P_i gains more utility if he collaborates with P_j rather than P_k. □

5 Comparison with Existing Techniques

Our contribution differs from *rational secret sharing* and *social secret sharing*, as shown in Figure 4. Our scheme is a repeated game that addresses the problem of secret recovery in the presence of rational foresighted parties, whereas:

- "rational secret sharing" is a one-time game with repeated rounds, and it deals with the problem of secret recovery of a secret in the presence of rational players, and
- "social secret sharing" defines how many shares each player can hold in a weighted secret sharing scheme with honest and malicious parties.

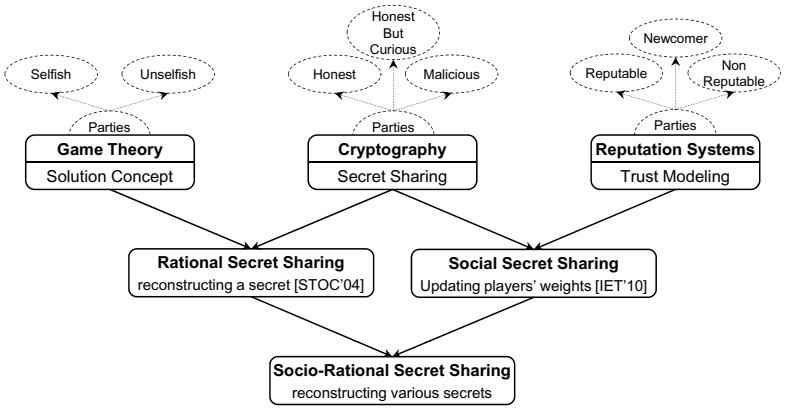

Fig. 4. Pedigree of the Socio-Rational Secret Sharing

Our contribution is also different from the *punishment strategy* used in the *repeated prisoners' dilemma* [23] where the players penalize potential deviants. As the authors have mentioned, the major point behind the repeated games is the fact that if each participant believes any deviation terminates the mutual cooperation (resulting in a subsequent loss that outweighs the short-term gain), he then prefers to cooperate. Our approach has the following advantages over the punishment strategy:

- In our model, a player is not just an abstract entity who selects actions. He also has a social characteristic reflected in his reputation that shows his trustworthiness. This attribute is solely determined by the player's actions.
- The punishment strategy is performed by selecting actions that are harmful for deviants whereas, in our model, punishment or reward (losing or gaining reputation and utility) is independent of action selection.
- Our approach avoids penalizing innocent players or the punisher himself. It also avoids being involved, to some extent, in a game with seriously selfish players who are not reputable (due to our "invitation approach").
- The punishment strategy does not consider that a game may have various levels of importance and utility weights when it is repeatedly played, e.g., a secret sharing scheme to launch a "missile" or to open a "safety box".
- The punishment strategy has a discrete penalizing approach whereas our construction has a continuous impact on the deviants. For example, it may take a long time for a player to regain lost reputation.
- Our proposed approach not only considers punishment and reward but also defines six different scenarios in order to fairly deal with various types of players, including good players, bad players, and newcomers.

Our contribution is also different from the constructions forming histories and beliefs such as *subgame perfect equilibrium* or *Bayesian equilibrium* [23]. In the former, players reassess their decisions based on the past *history*, i.e., a sequence of previous actions. In the latter, the game is designed to deal with the situations in which parties are not certain about the characteristics of each others. Therefore, they form *beliefs*, i.e., a probability distributions over actions, to anticipate any future behavior. Let P_i be a specific player, and let P_j for $1 \leq j \neq i \leq n$ denote any other player except P_i.

- In forming a belief about P_i's intentions, both parties contribute. That is, P_i is indirectly involved by his behavior, i.e., action selections, and the other players are directly involved by the methodology that they use in order to form the probability distribution over actions. A belief may or may not be common knowledge, meaning that various players may have different judgments and beliefs about P_i. On the other hand, the reputation of P_i in a trust network is solely determined by his behavior through a trust function, which is a commonly known function for reputation measurement. That is, the reputation is a direct reflection of P_i's attitude, and he knows the impact of his decision on the other players (i.e., whether he is known as a good player, a bad player, or a newcomer). He can also estimate how much extra utility he may gain or lose after his reputation's adjustment.
- Histories and beliefs are more general compared to the reputation system in a trust network. This means a belief as a probability distribution can be defined over any set of actions for any types of players. On the other hand, reputation is built over a specific set of actions, such as $\mathcal{C}$ooperation and $\mathcal{D}$efection, for specific types of players, such as good players, bad players, and newcomers. As a result, the reputation system is simpler and it is more suitable for cryptographic constructions.

- In the history and belief systems, measurements are "inside" the game-theoretic model whereas our reputation system isolates these computations from the game. For instance, two separate probability distributions can be defined over the players' types and actions by considering their past behavior. But our publicly known trust function combines these two measurements in a single reputation value outside of the game-theoretic model. In other words, the punishment or reward is embedded inside of our reputation system which continuously affects the players' utilities in the game-theoretic model, i.e., losing utility due to the reputation's decline or losing reputation and not being selected in the future secret sharing games.

6 Conclusion and Future Direction

This paper provides a multidisciplinary research connecting three major areas of computer science to propose a novel solution for a cryptographic primitive. We should note that having a trust network by considering long-term interactions can be seen as a new direction in game theory itself, specifically, the theoretical models used in social sciences such as economics and political science because elements in those frameworks are more close to human social behavior.

As our future work, we are interested to consider other complicated models. For instance, using *referral chain* in which two players who are interacting for the first time, can gain some information with respect to each other's reputation through other parties or common friends. We also would like to scrutinize the impact of a situation in which a player is involved in *various societies* while he is holding different reputation values associated with each one. It would be also interesting to construct a *hybrid model* in which both "reputation" and "belief" are considered. In this case, reputation can be seen as an estimation of the past behavior whereas belief can be viewed as an anticipation of the future activities.

References

1. Abraham, I., Dolev, D., Gonen, R., Halpern, J.Y.: Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In: 25th Annual ACM Symposium on Principles of Distributed Computing PODC, pp. 53–62 (2006)
2. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: 20th Annual ACM Symposium on Theory of Computing, STOC, pp. 1–10 (1988)
3. Blakley, G.: Safeguarding cryptographic keys. In: Proc. NCC, vol. 48, pp. 313–317. AFIPS Press (1979)
4. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols. In: 20th Annual ACM Symposium on Theory of Computing, STOC, pp. 11–19 (1988)
5. 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)

6. Fuchsbauer, G., Katz, J., Naccache, D.: Efficient Rational Secret Sharing in Standard Communication Networks. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 419–436. Springer, Heidelberg (2010)
7. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: 19th Annual ACM Symposium on Theory of Computing, STOC, pp. 218–229 (1987)
8. Halpern, J.Y., Teague, V.: Rational secret sharing and multiparty computation: extended abstract. In: 36th Annual ACM Symposium on Theory of Computing, STOC, pp. 623–632 (2004)
9. Harkavy, M., Tygar, J.D., Kikuchi, H.: Electronic auctions with private bids. In: 3rd Conference on USENIX Workshop on Electronic Commerce, WOEC, pp. 61–74. USENIX Association (1998)
10. Izmalkov, S., Micali, S., Lepinski, M.: Rational secure computation and ideal mechanism design. In: 46th Annual IEEE Symposium on Foundations of Computer Science, FOCS, pp. 585–595 (2005)
11. Katz, J.: Bridging Game Theory and Cryptography: Recent Results and Future Directions. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 251–272. Springer, Heidelberg (2008)
12. Kol, G., Naor, M.: Cryptography and Game Theory: Designing Protocols for Exchanging Information. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 320–339. Springer, Heidelberg (2008)
13. Kol, G., Naor, M.: Games for exchanging information. In: 40th Annual ACM Symposium on Theory of Computing, STOC, pp. 423–432 (2008)
14. Lepinski, M., Micali, S., Peikert, C., Shelat, A.: Completely fair sfe and coalition-safe cheap talk. In: 23th Annual ACM Symposium on Principles of Distributed Computing, PODC, pp. 1–10 (2004)
15. Lepinski, M., Micali, S., Shelat, A.: Collusion-free protocols. In: 37th Annual ACM Symposium on Theory of Computing, STOC, pp. 543–552 (2005)
16. Lysyanskaya, A., Triandopoulos, N.: Rationality and Adversarial Behavior in Multi-party Computation. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 180–197. Springer, Heidelberg (2006)
17. Mailath, G., Samuelson, L.: Repeated games and reputations: long-run relationships. Oxford University Press, USA (2006)
18. Maleka, S., Shareef, A., Rangan, C.P.: Rational Secret Sharing with Repeated Games. In: Chen, L., Mu, Y., Susilo, W. (eds.) ISPEC 2008. LNCS, vol. 4991, pp. 334–346. Springer, Heidelberg (2008)
19. Micali, S., shelat, a.: Purely Rational Secret Sharing (Extended Abstract). In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 54–71. Springer, Heidelberg (2009)
20. Nojoumian, M., Lethbridge, T.: A New Approach for the Trust Calculation in Social Networks. In: E-business and Telecommunication Networks: 3rd Int. Conf. on E-Business, ICE-B 2006, Best Papers, vol. 9, pp. 64–77. Springer (2008)
21. Nojoumian, M., Stinson, D., Grainger, M.: Unconditionally secure social secret sharing scheme. IET Information Security, Special Issue on Multi-Agent and Distributed Information Security 4(4), 202–211 (2010)
22. Nojoumian, M., Stinson, D.R.: Brief announcement: secret sharing based on the social behaviors of players. In: 29th ACM Symposium on Principles of Distributed Computing, PODC, pp. 239–240 (2010)
23. Osborne, M.J., Rubinstein, A.: A course in game theory. MIT Press (1994)
24. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)