Generalization of Socio-Rational Secret Sharing with a New Utility Function

Mehrdad Nojoumian
Department of Computer Science
Southern Illinois University, Carbondale, Illinois, USA
nojoumian@cs.siu.edu

***Abstract*—Rational secret sharing shows 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 parties. However, in socio-rational secret sharing, players not only are rational but also are foresighted. In other words, the secret sharing game is repeatedly played and players are only invited to each game based on their reputation. This social reinforcement stimulates the players to be cooperative. As our contribution, we revisit socio-rational secret sharing and generalize it from the utility computation aspect. We show that, in $(2, 2)$ and (t, n) socio-rational secret sharing, it is always in players' best interest to cooperate using our new utility function.**

Keywords: secret sharing, social secret sharing, socio-rational secret sharing, rational cryptography, trust management.

I. Introduction

The *threshold secret sharing* (TSS) was proposed in [1], where a dealer distributes shares of a secret among n players for a subsequent secret recovery. In this scheme, the dealer initially creates a random polynomial $f(x) \in \mathbb{Z}_q[x]$ of degree $t-1$ such that the constant term is the secret. He then sends $f(i)$ to player P_i for $1 \leq i \leq n$. As a result, any group of t or more players can recover the secret whereas any group of size less than t cannot gain any information about the secret.

In *rational secret sharing* (RSS) [2], 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. To further illustrate this, consider the following scenario for a player P_j where the degree of the secret sharing polynomial is $t-1$. If other players, denoted by P_i for $i < t-1$ or $i > t-1$, 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, P_j can not only learn the secret with his own private share but also can prevent the other players from learning the secret by not revealing his share.

In *social secret sharing* (SSS) [3], players' shares are allocated based on their reputation and the way that they interact with each other. In other words, weights of the players are adjusted such that parties who cooperate receive more shares compared to non-cooperative players. 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*.

In *socio-rational secret sharing* (SRS) [4], players are *rational* similar to standard rational secret sharing. In addition, they are *foresighted* and have concerns about future gain or loss since the secret sharing game is repeated for an unknown number of rounds. In the proposed scheme, each player has a reputation value which is updated according to his behavior each time the game is played. For instance, if a player cooperates (he reveals his share), his trust value is increased and he will be invited to more games in the future, otherwise, his trust value is decreased and he will have less chance to be invited to the future games.

Note that the existing trust function of [5] is used for trust management in social and socio-rational secret sharing.

II. Rational Secret Sharing

Rational secret sharing consists of a dealer D, who creates a secret sharing scheme with threshold t, and n players. The protocol proceeds in a sequence of iterations where only one iteration is the "real" secret recovery round (i.e., the last iteration) and the rest are "fake" iterations in order to trap selfish players. At the end of each iteration, the protocol either terminates or it proceeds to the next round. In fact, in any given iteration, players do not know whether the current round is the real recovery phase or a test round. The following steps illustrate the initial solution to the rational secret sharing game, where $n = t = 3$ and shares are revealed simultaneously [2]. See Table I for all the possibilities that may occur.

(a) In each round, D initiates a fresh secret sharing scheme where each player P_i receives share $f(i)$.
(b) During an iteration, each player P_i flips a biased coin $c_i \in \{0, 1\}$ where $\mathbf{Pr}[c_i = 1] = \rho$.
(c) Players compute $c^* = \oplus c_i$ by a multiparty computation protocol without revealing their private values c_i-s.
(d) Now c^* is known to everyone. If $c^* = c_i = 1$, P_i broadcasts his share. Therefore:
  (d.1) If 3 shares are revealed, the secret is recovered and the protocol ends.
  (d.2) If $c^* = 1$ and 0 or 2 shares are revealed, players terminate the protocol.
  (d.3) In any other cases, the dealer and players proceed to step (a).

Rows	c_1	c_2	c_3	Public c^*	Shares
1	0	0	0	0	-
2	0	0	1	1	$f(3)$
3	0	1	0	1	$f(2)$
4	0	1	1	0	-
5	1	0	0	1	$f(1)$
6	1	0	1	0	-
7	1	1	0	0	-
8	1	1	1	1	$f(1), f(2), f(3)$

TABLE I
3-PLAYER RATIONAL SECRET SHARING GAME

To see how this solution works, assume P_1 and P_2 follow the protocol whereas player P_3 deviates. He may deviate in "coin-tossing" or in "revealing" his share. Note that each P_i selects c_i independently. The following cases are possible deviation scenarios:

- It is not advantageous for P_3 to bias c_3 to be 0 with higher probability since, when $c_3 = 0$, either no share or one share is revealed.
- It is also not advantageous for P_3 to bias c_3 to be 1 with higher probability since, when $c_3 = 1$, either 0 or 1 share or all shares are revealed. This may lead to an early secret recovery but it does not have any effect on P_3's utility.
- If $c_3 = 0$ or $c^* = 0$ (Table I: rows $1, 3, 4, 5, 6$ and 7), there is no incentive for P_3 to deviate because in these cases he is supposed not to reveal his share.
- If $c_3 = 1$ and $c^* = 1$ (Table I: one of rows 2 or 8 occurs), then player P_3 is supposed to reveal his share. There exist two possibilities:

1) $c_1 = 1$ & $c_2 = 1$ occur with the following probability:

$$\begin{aligned}&\mathbf{Pr}[c_1 = 1 \wedge c_2 = 1 | c_3 = 1 \wedge c^* = 1] \\ &= \frac{\mathbf{Pr}[c_1 = 1 \wedge c_2 = 1 \wedge c_3 = 1]}{\mathbf{Pr}[c_3 = 1 \wedge c^* = 1]} \\ &= \frac{\rho^3}{(1-\rho)(1-\rho)\rho + \rho^3} = \frac{\rho^2}{(1-\rho)^2 + \rho^2}\,.\end{aligned}$$

2) $c_1 = 0$ & $c_2 = 0$ occur with the remaining probability:

$$\begin{aligned}&\mathbf{Pr}[c_1 = 0 \wedge c_2 = 0 | c_3 = 1 \wedge c^* = 1] \\ &= \frac{\mathbf{Pr}[c_1 = 0 \wedge c_2 = 0 \wedge c_3 = 1]}{\mathbf{Pr}[c_3 = 1 \wedge c^* = 1]} \\ &= \frac{(1-\rho)(1-\rho)\rho}{(1-\rho)(1-\rho)\rho + \rho^3} = \frac{(1-\rho)^2}{(1-\rho)^2 + \rho^2}\,.\end{aligned}$$

Therefore, if P_3 deviates by not revealing his share, either he will be the only player who learns the secret or the protocol terminates and he never learns the secret. Let assume P_3 gains U^+ if he is the only player who learns the secret, let U denotes the utility gain for each P_i if all three players learn the secret, and let U^- denotes the utility gain, say \$0, for each P_i if no one learns the secret. It is assumed that $U^+ > U > U^-$. Therefore, a rational P_3 will cheat only if:

$$U^+\left(\frac{\rho^2}{(1-\rho)^2+\rho^2}\right) + U^-\left(\frac{(1-\rho)^2}{(1-\rho)^2+\rho^2}\right) > U.$$

If we assign an appropriate value to ρ such that the above inequality is not satisfied, then P_3 has no incentive to deviate when $c_3 = 1$ and $c^* = 1$.

The authors in [2] showed that 3-player game can be generalized to a game with n players. As we mentioned, certain assumptions regarding the players' utility function are required for rational secret sharing to be achievable. Let $u_i(\vec{a})$ denote the utility of P_i in outcome $\vec{a}$ of the protocol. Suppose each $\ell_i(\vec{a})$ is a bit defining whether P_i has learned the secret or not in outcome $\vec{a}$. We define $\delta(\vec{a}) = \sum_i \ell_i(\vec{a})$, which denotes the number of players who have learned the secret. The assumptions of rational secret sharing are as follows:

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

The first assumption means P_i prefers an outcome in which he learns the secret; he prefers $\vec{a}$ since $\ell_i(\vec{a}) = 1$ and $\ell_i(\vec{a}') = 0$. The second assumption means P_i prefers an outcome where the fewest number of other players learn the secret.

III. SOCIO-RATIONAL SECRET SHARING

In a socio-rational model, the secret sharing game is repeatedly played for an unknown number of rounds. Each player 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 different periods of the game. Moreover, 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 to participate in the current game. Finally, each player computes two utility functions to select his action, i.e., long-term utility function u_i and actual utility function u_i'. See Figure 1 for details.

A. Utility Assumption

Let $u_i(\vec{a})$ denote P_i's utility by considering current and future games, let $u_i'(\vec{a})$ denote P_i's utility in the current game, let $\ell_i(\vec{a}) \in \{0, 1\}$ denote if P_i has learned the secret in the current game, and define $\delta(\vec{a}) = \sum_i \ell_i(\vec{a})$. Let $\mathcal{T}_i^{\vec{a}}(p)$ denote the reputation of P_i after outcome $\vec{a}$ in period p. The following assumptions are considered in socio-rational secret sharing:

- $\ell_i(\vec{a}) = \ell_i(\vec{a}')$ and $\mathcal{T}_i^{\vec{a}}(p) > \mathcal{T}_i^{\vec{a}'}(p) \Rightarrow u_i(\vec{a}) > u_i(\vec{a}')$.
- $\ell_i(\vec{a}) > \ell_i(\vec{a}') \Rightarrow u_i'(\vec{a}) > u_i'(\vec{a}')$.
- $\ell_i(\vec{a}) = \ell_i(\vec{a}')$ and $\delta(\vec{a}) < \delta(\vec{a}') \Rightarrow u_i'(\vec{a}) > u_i'(\vec{a}')$.

The first assumption states that P_i prefers to maintain a high reputation no matter if he learns the secret or not. The other two preferences are standard assumptions of RSS.

B. Generalization of Utility Computation

The long-term utility function $u_i : \mathcal{A} \times \mathcal{T}_i \mapsto \mathbb{R}$ computes the utility that each P_i potentially gains or loses by considering both current and future games (based on all three assumptions) whereas the actual utility function $u_i' : \mathcal{A} \mapsto \mathbb{R}$ only computes the current gain or loss in a given period (based on second and third assumptions).

Secret Sharing

1) Let ϕ be the current probability distribution over players' types, i.e., good, bad and newcomer. 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 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, $f(x)$ 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) The reputation values $\mathcal{T}_i$ of all the chosen players are publicly updated based on each player's behavior using a trust function.

Fig. 1. Socio-Rational Secret Sharing

Let $\omega_i(\vec{a}) = 3/(2 - \mathcal{T}_i^{\vec{a}}(p))$ and $\tau_i(\vec{a}) = \mathcal{T}_i^{\vec{a}}(p) - \mathcal{T}_i^{\vec{a}}(p-1)$ for the n participating players of the current game. Since $-1 \leq \mathcal{T}_i^{\vec{a}}(p) \leq +1$, then $+1 \leq \omega_i(\vec{a}) \leq +3$. Also, let $\Omega > 0$ be a unit of utility, say \$100. To satisfy the stated assumptions in Section III-A, we have:

$$Eq.1 \quad : \quad \frac{|\tau_i(\vec{a})|}{\tau_i(\vec{a})} \times \omega_i(\vec{a}) \times \Omega$$

$$\text{where} \quad \frac{|\tau_i(\vec{a})|}{\tau_i(\vec{a})} = \begin{cases} +1 \text{ if } a_i = \mathcal{C} \\ -1 \text{ if } a_i = \mathcal{D} \end{cases}$$

$$Eq.2 \quad : \quad \ell_i(\vec{a}) \times \Omega \quad \text{where} \quad \ell_i(\vec{a}) \in \{0, 1\}$$

$$Eq.3 \quad : \quad \frac{\ell_i(\vec{a})}{\delta(\vec{a}) + 1} \times \Omega \quad \text{where} \quad \delta(\vec{a}) = \sum_{i=1}^{N} \ell_i(\vec{a}).$$

- *Eq.*1 means P_i gains or loses at least 1Ω and at most 3Ω units of utility in the future games due to his current behavior.
- *Eq.*2 illustrates that a player gains one unit of utility if he learns the secret in the current game and he loses this opportunity, otherwise.
- *Eq.*3 results in "almost" one unit of utility being divided among all the players P_i who have learned the secret in the current game.

The linear combination of these terms with their impact factors gives the long-term utility function $u_i(\vec{a})$, however, actual utility $u_i'(\vec{a})$ only consists of equations *Eq.*2 and *Eq.*3.

It is worth mentioning that one can design any function as long as it satisfies the utility assumptions of a rational foresighted player. For instance, to consider the number of players learning the secret, we can define a monotonically decreasing function $f(\delta(\vec{a})) : \{0, \ldots, n\} \mapsto \mathbb{R}$.

A utility function $F_i(\vec{a})$ with the following linear combination of impact factors $\rho_1 \gg \rho_2 \geq \rho_3 \geq 1$ and functions $f_1(\mathcal{T}_i(\vec{a}))$, $f_2(\ell_i(\vec{a}))$ and $f_3(\delta(\vec{a}))$ satisfies the preference of a rational foresighted player, where

- $|f_1|$ is a monotonically increasing function.
- f_3 is a monotonically decreasing function.
- $|f_1(\mathcal{T}_i(\vec{a}))| \geq f_2(\ell_i(\vec{a})) \geq f_3(\delta(\vec{a}))$ except in a situation when $\ell_i = \delta = 0$.

$$F_i(\vec{a}) = \Omega\Big(\rho_1 f_1(\mathcal{T}_i(\vec{a})) + \rho_2 f_2(\ell_i(\vec{a})) + \ell_i(\vec{a})\rho_3 f_3(\delta(\vec{a}))\Big).$$

$$f_1 : \begin{cases} \mathbb{R}_{>0} & \tau_i(\vec{a}) > 0 \\ \mathbb{R}_{<0} & \text{otherwise} \end{cases} \qquad f_2 : \begin{cases} 0 & \ell_i(\vec{a}) = 0 \\ \mathbb{R}_{>0} & \ell_i(\vec{a}) = 1 \end{cases}$$

$$f_3 : \begin{cases} 1 & \delta(\vec{a}) = 0 \\ \mathbb{R}_{>0} & \delta(\vec{a}) \in \{1 \ldots n\} \end{cases}$$

Theorem-1: *In a $(2, 2)$ socio-rational secret sharing, $\mathcal{C}$ strictly dominates $\mathcal{D}$ when we use our new utility function.*

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

1) If both players cooperate, then τ_i is positive, $\ell_i = 1$ since P_i has learned the secret, and $\delta = 2$ because both players have learned the secret:
$$\big(\tau_i > 0, \ell_i = 1, \delta = 2\big) \Rightarrow$$
$$u_i^{(\mathcal{C},\mathcal{C})} = \Omega\Big(\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3\Big).$$
2) If only P_i cooperates, then τ_i is positive, $\ell_i = 0$ since P_i has not learned the secret, and $\delta = 1$ because only player P_j has learned the secret:
$$\big(\tau_i > 0, \ell_i = 0, \delta = 1\big) \Rightarrow u_i^{(\mathcal{C},\mathcal{D})} = \Omega\Big(\rho_1 f_1\Big).$$
3) If only P_j cooperates, then τ_i is negative, $\ell_i = 1$ since P_i has learned the secret, and $\delta = 1$ because only player P_i has learned the secret:
$$\big(\tau_i < 0, \ell_i = 1, \delta = 1\big) \Rightarrow$$
$$u_i^{(\mathcal{D},\mathcal{C})} = \Omega\Big(-\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3\Big).$$
4) If both players defect, then τ_i is negative, $\ell_i = 0$ since P_i has not learned the secret, and $\delta = 0$ because no one has learned the secret:
$$\big(\tau_i < 0, \ell_i = 0, \delta = 0\big) \Rightarrow u_i^{(\mathcal{D},\mathcal{D})} = \Omega\Big(-\rho_1 f_1\Big).$$

We ignore the common factor Ω. We know $|f_1| \geq f_2 \geq f_3$ and $\rho_1 \gg \rho_2 \geq \rho_3 \geq 1$.

- First, we have:
$$u_i^{(\mathcal{C},\mathcal{C})} = \rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3 > \rho_1 f_1 = u_i^{(\mathcal{C},\mathcal{D})}.$$
- Next, it is easy to see that
$$u_i^{(\mathcal{C},\mathcal{D})} = \rho_1 f_1 > -\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3 = u_i^{(\mathcal{D},\mathcal{C})}$$
if and only if $2\rho_1 f_1 > \rho_2 f_2 + \rho_3 f_3$. We have:
$$\begin{aligned} 2\rho_1 f_1 &\geq \rho_1 f_2 + \rho_1 f_3 \\ &> \rho_2 f_2 + \rho_3 f_3 \end{aligned}$$
so the desired conclusion follows.
- Finally,
$$u_i^{(\mathcal{D},\mathcal{C})} = -\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3 > -\rho_1 f_1 = u_i^{(\mathcal{D},\mathcal{D})}.$$

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

$$\overbrace{u_i^{(\mathcal{C},\mathcal{C})}(\vec{a}) > u_i^{(\mathcal{C},\mathcal{D})}(\vec{a})}^{P_i \text{ cooperates}} > \overbrace{u_i^{(\mathcal{D},\mathcal{C})}(\vec{a}) > u_i^{(\mathcal{D},\mathcal{D})}(\vec{a})}^{P_i \text{ defects}} \quad \square$$

To expand our proof to a case with n players, 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 $\mathcal{M}_{-i}$ denote that, excluding P_i, some players cooperate and some of them defect.

Theorem-2: *In a (t, n) socio-rational secret sharing, $\mathcal{C}$ strictly dominates $\mathcal{D}$ when we use our new utility function.*

Proof: We compute the utility of each outcome based on the threshold, i.e., the required shares to learn the secret. For the sake of simplicity, let $n > t > 2$.

1) If all the players cooperate, τ_i is positive, $\ell_i = 1$ since P_i has learned the secret, and $\delta = n$ because all the players have learned the secret:
$$\big(\tau_i > 0, \ell_i = 1, \delta = n\big) \Rightarrow u_i^{(\mathcal{C}_i,\mathcal{C}_{-i})} = \Omega\Big(\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3\Big).$$
2) If player P_i as well as Δ players cooperate but the rest of the them defect:

(2.1) If $\Delta \geq t-1$, τ_i is positive, $\ell_i = 1$ & $\delta = n$:
$$\big(\tau_i > 0, \ell_i = 1, \delta = n\big) \Rightarrow u_i^{(\mathcal{C}_i,\mathcal{M}_{-i})} = \Omega\Big(\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3\Big).$$
(2.2) If $\Delta < t-1$, τ_i is positive, $\ell_i = 0$ & $\delta = 0$:
$$\big(\tau_i > 0, \ell_i = 1, \delta = n\big) \Rightarrow u_i^{(\mathcal{C}_i,\mathcal{M}_{-i})} = \Omega\Big(\rho_1 f_1\Big).$$
3) If only P_i cooperates, τ_i is positive, $\ell_i = 0$, and $\delta = n-1$ because all the players, except P_i, have learned the secret:
$$\big(\tau_i > 0, \ell_i = 0, \delta = 0\big) \Rightarrow u_i^{(\mathcal{C}_i,\mathcal{D}_{-i})} = \Omega\Big(\rho_1 f_1\Big).$$
4) If only P_i defects, τ_i is negative, $\ell_i = 1$ and $\delta = n$ because all the players have learned the secret:
$$\big(\tau_i < 0, \ell_i = 1, \delta = n\big) \Rightarrow u_i^{(\mathcal{D}_i,\mathcal{C}_{-i})} = \Omega\Big(-\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3\Big).$$
5) If P_i defects, Δ players cooperate and the rest of the players also defect:

(5.1) If $\Delta \geq t$, τ_i is negative, $\ell_i = 1$ & $\delta = n$:
$$\big(\tau_i < 0, \ell_i = 1, \delta = n\big) \Rightarrow u_i^{(\mathcal{C}_i,\mathcal{M}_{-i})} = \Omega\Big(-\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3\Big).$$
(5.2) If $\Delta < t$, τ_i is negative, $\ell_i = 0$ & $\delta = 0$:
$$\big(\tau_i < 0, \ell_i = 0, \delta = 0\big) \Rightarrow u_i^{(\mathcal{C}_i,\mathcal{M}_{-i})} = \Omega\Big(-\rho_1 f_1\Big).$$
6) If all the players defect, τ_i is negative, $\ell_i = 0$, and $\delta = 0$ because no one has learned the secret:
$$\big(\tau_i < 0, \ell_i = 0, \delta = 0\big) \Rightarrow u_i^{(\mathcal{D}_i,\mathcal{D}_{-i})} = \Omega\Big(-\rho_1 f_1\Big).$$

We now analyze these six scenarios, let $*_{-i}$ be $\mathcal{C}_{-i}$ or $\mathcal{M}_{-i}$ or $\mathcal{D}_{-i}$:

- If player P_i cooperates (cases $1-3$), regardless of whether the other players cooperate or defect:
$$u_i^{(\mathcal{C}_i,*_{-i})} \geq \rho_1 f_1.$$
- If P_i defects (cases $4-6$), regardless of whether the other players cooperate or defect:
$$u_i^{(\mathcal{D}_i,*_{-i})} \leq -\rho_1 f_1 + \rho_2 f_2 + \rho_3 f_3.$$

The proof of the above equation is essentially the same as the previous proof. As a result, it is always in P_i's best interest to cooperate:

$$u_i^{(\mathcal{C}_i,*_{-i})}(\vec{a}) > u_i^{(\mathcal{D}_i,*_{-i})}(\vec{a}) \qquad \square$$

REFERENCES

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] J. Y. Halpern and V. Teague, "Rational secret sharing and multiparty computation," in *36th Annual ACM Symposium on Theory of Computing*, 2004, pp. 623–632.

[3] M. Nojoumian, D. Stinson, and M. Grainger, "Unconditionally secure social secret sharing scheme," *IET Information Security, Special Issue on Multi-Agent and Distributed Information Security*, vol. 4, no. 4, pp. 202–211, 2010.

[4] M. Nojoumian and D. R. Stinson, "Socio-rational secret sharing as a new direction in rational cryptography," in *3rd International Conference on Decision and Game Theory for Security*, ser. LNCS, vol. 7638. Springer, 2012, pp. 18–37.

[5] M. Nojoumian and T. Lethbridge, "A New Approach for the Trust Calculation in Social Networks," in *E-business and Telecommunication Networks: best papers of ICE-B'06*, vol. 9. Springer, 2008, pp. 64–77.