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

Mehrdad Nojoumian *

David R. Cheriton School of Computer Science
University of Waterloo, Waterloo, Canada
mnojoumi@cs.uwaterloo.ca

Abstract. Rational secret sharing was proposed by Halpern and Teague in STOC'04. 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. We consider a "social model" for repeated rational secret sharing which has elegant properties. We propose a novel scheme, named *socio-rational secret sharing*, in which the players are invited to each game based on their reputations in the community. Indeed, they 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 several sealed-bids from the bidders in order to define 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. We show that this social reinforcement rationally stimulates the players to be cooperative.

Keywords: cryptography, game theory, reputation systems.

1 Introduction

The classical (t, n)-*secret sharing scheme* was proposed in [29, 5], 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 [29], 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 of size less than t cannot gain any information about the secret. The standard assumption in the traditional secret sharing is that each player is either *honest*

* Research supported by NSERC Canada Graduate Scholarship.

or *malicious* 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.

As started by Halpern and Teague [12], a new research direction was initiated in the area of secret sharing and multiparty computation in a game-theoretic sense. In this new construction, players are *rational* rather than being honest or malicious. This means they only act in their own self-interest. As illustrated by the authors, the classical secret sharing fails in this setting due to the failure of the secret reconstruction round. Here is a high-level description of the problem:

If players are incentivized to learn the secret while preferring fewer of other parties learn it, then it is not rational for each player to reveal his share in the recovery phase. For instance, consider a situation in which 3 players have shares on a polynomial of degree 2. If first two players reveal their shares, then the third player can reconstruct the secret by using the 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 (see [7, 15] for an overview in this direction).

Before providing our solution to the stated problem, we briefly introduce the notion of *social secret sharing* [25, 26] in which the player are either honest or malicious. In this protocol, weights of players, i.e., the number of shares each can hold, are periodically updated such that 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 calculation model to construct a new solution concept in rational cryptography.

1.1 Our Solution in Nutshell

The general idea is that each *rational foresighted player* is "selfish" and also has "concerns" about the future gain or loss, and the game (secret sharing) is going to be repeated over time for an unknown number of times. Each player has a reputation value which is adjusted each time the game is played. The initial value of the reputation is zero and its computation is public. If a player cooperates (e.g., reveal his share) his trust value is enhanced, otherwise, it is decreased. Then, the utility estimation (used for action selection) and utility gain (used for the real payment) are computed based on the following parameters:

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

That is, all three factors are used by each player to estimate his long-term utility and consequently select his action, whereas only the last two items are used to compute the real payment at the end of each game.

To estimate the future impact, we consider the following scenario: whenever a player cooperates, we assume he can potentially gain some extra units of utility (i.e., he has a chance to learn more secrets in the next games), and whenever he defects, we assume he can potentially lose some extra units of utility (i.e., he loses

a chance to learn more secrets in the next games). This gain or loss is **virtual** at the current time but will be **realized** in the future. As an example, consider a scenario in which a retail store says if you buy something today (cooperate), you will receive a discount (utility) on your next purchase (future). In other words, if the reputation of P_i is decreased, he will have less chance to be invited to the future secret sharing. Otherwise, P_i is going to be invited to more secret sharing. 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.

1.2 Our Motivation

In *secure multiparty computation* [9, 4, 6], 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 used by the players to inject their private data into a multiparty computation protocol. At the end of the computation, each player has a share of the function value. Therefore, they can collaborate to reveal this secret value. We can refer to *sealed-bid auctions* [13] as an application of multiparty computation. In a secure auction, the auctioneers receive the sealed-bids of the bidders in order to determine the auction outcome (i.e., the winner and the selling price) without revealing the losing bids. The main reason for using secret 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 the auction.

To motivate our "socio-rational secret sharing", consider the following repeated game, as shown in Figure 1. In this scheme, bidders initially agree to select a subset of auctioneers based on a non-uniform probability distribution over the auctioneers' types (that is, reputable, non-reputable, and newcomer). Each bidder then acts as an independent dealer to distribute the shares of his bid among the selected auctioneers. Subsequently, these auctioneers simulate a multiparty computation protocol to define the outcome. In the last phase of the computation, they are supposed to reconstruct the selling price α. In this setting, the seller pays money only to the auctioneers who have reported α; each of which can earn more money if fewer of them learn α. This scheme can be modeled as a "repeated" secret sharing game in a "rational" setting.

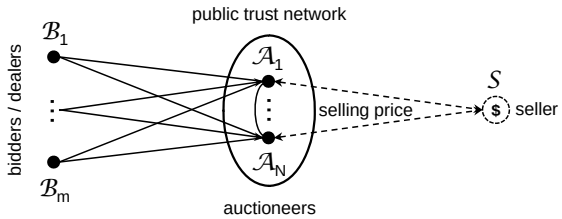


Fig. 1. Sealed-Bid Auction as a Repeated Secret Sharing Game

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 utilities. In other words, they avoid any 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 [21] for further discussions in this direction.

It is worth mentioning that our solution is independent of the security assumption and the communication model of its secret sharing scheme, i.e., any secret sharing scheme can be used in our proposed dealer-free construction. In addition, our scheme has the following elegant properties:

- It has a single reconstruction round.
- It provides a stable solution concept.
- It is immune to rushing attack.
- It prevents the players to abort.

Most of the existing solutions are not really fair since the protocol is aborted if a selfish player deviates. This means a selfish player can force the protocol to be executed for an exponential number of iterations (i.e., unfair punishment), which may cause the cryptographic primitives used in the scheme to be broken.

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

We now briefly review some definitions of [10] 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. A* **game** $\Gamma = (\mathcal{A}_i, u_i)$ *for* $1 \leq i \leq n$*, presented in normal form, is a set of possible actions* $\mathcal{A}_i$ *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 (i.e., 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 he samples $a_i \in \mathcal{A}_i$ according to σ_i. A strategy is said to be *pure-strategy* if each σ_i assigns probability 1 to an action, otherwise, it is said to be *mixed-strategy*. Let $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ be the vector of players' strategies, and let $(\sigma'_i, \boldsymbol{\sigma}_{-i}) \stackrel{\text{def}}{=} (\sigma_1, \ldots, \sigma_{i-1}, \sigma'_i, \sigma_{i+1}, \ldots, \sigma_n)$, i.e., only P_i changes σ_i into σ'_i and 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 rational player's goal is to maximize this utility. 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 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 $u_i(\sigma_i, \boldsymbol{\sigma}_{-i}) < u_i(\sigma'_i, \boldsymbol{\sigma}_{-i})$.*

Meaning that P_i can never improve its utility by playing σ_i, and can sometimes improve it by not playing σ_i. [1]

Definition 5. *Given $\Gamma = (\mathcal{A}_i, u_i)$ for $1 \leq i \leq n$ and a strategy profile $\mathcal{S}$, let $\mathcal{DOM}_i(\mathcal{S})$ denotes the set of strategies in $\mathcal{S}_i$ that are weakly dominated by other strategies with respect to $\mathcal{S}_{-i}$. Let $\mathcal{S}_i^0$ denotes the initial set of P_i's strategies.*

1. *For $k \geq 1$, define $\mathcal{S}_i^k \stackrel{\text{def}}{=} \mathcal{S}_i^{k-1} \setminus \mathcal{DOM}_i(\mathcal{S}^{k-1})$.*
2. *Let $\mathcal{S}_i^\infty \stackrel{\text{def}}{=} \bigcap_k \mathcal{S}_i^k$, i.e., strategies that are survived in all elimination rounds.*

We say $\sigma_i \in \mathcal{S}_i^\infty$ **survives iterated deletion** *of weakly dominated strategies.*

Nash equilibrium surviving iterated deletion of weakly dominated strategies are used in [12, 10, 20, 1].

2.2 Rational Secret Sharing Scheme

In this section, we briefly review *rational secret sharing*, initiated by Halpern and Teague [12]. This construction was later improved by Gordon and Katz [10]. The scheme consists of a *dealer* who holds a secret and n players $P_1, \ldots, P_n$.

The protocol proceeds in a sequence of iterations where only one iteration is the real reconstruction 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

[1] 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.

either terminates due to the selfish behavior's observation/cooperation for secret recovery, or proceeds to the next iteration otherwise. Indeed, in any given round, players do not know whether the current iteration is the real reconstruction phase (where a player may gain more utility by being silent and not sending his share to others), or just a test round in which a player must cooperate, otherwise, the other players abort the protocol.

To make this more clear, consider the following scenario for a player P_j where the degree of the secret sharing polynomial is $t-1$. If players 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 to learn it by not revealing his share, i.e., 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.

Let $u_i(\boldsymbol{a})$ denotes the utility of player P_i for 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 a specific outcome. We therefore define $\delta(\boldsymbol{a}) = \sum_i l_i(\boldsymbol{a})$ that denotes the number of players who have learned the secret. As proposed in [12], the following assumptions regarding players' utility functions are made:

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

The first assumption means P_i prefers the outcome in which he learns the secret, that is, since $l_i(\boldsymbol{a}) = 1$ and $l_i(\boldsymbol{a}') = 0$, therefore, he prefers $\boldsymbol{a}$. The second one means P_i prefers the outcome in which the fewest number of other players learn the secret. As illustrated in [12], the Nash equilibrium is too weak for rational secret sharing. As a result, they suggested to design a protocol that applies a NE surviving iterated deletion of weakly dominated strategies.

2.3 Social Secret Sharing Scheme

Now we review *social secret sharing*, introduced by Nojoumian et al. [25], 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 measure the reputation value, the authors apply the trust calculation method proposed in [24]; this work significantly improves the well-known solution in [30]. Next, we review this technique in order to use it in our scheme; the design of this function is out of the scope of our construction.

Definition 6. *Let $\mathcal{T}_i^j(p)$ be the trust value assigned by P_j to P_i in period p. Let $\mathcal{T}_i : \mathbb{N} \mapsto \mathbb{R}$ be the* **trust function** *representing the reputation of P_i.*

$$\mathcal{T}_i(p) = \frac{1}{n-1} \sum_{j \neq i} \mathcal{T}_i^j(p) \text{ where } -1 \leq \mathcal{T}_i(p) \leq +1 \text{ and } \mathcal{T}_i(0) = 0$$

$\mathcal{T}_i(p) = \mathcal{T}_i^j(p)$ if P_j for $1 \leq j \neq i \leq n$ have equal trust values for P_i, i.e., trust values (personal quantity) are equal to the reputation value (social quantity).

The general idea is to support good players, discredit bad ones, and create opportunities for newcomers whom we do not know much about their behaviors. As shown in Table 1, six possible actions and three sets $\mathcal{B}, \mathcal{N}, \mathcal{G}$ are defined for bad, new, and good players respectively, where α, β define boundaries on the trust values for different sets of players.

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

Table 1. Six Possible Actions for the Trust Management

This approach applies increasing and decreasing functions $\mu(x)$ and $\mu'(x)$ (where $P_i(\mathcal{C})$ denotes cooperation and $P_i(\mathcal{D})$ denotes defection) in order to update the trust (or reputation) value of each player P_i, as shown in Figure 2. For instance, by assigning $\eta = 0.01 < \theta = 0.05 < \kappa = 0.09$, we can simply define various points and construct an appropriate trust function via regression.

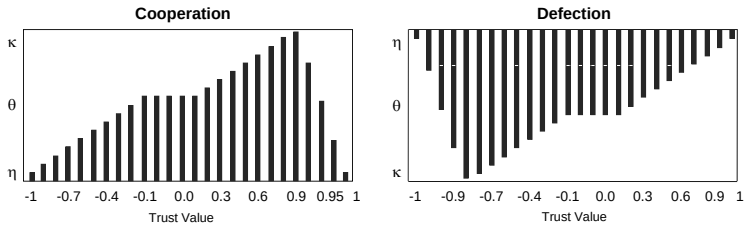


Fig. 2. Trust Adjustment by $\mu(x)$ and $\mu'(x)$ Functions

$$P_i(\mathcal{C}) \Rightarrow \mathcal{T}_i(p) = \mathcal{T}_i(p-1) + \mu(x) \qquad P_i(\mathcal{D}) \Rightarrow \mathcal{T}_i(p) = \mathcal{T}_i(p-1) - \mu'(x)$$

$$\mu(x) \in \begin{cases} [\eta, \theta) & P_i \in \mathcal{B} \text{ encourage} \\ \theta & P_i \in \mathcal{N} \text{ give a chance} \\ (\theta, \kappa] & P_i \in \mathcal{G} \text{ reward} \end{cases} \qquad \mu'(x) \in \begin{cases} [\kappa, \theta) & P_i \in \mathcal{B} \text{ penalize} \\ \theta & P_i \in \mathcal{N} \text{ take a chance} \\ (\theta, \eta] & P_i \in \mathcal{G} \text{ discourage} \end{cases}$$

It is worth mentioning that the authors also define λ as the *transaction cost* to fairly deal with *cheap* cooperations and *expensive* defections.

3 Literature Review

As we mentioned, the notion of *rational secret sharing* is introduced by Halpern and Teague [12], which is later improved in [10]. Assuming the same game-theoretic model, Lysyanskaya and Triandopoulos [20] 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 constructions in [18, 19, 14] rely on *physical assumptions* such as secure envelopes and ballot boxes. In the same model, Micali and shelat [23] provide a purely rational secret sharing scheme using a verifiable trusted channel. They show 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, if P_i believes that equilibrium (a, b) will be played whereas P_j believes equilibrium (a', b') is going to be played, then the game ends up with (a, b') which may not be an equilibrium at all.

Kol and Naor [17] introduce an equilibrium notion of *strict Nash equilibrium* in an information-theoretic secure setting. In Nash equilibrium, no deviations are advantageous (i.e., no incentive to deviate). In its strict counterpart, all deviations are disadvantageous (i.e., an incentive not to deviate). They first consider both simultaneous and non-simultaneous broadcast channels and then provide a new solution to avoid the simultaneous channel at the cost of increasing the round complexity by using the synchronous broadcast channel.

They later [16] show that all the existing computational-based cryptographic 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 *computational strict Nash equilibrium* is introduced in [8] which is a stable solution concept with respect to trembles. This construction is dealer-free and 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. [22] present *repeated rational secret sharing*, with the exact same approach proposed in [28], 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. These constructions are severely problematic. In the first one, 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* reconstruction without having

any concern for k subsequent *cheap* reconstructions. Indeed, the nature of a punishment strategy must depend on how much future outcomes are worth for each player. Finally, they only consider a fixed number of m players without considering newcomers.

Other results have been recently presented in the literature. For instance, Ong et al. [27] illustrate a protocol which is fair when the reconstruction phase is executed with many rational players together with a minority of honest parties. Asharov and Lindell [3] explain that in all the existing protocols, the designer needs to know the actual utility values of the players. They then show that it is possible to achieve utility independence through the relaxation of assumptions. Gradwohl et al. [11] provide the definitions of computational solution concepts that guarantee sequential rationality. Finally, Asharov et al. [2] show how game theoretic concepts can be used to capture cryptographic notions of security.

4 Socio-Rational Secret Sharing ($\mathcal{SRS}$)

We first provide the formal definitions of a *social game*, which is repeated for an unknown number of times, a *social Nash equilibrium*, and *socio-rational secret sharing*. In our model, we assume that trust values are equal to the reputation value of each P_i, i.e., $\mathcal{T}_i(p) = \mathcal{T}_i^j(p)$ for $1 \leq j \neq i \leq n$ where $\mathcal{T}_i(0) = 0$. The construction of this function is independent of our protocol, therefore, we apply the existing function proposed in [24]. Since the significance of each game might be different from case to case, we assume that the *transaction cost* (as stated in Section 2.3) is considered during trust adjustment. We should also stress that the trust function is not just a function of the round p, but of the history.

Definition 7. *Let $\mathcal{A} \stackrel{\text{def}}{=} \mathcal{A}_1 \times \cdots \times \mathcal{A}_N$ and $\mathcal{T} \stackrel{\text{def}}{=} \mathcal{T}_1 \times \cdots \times \mathcal{T}_N$ be the action and reputation profiles respectively. In a society S of size $|S| = N$, a* **social game** *$\Gamma = (\mathcal{A}_i, \mathcal{T}_i, u_i)$ is repeatedly played for an unbounded number of times among different subsets of players. It contains a set of possible actions $\mathcal{A}_i$, a trust value $\mathcal{T}_i$, and a utility estimation function u_i for each P_i. In each round of the game:*

- *A subset of players P_i, for $1 \leq i \leq n$ and $n \leq N$, is chosen based on $\mathcal{T}_i$, i.e, the reputable players have more chance to be selected. Let $\mathcal{A}' \stackrel{\text{def}}{=} \mathcal{A}_1 \times \cdots \times \mathcal{A}_n$.*
- *Then, $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathcal{A}'$ is said to be the game's outcome, and the utility of each P_i is computed based on a function $u_i' : \mathcal{A}' \mapsto \mathbb{R}$ in the current round.*
- *Finally, the reputation value $\mathcal{T}_i$ is publicly updated by a function $\mathcal{T} : \mathcal{A}_i \mapsto \mathbb{R}$ based on each player's action (or behavior) in the current round.*

The aggregated utility throughout the game Γ can be seen as a function $U_i : \mathcal{A} \times \mathcal{T}_i \mapsto \mathbb{R}$, and $u_i : \mathcal{A}' \times \mathcal{T}_i \mapsto \mathbb{R}$ estimates the utility of P_i in the current round by considering a few rounds further.

U_i denotes the **total utility** throughout Γ, u_i denotes the **utility estimation** of the current round and a few rounds further (used for action selection), and u_i' denotes the **actual utility** of the current round (used for the real payment).

Definition 8. *A vector of strategies* $\boldsymbol{\sigma}$ *is said to be a* **social Nash equilibrium** *in each round 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 a few rounds further, a player cannot gain any benefit by deviating from the protocol in the current round.*

We further discuss about the utility function which is a central part in every game. This is due to the fact that players make decision based on this function. The *utility assumption* refers to the players' preferences over the game's outcome whereas the *utility computation* shows the method of computing the utility of each player, also known as, utility function.

4.1 Utility Assumption

Let $u_i(\boldsymbol{a})$ denotes P_i's utility of $\boldsymbol{a}$ by considering a few rounds further, let $l_i(\boldsymbol{a})$ denotes if P_i has learned the secret, and define $\delta(\boldsymbol{a}) = \sum_i l_i(\boldsymbol{a})$. Finally, assume $\mathcal{T}_i^{\boldsymbol{a}}(p)$ shows the reputation of P_i after $\boldsymbol{a}$ in the round p of the game.

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

The preference A illustrates that whether P_i learns the secret or not he prefers to remain reputable. The preferences B and C are the standard assumptions of rational secret sharing.

Definition 9. *In a social game, a* **rational foresighted player** *has prioritized preferences:* $A^{\rho_1} \succ B^{\rho_2} \succeq C^{\rho_3}$*: A (greediness) is strictly preferred to B by the multiplicative factor* ρ_1*, B (selfishness) is at least as good as C by a significance factor* ρ_2*, and C (selfishness) with the impact factor* ρ_3*, where* $\rho_1 \gg \rho_2 \geq \rho_3 \geq 1$.

This means a rational foresighted player has a long-term vision and first prefers to achieve the highest level of trustworthiness. Only in that case, he would be involved in the future games and consequently gains more profits; this can be interpreted as greediness. He secondly prefers the outcome in which he learns the secret. Moreover, he desires the fewest number of other players learn it. We next construct a new utility function which satisfies all three preferences.

4.2 Utility Computation

Our proposed function $u_i : \mathcal{A}' \times \mathcal{T}_i \mapsto \mathbb{R}$ shows the utility that each player P_i can potentially gain or lose in a specific outcome by considering subsequent rounds.

I. Sample Function. Let $\omega_i(\boldsymbol{a}) = 3/(2 - \mathcal{T}_i^{\boldsymbol{a}}(p))$ where $\mathcal{T}_i^{\boldsymbol{a}}(p) \in [-1, +1]$, and let $\tau_i(\boldsymbol{a}) = \mathcal{T}_i^{\boldsymbol{a}}(p) - \mathcal{T}_i^{\boldsymbol{a}}(p-1)$. We assume $\Omega > 0$ to be a unit of utility, e.g., \$100. To satisfy the stated assumptions, consider the following mathematical terms:

$$A : \frac{|\tau_i(\boldsymbol{a})|}{\tau_i(\boldsymbol{a})} \times \omega_i(\boldsymbol{a}) \times \Omega, \text{ i.e., future gain or loss} \tag{1}$$

$$B : l_i(\boldsymbol{a}) \times \Omega \text{ where } l_i(\boldsymbol{a}) \in \{0, 1\} \tag{2}$$

$$C : \frac{\Omega}{\delta(\boldsymbol{a}) + 1} \text{ where } \delta(\boldsymbol{a}) = \sum_i l_i(\boldsymbol{a}) \tag{3}$$

1. The first equation would be $+\omega_i(\boldsymbol{a})\Omega$ if a player cooperates and it would be $-\omega_i(\boldsymbol{a})\Omega$ otherwise. This means a player gains or loses at least 1 and at most 3 (depending on his reputation value reflected in ω_i) units of utility in the future sharing due to his current behavior; although the gain or loss might be more than our estimation. This estimation is just for "action selection".
2. The second equation illustrate that a player gains one unit of utility if he learns the secret at the moment and he loses this opportunity otherwise.
3. The final equation expresses that one unit of utility is divided among all the players who have learned the secret.

We therefore combine these terms with their corresponding coefficients as follows:

$$u_i(\boldsymbol{a}) = \rho_1\left(\frac{|\tau_i(\boldsymbol{a})|}{\tau_i(\boldsymbol{a})} \times \omega_i(\boldsymbol{a}) \times \Omega\right) + \rho_2\left(l_i(\boldsymbol{a}) \times \Omega\right) + \rho_3\left(\frac{\Omega}{\delta(\boldsymbol{a}) + 1}\right) \tag{4}$$

$$= \Omega \times \left(\rho_1\left(\frac{|\tau_i(\boldsymbol{a})|}{\tau_i(\boldsymbol{a})} \times \omega_i(\boldsymbol{a})\right) + \rho_2\left(l_i(\boldsymbol{a})\right) + \rho_3\left(\frac{1}{\delta(\boldsymbol{a}) + 1}\right)\right) \tag{5}$$

This function illustrates that if a player defects (or cooperates), he may gain (or lose) a unit of utility Ω in the current round, but he will definitely lose (or gain) "x" units of utility in the future where $\Omega \leq x \leq 3\Omega$. We consider this estimation although it may not be precise due to the reduction (or amplification) of the reputation as an everlasting characteristic; it remains with the player in his entire life. In addition, we later show that the dealer gives less (or more) chance of contribution to non-reputable (or reputable) players in the future games.

II. General Function. It is worth mentioning that one can design any arbitrary function as long as it satisfies our utility assumptions. For instance, instead of using $\delta(\boldsymbol{a})$, we can define a function $f(\delta(\boldsymbol{a}))$ where $f : \{0, \ldots, n\} \mapsto \mathbb{R}$ in order to consider the number of players learning the secret, and so forth. A perfect design of this function is out of the scope of this paper. Our intention is to show the impact of the first property on socio-rational secret sharing, in which rational foresighted players with future concerns are considered.

Proposition 1. *A utility function F_i with the following linear combination of preference factors $\rho_1 \gg \rho_2 \geq \rho_3 \geq 1$ and functions $f_1(\mathcal{T}_i), f_2(l_i), f_3(\delta)$ satisfies the preference of a rational foresighted player, that is, $A^{\rho_1} \succ B^{\rho_2} \succeq C^{\rho_3}$, where $|f_1|$ is a monotonically increasing function, f_3 is a monotonically decreasing function (excluding zero), and $|f_1(\mathcal{T}_i)| \geq f_2(l_i) \geq f_3(\delta)$ except that $f_2(0) < f_3(0)$.*

$$F_i(\boldsymbol{a}) = \Omega\Big(\rho_1 f_1(\mathcal{T}_i) + \rho_2 f_2(l_i) + \rho_3 f_3(\delta)\Big) \tag{6}$$

$$f_1 : \begin{cases} \mathbb{R}_{>0} & \tau_i > 0 \\ \mathbb{R}_{<0} & \textit{otherwise} \end{cases} \qquad f_2 : \begin{cases} 0 & l_i = 0 \\ \mathbb{R}_{>0} & l_i = 1 \end{cases} \qquad f_3 : \begin{cases} 1 & \delta = 0 \\ \mathbb{R}_{>0} & \delta \in \{1 \dots n\} \end{cases}$$

Proof. Due to the lack of space, we leave the proof but only analyze the situation in which $f_2(0) < f_3(0)$, i.e., $l_i = 0$ and $\delta = 0$ (no one has learned the secret). This means that at most $t-1$ players, where t is the threshold, have cooperated. As a result, P_i is either among the cooperative players who have revealed their shares or among the non-cooperative parties. However, the first property states that P_i potentially gains more utilities if he enhances his reputation, no matter if he learns the secret or not. Therefore, in the case of the cooperation we have:

$$P_i(\mathcal{C}) : (\tau_i > 0, f_2 = 0, f_3 = 1) \text{ then } u_i^{P_i(\mathcal{C})}(\boldsymbol{a}) = \Omega\Big(\rho_1 f_1 + \rho_3\Big)$$

We can simply compute the utility of P_i in the case of the defection as follows:

$$P_i(\mathcal{D}) : (\tau_i < 0, f_2 = 0, f_3 = 1) \text{ then } u_i^{P_i(\mathcal{D})}(\boldsymbol{a'}) = \Omega\Big(-\rho_1 f_1 + \rho_3\Big)$$

Consequently we get $u_i^{P_i(\mathcal{C})}(\boldsymbol{a}) > u_i^{P_i(\mathcal{D})}(\boldsymbol{a'})$ which confirms the statement. □

4.3 Proposed Protocol

Before illustrating any details, we first define socio-rational secret sharing. For the sake of simplicity, let assume all the players use a "pure-strategy".

Definition 10. *A* **socio-rational secret sharing** *$\Gamma = (\mathcal{A}_i, \mathcal{T}_i, u_i)$ is a social game with (1) an action set $\mathcal{A}_i = \{\mathcal{C}, \mathcal{D}\}$, (2) a trust function $\mathcal{T}_i$ for rational foresighted players with types $\mathcal{G}, \mathcal{N}, \mathcal{B}$, as defined in Section 2.3, and (3) a utility estimation function $u_i : \mathcal{A}' \times \mathcal{T}_i \mapsto \mathbb{R}$, as defined in Section 4.2.*

Our socio-rational secret sharing scheme is illustrated in Figure 3. For the sake of simplicity, suppose the public trust network has already been constructed, and assume we only have a single dealer.[2]

[2] In the context of rational secret sharing, "defection" means a player has not revealed his share during the reconstruction phase, but sending incorrect shares is another issue which can be simply prevented by having the dealer sign the shares. For a simple example of such an authentication, see [17]: the third footnote.

As you can see, the sharing phase is similar to that of the regular secret sharing. The only difference is the way that the dealer selects n players out of N for secret sharing. In other words, the dealer gives more chance to reputable players compared to unreliable parties. This method of selection realizes the term $\rho_1 f_1(\mathcal{T}_i)$ in our utility estimation function. Although it is the best approach to invite only the reputable players, it is not fair if the dealer does not provide any opportunity for the newcomers, or if he completely ignores the bad players. Once in a while he should give a chance to the bad players such that they can compensate for their past behaviors. This is a realistic approach even in human society and can be interpreted as a "forgiveness factor".

The secret recovery phase is also similar to that of the standard secret sharing. This means any scheme can be selected independent of its security assumption and the communication model. In fact, we attach a reputation system along with our new game-theoretic model to rational secret sharing. We should also mention that since the players' reputations and the trust function are public information, therefore, all computations associated to the reputation system can be done by any authority or a committee of the players.

Secret Sharing

1. Let ϕ be the probability distribution over players' types $\mathcal{B}, \mathcal{N}, \mathcal{G}$. The dealer first selects n players out of N, where $n \leq N$, from the society based on this non-uniform probability distribution:

$$\phi = \sum_{j \in \{\mathcal{B},\mathcal{N},\mathcal{G}\}} \phi_j = 1 \text{ where } \phi_{\mathcal{B}} \ll \phi_{\mathcal{N}} < \phi_{\mathcal{G}}$$

2. The dealer then initiates a secret sharing scheme by selecting a polynomial $f(x) \in \mathbb{Z}_q[x]$ of degree $t-1$ where $f(0) = \alpha$ is the secret. Subsequently, he sends shares $f(i)$ to P_i for $1 \leq i \leq n$, and leaves the scheme.

Secret Recovery

1. Each player P_i computes his utility estimation 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 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 players are publicly updated according to each player's behavior and the trust function $\mathcal{T} : \mathcal{A}_i \mapsto \mathbb{R}$.

Fig. 3. Socio-Rational Secret Sharing Protocol

It is worth mentioning that it is not required to consider unknown number of iterations in the reconstruction of a secret (which is the case in all the existing rational secret sharing schemes) since we consider socio-rational secret sharing as a repeated game. In other words, those iterations in the reconstruction phase of the standard rational secret sharing are conceptually stretched over time on sequential reconstructions of different secrets in a socio-rational setting. Next, we initially analyze the 2-out-of-2 case by considering our sample function in Equation (5), and then we use the general form of our utility function.

Theorem 1. *In our $(2,2)$-socio-rational secret sharing, $\mathcal{C}$ strictly dominates $\mathcal{D}$, considering our sample utility function. In other words, $\mathcal{D}$ is strictly dominated by $\mathcal{C}$. As a result, $(\mathcal{C},\mathcal{C})$ is a strict social NE which is a unique solution.*

Proof. We compute the utility of each outcome for P_i. For the sake of simplicity we assume $\omega_i(\boldsymbol{a}) = 1$; although the proof is valid for all values of $\omega_i(\boldsymbol{a}) \in [1,3]$:

1. $(\mathcal{C},\mathcal{C}) : (\tau_i > 0, l_i = 1, \delta = 2)$ then $u_i^{(\mathcal{C},\mathcal{C})}(\boldsymbol{a}) = \Omega\Big(\rho_1 + \rho_2 + \frac{\rho_3}{3}\Big)$
2. $(\mathcal{C},\mathcal{D}) : (\tau_i > 0, l_i = 0, \delta = 1)$ then $u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a}) = \Omega\Big(\rho_1 + \frac{\rho_3}{2}\Big)$
3. $(\mathcal{D},\mathcal{C}) : (\tau_i < 0, l_i = 1, \delta = 1)$ then $u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a}) = \Omega\Big(-\rho_1 + \rho_2 + \frac{\rho_3}{2}\Big)$
4. $(\mathcal{D},\mathcal{D}) : (\tau_i < 0, l_i = 0, \delta = 0)$ then $u_i^{(\mathcal{D},\mathcal{D})}(\boldsymbol{a}) = \Omega\Big(-\rho_1 + \rho_3\Big)$

We simply ignore the common term Ω. Since $\rho_1 \gg \rho_2 \geq \rho_3 \geq 1$, we have:

$$\begin{aligned}
u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a}) &= \rho_1 + \frac{\rho_3}{2} \\
&\leq \rho_1 + \frac{\rho_2}{2} \\
&< \rho_1 + \rho_2 \\
&< \rho_1 + \rho_2 + \frac{\rho_3}{3} = u_i^{(\mathcal{C},\mathcal{C})}(\boldsymbol{a}) \\
u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a}) &= -\rho_1 + \rho_2 + \frac{\rho_3}{2} \\
&< \rho_2 + \frac{\rho_3}{2} \\
&< \rho_1 + \frac{\rho_3}{2} = u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a}) \\
u_i^{(\mathcal{D},\mathcal{D})}(\boldsymbol{a}) &= -\rho_1 + \rho_3 \\
&\leq -\rho_1 + \rho_2 \\
&< -\rho_1 + \rho_2 + \frac{\rho_3}{2} = u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a})
\end{aligned}$$

Consequently, we gain the following payoff inequality which proofs the theorem:

$$\overbrace{u_i^{(\mathcal{C},\mathcal{C})}(\boldsymbol{a}) > u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a})}^{P_i \text{ cooperates}} > \overbrace{u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a}) > u_i^{(\mathcal{D},\mathcal{D})}(\boldsymbol{a})}^{P_i \text{ defects}} \tag{7}$$

The interesting observation is the difference between two consecutive utilities $u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a})$ and $u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a})$. This means it is better for P_i to cooperate even if he knows he will not learn the secret whereas the other party will learn it. On the other hand, even if P_i learns the secret by deviating at the moment and using the share of the other party, he will gain less utility. This is due to the potential future gain or loss and the significance of being reputable in a society. □

As we mentioned earlier, a more realistic approach by common sense is to consider a suitable multiplicative factor ρ_1 for the estimation of the future loss (or gain). In that case, the enforcement for the cooperation would be even more and the following inequality is going to be hold:

$$u_i^{(\mathcal{C},\mathcal{C})}(\boldsymbol{a}) > u_i^{(\mathcal{C},\mathcal{D})}(\boldsymbol{a}) \overset{\rho_1}{\gg} u_i^{(\mathcal{D},\mathcal{C})}(\boldsymbol{a}) > u_i^{(\mathcal{D},\mathcal{D})}(\boldsymbol{a}) \tag{8}$$

In all the existing solutions, the payoff matrix shown in Table 2 has been considered. This matrix satisfies the properties B and C without defining any impact factors, where $\mathcal{U}^+ > \mathcal{U} > \mathcal{U}^- > \mathcal{U}^{--}$. The payoff matrix associated to socio-rational secret sharing is illustrated in Table 3, which satisfies all three preference assumptions.

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 2. $(2,2)$-Rational SS [3]

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

We should state that our socio-rational game is a non-cooperative game. In fact, the cooperation is self-enforcing due to (a) the importance of reputation and (b) future concerns of a rational foresighted player who decides individually. In a cooperative game, this enforcement is provided by a third party and players do not really compete. Second, this payoff matrix does not mean that players never deviate. As an example, consider a scenario in which a player is involved in different societies. If he simultaneously receives many requests for cooperation in the secret recovery phase of various schemes, he will select the one in which he can gain more utility, of course, by considering his reputation.

Theorem 2. *In a socio-rational secret sharing scheme with n parties, $\mathcal{C}$ strictly dominates $\mathcal{D}$ for all players P_i, assuming the preferences of rational foresighted parties. Consequently, the vector $\boldsymbol{a}^{\mathcal{C}} = (a_1^{\mathcal{C}}, \ldots, a_n^{\mathcal{C}})$ (or $\boldsymbol{\sigma}^{\mathcal{C}} = (\sigma_1^{\mathcal{C}}, \ldots, \sigma_n^{\mathcal{C}})$ in the case of the mixed-strategy) is a strict social NE as a unique solution.*

Proof. We first compute the utility of each outcome based on Equation (6) for the least possible threshold $t = 2$ where $n > 2$, i.e., two shares are enough to

learn the secret. $\mathcal{C}_i$ (or $\mathcal{D}_i$) denotes P_i cooperates (or defects), $\mathcal{C}_{-i}$ (or $\mathcal{D}_{-i}$) denotes, excluding P_i, all the other players cooperate (or defect), and $\mathcal{M}_{-i}$ denotes, excluding P_i, some players cooperate and some of them defect, i.e., we have both $\mathcal{C}$ooperation and $\mathcal{D}$efection.

1. $(\mathcal{C}_i, \mathcal{C}_{-i}) : (\tau_i > 0, l_i = 1, \delta = n)$
$$u_i^{(\mathcal{C}_i, \mathcal{C}_{-i})}(\boldsymbol{a}) = \Omega\Big(\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3(n)\Big)$$
2. $(\mathcal{C}_i, \mathcal{M}_{-i}) : (\tau_i > 0, l_i = 1, \delta = n)$
$$u_i^{(\mathcal{C}_i, \mathcal{M}_{-i})}(\boldsymbol{a}) = \Omega\Big(\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3(n)\Big)$$
3. $(\mathcal{C}_i, \mathcal{D}_{-i}) : (\tau_i > 0, l_i = 0, \delta = n-1)$
$$u_i^{(\mathcal{C}_i, \mathcal{D}_{-i})}(\boldsymbol{a}) = \Omega\Big(\rho_1 f_1 + \rho_3 f_3(n-1)\Big)$$
4. $(\mathcal{D}_i, \mathcal{C}_{-i}) : (\tau_i < 0, l_i = 1, \delta = n)$
$$u_i^{(\mathcal{D}_i, \mathcal{C}_{-i})}(\boldsymbol{a}) = \Omega\Big(-\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3(n)\Big)$$
5. $(\mathcal{D}_i, \mathcal{M}_{-i}) : (\tau_i < 0, l_i = 1, \delta \in \{n-1, n\})$
$$u_i^{(\mathcal{D}_i, \mathcal{M}_{-i})}(\boldsymbol{a}) = \Omega\Big(-\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3(\delta)\Big)$$
6. $(\mathcal{D}_i, \mathcal{D}_{-i}) : (\tau_i < 0, l_i = 0, \delta = 0)$
$$u_i^{(\mathcal{D}_i, \mathcal{D}_{-i})}(\boldsymbol{a}) = \Omega\Big(-\rho_1 f_1 + \rho_3\Big)$$

As before, we ignore the common term Ω. Since the utilities of items 1 and 2 as well as 4 and 5 are almost equal, we ignore the items 2 and 5. Based on our proposed utility function, we have:

$$\begin{aligned}
u_i^{(\mathcal{C}_i, \mathcal{D}_{-i})}(\boldsymbol{a}) &= \rho_1 f_1 + \rho_3 f_3(n-1) \\
&\leq \rho_1 f_1 + \rho_3 f_2 \\
&\leq \rho_1 f_1 + \rho_2 f_2 \\
&< \rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3(n) = u_i^{(\mathcal{C}_i, \mathcal{C}_{-i})}(\boldsymbol{a}) \\
u_i^{(\mathcal{D}_i, \mathcal{C}_{-i})}(\boldsymbol{a}) &= -\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3(n) \\
&\leq -\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_2 \\
&\leq -\rho_1 f_1 + \rho_2 f_2 + \rho_2 f_2 \\
&< -\rho_1 f_1 + \rho_1 f_2 + \rho_1 f_2 = \rho_1(2f_2 - f_1) \\
&\leq \rho_1 f_1 \text{ since } f_2 \leq f_1 \\
&< \rho_1 f_1 + \rho_3 f_3(n-1) = u_i^{(\mathcal{C}_i, \mathcal{D}_{-i})}(\boldsymbol{a}) \\
u_i^{(\mathcal{D}_i, \mathcal{D}_{-i})}(\boldsymbol{a}) &= -\rho_1 f_1 + \rho_3 \\
&\leq -\rho_1 f_1 + \rho_2 \\
&\leq -\rho_1 f_1 + \rho_2 f_2 \\
&< -\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3(n) = u_i^{(\mathcal{D}_i, \mathcal{C}_{-i})}(\boldsymbol{a}) \text{ where } f_2 \neq 0
\end{aligned}$$

Consequently, we gain the following payoff inequality:

$$\overbrace{u_i^{(\mathcal{C}_i,\mathcal{C}_{-i})}(\boldsymbol{a}) > u_i^{(\mathcal{C}_i,\mathcal{D}_{-i})}(\boldsymbol{a})}^{P_i \text{ cooperates}} > \overbrace{u_i^{(\mathcal{D}_i,\mathcal{C}_{-i})}(\boldsymbol{a}) > u_i^{(\mathcal{D}_i,\mathcal{D}_{-i})}(\boldsymbol{a})}^{P_i \text{ defects}} \tag{9}$$

The same result can be gained for any values of t, which proofs the theorem. □

Expected Utility. In this section, we show how each player can compute his expected utility. This is specifically useful if he would like to decide on different requests received from various societies, i.e., $\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}) \stackrel{?}{>} \mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}')$ where $\boldsymbol{a}, \boldsymbol{a}'$ are associated to different games.

The utility value represents the connection between actions and their corresponding consequences for a player whereas the *expected utility* of P_i is an estimation of gain or loss when he plays with a player P_j. We therefore compute the expected utility with a linear combination of utility values and the probability of P_j's cooperation. Let $\epsilon_j = (\mathcal{T}_j^{\boldsymbol{a}}(p) + 1)/2$ where $\epsilon_j \in [0, 1]$ shows how probably the opponent P_j may cooperate.

$$\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}) = \epsilon_j \, \mathcal{U}^{+} + (1 - \epsilon_j) \, \mathcal{U} \tag{10}$$

$$\mathcal{EU}_i^{\mathcal{D}}(\boldsymbol{a}) = \epsilon_j \, \mathcal{U}^{-} + (1 - \epsilon_j) \, \mathcal{U}^{--} \tag{11}$$

Corollary 1. *In our socio-rational secret sharing,* $\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}) \stackrel{always}{>} \mathcal{EU}_i^{\mathcal{D}}(\boldsymbol{a})$.

Proof.

$$\begin{gathered}
\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}) > \mathcal{EU}_i^{\mathcal{D}}(\boldsymbol{a}) \\
\epsilon_j \, \mathcal{U}^{+} + (1 - \epsilon_j) \, \mathcal{U} > \epsilon_j \, \mathcal{U}^{-} + (1 - \epsilon_j) \, \mathcal{U}^{--} \\
\epsilon_j \, (\mathcal{U}^{+} - \mathcal{U}^{-}) > (1 - \epsilon_j) \, (\mathcal{U}^{--} - \mathcal{U}) \\
\frac{\mathcal{U}^{+} - \mathcal{U}^{-}}{\mathcal{U}^{--} - \mathcal{U}} < \frac{1 - \epsilon_j}{\epsilon_j} \quad \text{since } (\mathcal{U}^{--} - \mathcal{U}) < 0
\end{gathered}$$

Since $\epsilon_j \in [0, 1]$ and the LH side is negative, the inequality is always hold. □

Corollary 2. *In our social setting, players have more motivation to cooperate with trustworthy parties or contribute in a society with more reliable participants.*

Proof. Suppose P_i is involved in two games with P_j and P_k who have different reputation values, for instance, let $\epsilon_j > \epsilon_k$. Assume P_i receives the same unit of utility in both games, and let $\boldsymbol{a}_{ij}, \boldsymbol{a}_{ik}$ be the outcomes of two games accordingly. We therefore have:

$$\begin{gathered}
\mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}_{ij}) \stackrel{?}{>} \mathcal{EU}_i^{\mathcal{C}}(\boldsymbol{a}_{ik}) \\
\epsilon_j \, \mathcal{U}^{+} + (1 - \epsilon_j) \, \mathcal{U} \stackrel{?}{>} \epsilon_k \, \mathcal{U}^{+} + (1 - \epsilon_k) \, \mathcal{U} \\
\epsilon_j \, \mathcal{U}^{+} - \epsilon_k \, \mathcal{U}^{+} \stackrel{?}{>} (1 - \epsilon_k) \, \mathcal{U} - (1 - \epsilon_j) \, \mathcal{U} \\
(\epsilon_j - \epsilon_k) \, \mathcal{U}^{+} \stackrel{?}{>} (\epsilon_j - \epsilon_k) \, \mathcal{U} \quad \text{since } \epsilon_j > \epsilon_k \\
\mathcal{U}^{+} > \mathcal{U} \quad \text{which is true}
\end{gathered}$$

□

5 Comparison with the Existing Techniques

1. 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, and it deals with the problem of secret recovery in the presence of rational players.
- "Social secret sharing" defines how many shares each player can hold in a weighted secret sharing scheme with honest and malicious parties.

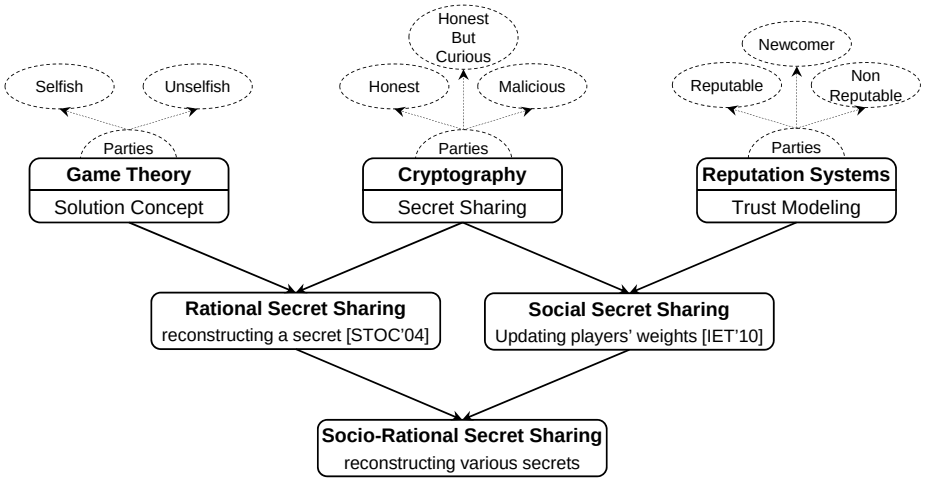


Fig. 4. Pedigree of the Socio-Rational Secret Sharing

2. Our contribution is totally different from the *punishment strategy* used in the *repeated prisoners' dilemma* [28] 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. For instance, consider the prisoners' dilemma with $\mathcal{C}ooperation$ and $\mathcal{D}efection$ actions. Both players cooperate until one of them deviates. Then, the other player chooses $\mathcal{D}$ for a specific number of times as a punishment. Meanwhile, the deviant rewards the punisher by selecting $\mathcal{C}$ as a compensation. Finally, the game returns to the mutual cooperation. Indeed, our approach has the following advantages over the punishment strategy:

- In our model, a player is not just an abstract entity who selects actions. It also has a social characteristic reflected in his reputation that shows his trustworthiness. This attribute is solely built by the player himself.
- 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 extend, 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 importance and utility weights whenever it is repeatedly played. For instance, whether it is a secret sharing for a "missile launch" or for 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 to regain the lost reputation.
- Our proposed approach not only consider punishment or reward but also defines six different scenarios in order to fairly deal with various types of players including good player, bad player, and newcomers.

3. Our contribution is also different from the constructions forming histories and beliefs such as *subgame perfect equilibrium* or *Bayesian equilibrium* [28]. 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 behaviors.

Let P_i be a specific player and P_j for $1 \leq j \neq i \leq n$ denotes all the other players except P_i. More specifically, our trust calculation method and social setting differs from these kinds of solution concepts in the following aspects:

- 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 P_j-s 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 a common knowledge meaning that various players may have different judgments and beliefs about P_i. Whereas, the reputation of P_i in a trust network is solely constructed by his behavior through a trust function, which is a commonly known function for the reputation measurement. That is, the reputation is a direct reflection of P_i's attitude (no misunderstanding), and he very well knows the impact of his decision on the other players' mind considering his current characteristic (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, which is a strong enforcement.
- 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. Whereas, the reputation is built over a specific set of actions, such as $\mathcal{C}$ooperation and

$\mathcal{D}$efection ($\mathcal{X}$: corruption as a malicious behavior might be also considered in a mixed model), for a specific types of players, such as good or bad players, and newcomers. As a result, the reputation system is simpler to be analyzed in a solution concept and it is more suitable for cryptographic constructions.

- In the history and belief systems all the measurements are inside of 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 the past behaviors [3]. But our publicly known trust function combines these two measurements in a single reputation value outside of the game-theoretic model (although these values might be interpreted similar to "types" and "beliefs"). 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 in order to propose a novel solution for one of the most fundamental cryptographic primitives.

As we illustrated, the social network with reputation consideration is a strong enforcement for the participants to cooperate, for instance, a player may change his non-cooperative approach after analyzing his reputation, or after estimating his future loss. In our social setting, bad players can compensate for their past behavior by continuous cooperation. On the other hand, reputable players can gain more profits as long as they act properly, and newcomers can fairly start their social interactions. Finally, we should stress 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 to 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 behaviors whereas belief can be viewed as an anticipation of the future activities.

[3] P_i is good or bad with 0.7 or 0.3 probabilities respectively. Based on that, a P_j may belief that P_i reveals or not reveals his share with 0.9 or 0.1 probabilities accordingly.

References

1. Abraham, I., Dolev, D., Gonen, R., and 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* (2006), pp. 53–62.
2. Asharov, G., Canetti, R., and Hazay, C. Towards a game theoretic view of secure computation. In *30th Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT* (2011), vol. 6632 of *LNCS*, Springer, pp. 426–445.
3. Asharov, G., and Lindell, Y. Utility dependence in correct and fair rational secret sharing. In *29th Annual International Cryptology Conference CRYPTO* (2009), vol. 5677 of *LNCS*, Springer, pp. 559–576.
4. Ben-Or, M., Goldwasser, S., and Wigderson, A. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *20th Annual ACM Symposium on Theory of Computing STOC* (1988), pp. 1–10.
5. Blakley, G. Safeguarding cryptographic keys. In *Proc. NCC* (1979), vol. 48, AFIPS Press, pp. 313–317.
6. Chaum, D., Crépeau, C., and Damgård, I. Multiparty unconditionally secure protocols. In *20th Annual ACM Symposium on Theory of Computing STOC* (1988), pp. 11–19.
7. Dodis, Y., Halevi, S., and Rabin, T. A cryptographic solution to a game theoretic problem. In *20th Annual International Cryptology Conference CRYPTO* (2000), vol. 1880 of *LNCS*, Springer, pp. 112–130.
8. Fuchsbauer, G., Katz, J., and Naccache, D. Efficient rational secret sharing in standard communication networks. In *7th Theory of Cryptography Conference TCC* (2010), vol. 5978 of *LNCS*, Springer, pp. 419–436.
9. Goldreich, O., Micali, S., and 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* (1987), pp. 218–229.
10. Gordon, S. D., and Katz, J. Rational secret sharing, revisited. In *5th International Conference on Security and Cryptography for Networks SCN* (2006), vol. 4116 of *LNCS*, Springer, pp. 229–241.
11. Gradwohl, R., Livne, N., and Rosen, A. Sequential rationality in cryptographic protocols. In *51th Annual IEEE Symposium on Foundations of Computer Science FOCS* (2010), pp. 623–632.
12. Halpern, J. Y., and Teague, V. Rational secret sharing and multiparty computation: extended abstract. In *36th Annual ACM Symposium on Theory of Computing STOC* (2004), pp. 623–632.
13. Harkavy, M., Tygar, J. D., and Kikuchi, H. Electronic auctions with private bids. In *3rd Conference on USENIX Workshop on Electronic Commerce WOEC* (1998), USENIX Association, pp. 61–74.
14. Izmalkov, S., Micali, S., and Lepinski, M. Rational secure computation and ideal mechanism design. In *46th Annual IEEE Symposium on Foundations of Computer Science FOCS* (2005), pp. 585–595.
15. Katz, J. Bridging game theory and cryptography: Recent results and future directions. In *5th Theory of Cryptography Conference TCC* (2008), vol. 4948 of *LNCS*, Springer, pp. 251–272.
16. Kol, G., and Naor, M. Cryptography and game theory: Designing protocols for exchanging information. In *5th Theory of Cryptography Conference TCC* (2008), vol. 4948 of *LNCS*, Springer, pp. 320–339.

17. Kol, G., and Naor, M. Games for exchanging information. In *40th Annual ACM Symposium on Theory of Computing STOC* (2008), pp. 423–432.
18. Lepinski, M., Micali, S., Peikert, C., and Shelat, A. Completely fair sfe and coalition-safe cheap talk. In *23th Annual ACM Symposium on Principles of Distributed Computing PODC* (2004), pp. 1–10.
19. Lepinski, M., Micali, S., and Shelat, A. Collusion-free protocols. In *37th Annual ACM Symposium on Theory of Computing STOC* (2005), pp. 543–552.
20. Lysyanskaya, A., and Triandopoulos, N. Rationality and adversarial behavior in multi-party computation. In *26th International Cryptology Conference CRYPTO* (2006), vol. 4117 of *LNCS*, Springer, pp. 180–197.
21. Mailath, G., and Samuelson, L. *Repeated games and reputations: long-run relationships*. Oxford University Press, USA, 2006.
22. Maleka, S., Shareef, A., and Rangan, C. P. Rational secret sharing with repeated games. In *4th Int. Conf. on Information Security Practice and Experience ISPEC* (2008), vol. 4991 of *LNCS*, Springer, pp. 334–346.
23. Micali, S., and Shelat, A. Purely rational secret sharing. In *6th Theory of Cryptography Conference TCC* (2009), vol. 5444 of *LNCS*, Springer, pp. 54–71.
24. Nojoumian, M., and 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'06, Best Papers* (2008), vol. 9, Springer, pp. 64–77.
25. Nojoumian, M., Stinson, D., and Grainger, M. Unconditionally secure social secret sharing scheme. *IET Information Security, Special Issue on Multi-Agent and Distributed Information Security 4*, 4 (2010), 202–211.
26. Nojoumian, M., and Stinson, D. R. Brief announcement: secret sharing based on the social behaviors of players. In *29th ACM symposium on Principles of distributed computing PODC* (2010), pp. 239–240.
27. Ong, S. J., Parkes, D. C., Rosen, A., and Vadhan, S. P. Fairness with an honest minority and a rational majority. In *6th Theory of Cryptography Conference TCC* (2009), vol. 5444 of *LNCS*, Springer, pp. 36–53.
28. Osborne, M. J., and Rubinstein, A. *A course in game theory*. MIT press, 1994.
29. Shamir, A. How to share a secret. *Communications of the ACM 22*, 11 (1979), 612–613.
30. Yu, B., and Singh, M. P. A social mechanism of reputation management in electronic communities. In *4th International Workshop on Cooperative Information Agents CIA* (2000), vol. 1860 of *LNCS*, Springer, pp. 154–165.