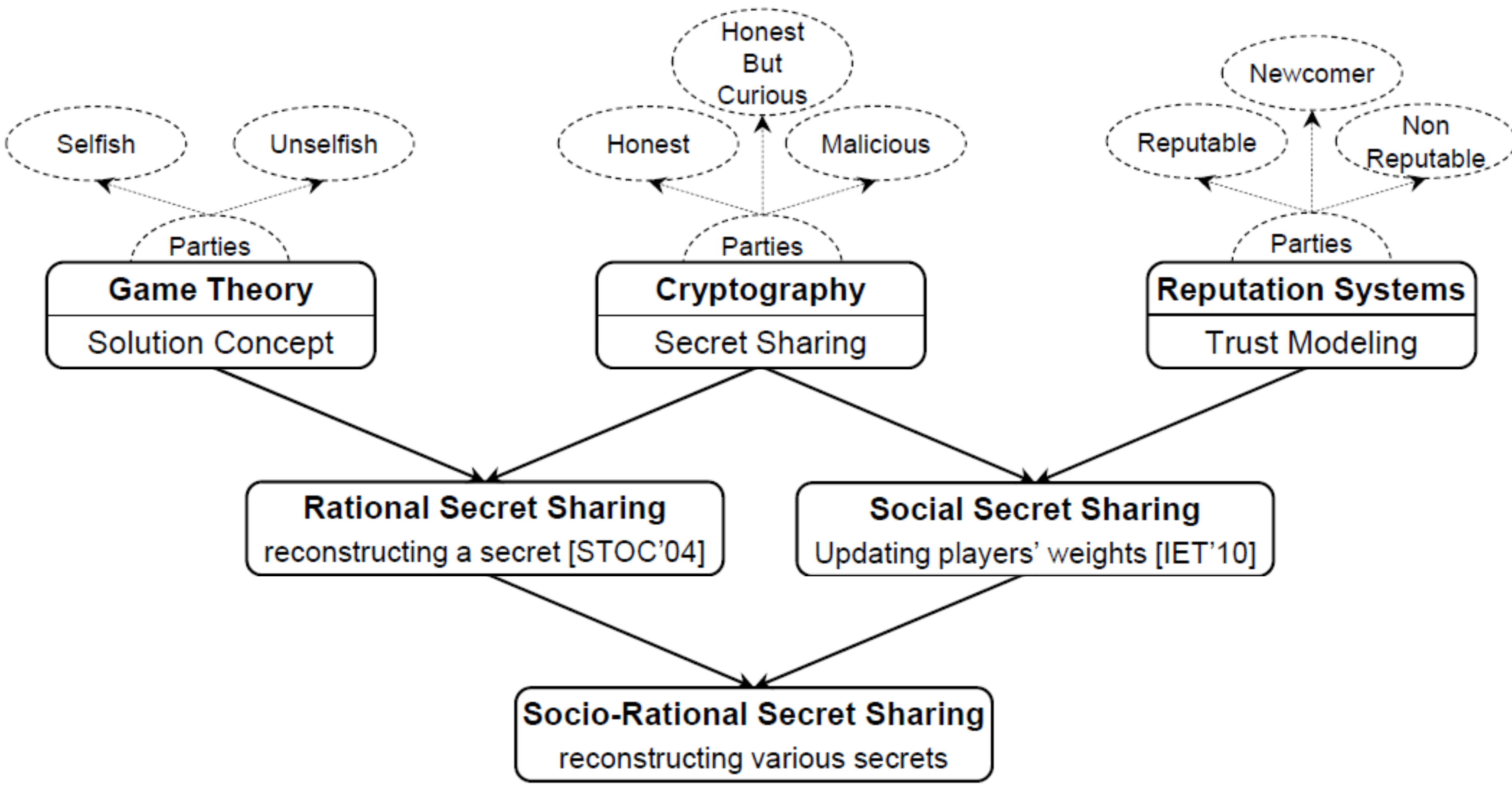
From Rational Secret Sharing to Social and Socio-Rational Secret Sharing

Mehrdad Nojoumian
Department of Computer Science
Florida Atlantic University, USA

Douglas R. Stinson
David R. Cheriton School of Computer Science
University of Waterloo, Canada

GAMES 2016
Maastricht, The Netherlands

Secret Sharing in a Multidisciplinary Model



Trust and Reputation Systems

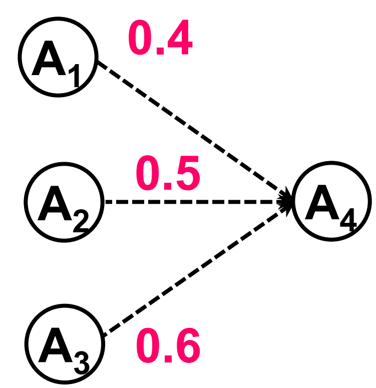
- **Trust versus Reputation:**
  - ✓ **Trust** is a personal quantity, created between "2" players, whereas
  - ✓ **Reputation** is a social quantity in a network of "n" players.

- **Trust Function:** Let T_i^j (p) be the **trust** value assigned by player P_j to P_i in period "p". Let T_i be the trust function representing the **reputation** of P_i.

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

Example:

$$T_4(p) = 1/(4-1) \sum_{j=1}^{n} T_4^j(p) = 1/3\,(0.4 + 0.5 + 0.6) = \mathbf{0.5}$$

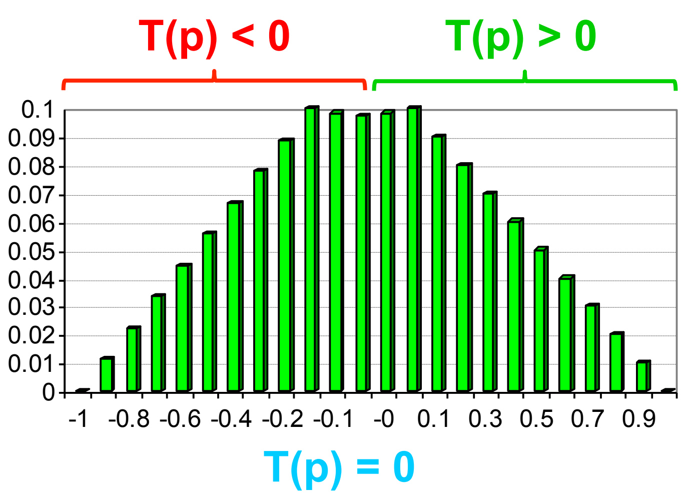


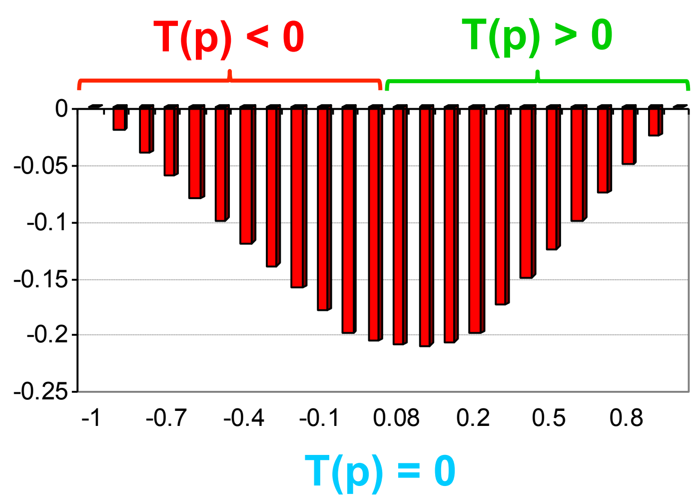
If all players have an equal view, **trust = reputation**.

Review of a Well-Known Solution

- **Previous Solution:** trust value T(p+1) is given by the following equations and it depends on the previous trust rating where: $\alpha \geq 0$ and $\beta \leq 0$ [CIA'00].

T(p)	Cooperation	Defection
> 0	$T(p) + \alpha\,(1-T(p))$	$(T(p) + \beta)\,/\,(1- \min\{\,\lvert T(p)\rvert\,,\,\lvert\beta\rvert\,\})$
< 0	$(T(p) + \alpha\,)\,/\,(1 - \min\{\,\lvert T(p)\rvert\,,\,\lvert\alpha\rvert\,\})$	$T(p) + \beta\,(1+T(p))$
= 0	α	β

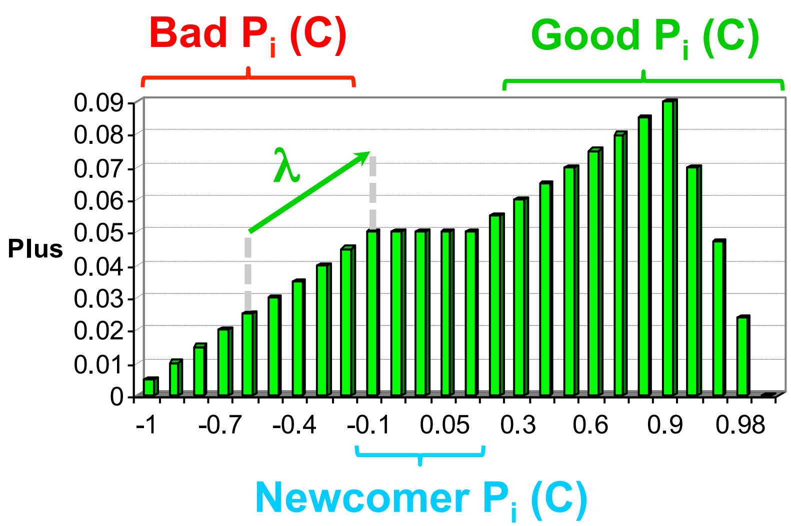


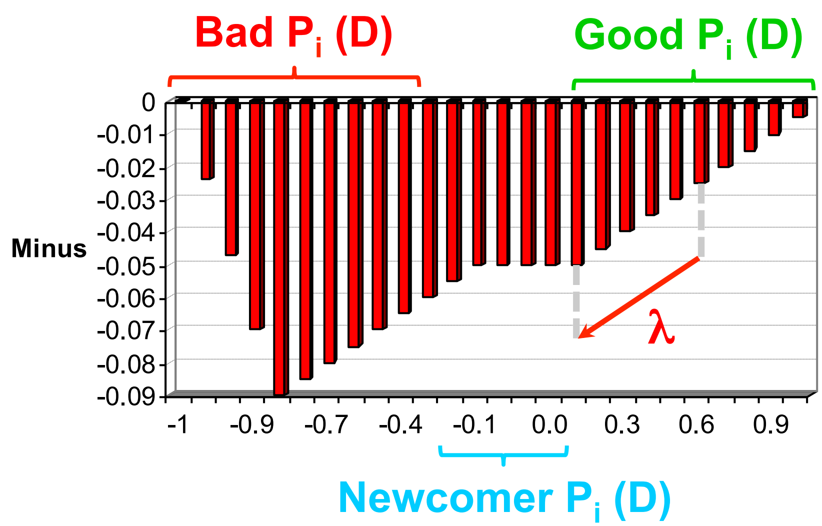


Our Trust Model

- **Our Function** is not just a function of a single round, but of the history:
  - ✓ **Reward** more (or same) the better a participant is,
  - ✓ **Penalize** more (or same) the worse a participant is.

Trust Value	Cooperation	Defection
$T_{Bad\ P_i} \in [-1,\beta)$	Encourage	**Penalize**
$T_{New\ P_i}$: $[\beta,\alpha]$	Give/Take Opportunities	
$T_{Good\ P_i} \in (\alpha,+1]$	**Reward**	Discourage





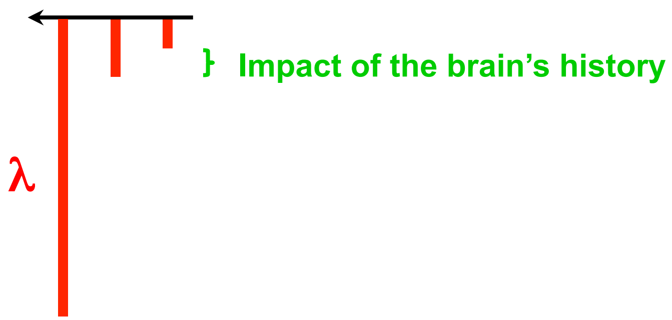
Intuition and Motivation

There exist some common principles for trust modeling

A lies to *B* for the 1st time: *defection*

A lies to *B* for the 2nd time: *same defection + past history*

A cheat on *B*: *costly defection*



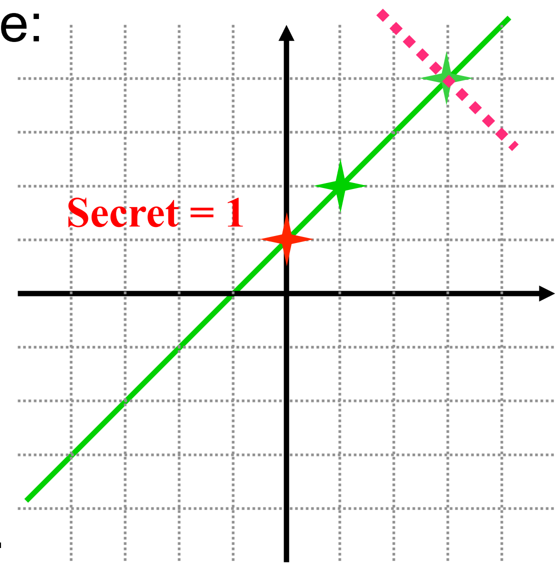
Shamir Secret Sharing

1. **Sharing:** a secret is divided into **n** shares in order to be distributed among **n** players.

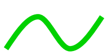
2. **Reconstruction:** an authorize subset of players then cooperate to reveal the secret, e.g., **t** players where **t < n** is the threshold.

Example: t = 2 points are sufficient to define a line:

(1, 2), (2, 3), (3, 4), (4, 5) → y = x+**1**



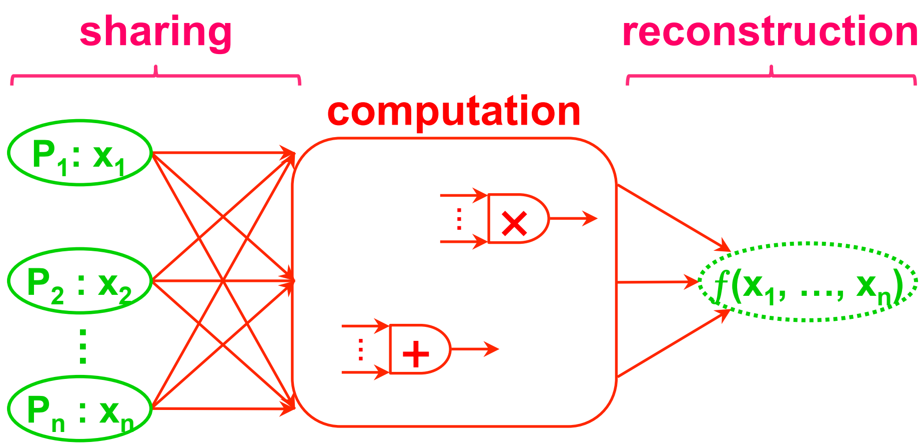
 t = 3 points are sufficient to define a parabola.

 t = 4 points are sufficient to define a cubic curve.

In general, it takes **t points** to define a polynomial of **degree t-1**.

Application of Secret Sharing

- **Secure Multiparty Computation:** compute f with private inputs.



Sealed-Bid 1st-Price Auctions: the bidder who proposes the highest bid β wins & pays $β.

- **Sealed-Bid Auctions:** preserve the privacy of different parameters.

  ✓ Secrecy of the selling price and winner's identity are optional.

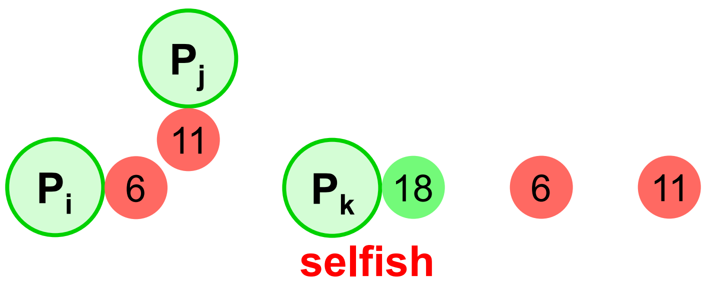
  ✓ To have a fair auction, confidentiality of the losing bids is important:

  They can be used in future auctions and negotiations by different parties, e.g., auctioneers to maximize their revenues or competitors to win the auction.

Rational Secret Sharing

- **Problem:** the players deny to reveal their shares in the secret recovery phase, therefore, the secret is not reconstructed at all.

Example: f (x) = 3 + 2 x + x^2 → t=3 shares are enough for recovery.

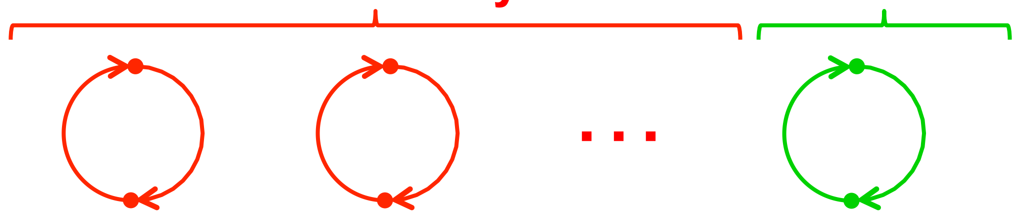


only P_k learns the secret “3”

- ✓ Model: players are selfish rather than being honest or malicious. If all players act selfishly, secret recovery fails.

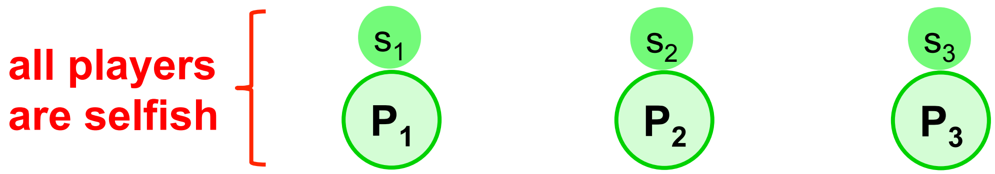
- **Solution:**

fake secret recovery rounds **unknown real recovery round**



STOC'04 Paper

➢ **Problem:** 3-out-of-3 rational secret sharing.



➢ **Solution:** a multi-round recovery approach.

	c_1	c_2	c_3	$\oplus c_i$	
	0	0	0	0	← 0
0 →	0	0	1	1	← 1
0 →	0	1	0	1	← 1
	0	1	1	0	← 0
0 →	1	0	0	1	← 1
	1	0	1	0	← 0
	1	1	0	0	← 0
3 → 0 , 2 →	1	1	1	1	← 1

1. In each round, **dealer** initiates a fresh secret sharing of the same secret.
2. During an iteration, each $\mathbf{P_i}$ flips a biased coin $\mathbf{c_i}$ with $\mathbf{Pr[c_i = 1] = \alpha}$.
3. Players then compute $\mathbf{c^* = \oplus\, c_i}$ by MPC without revealing $\mathbf{c_i}$-s.
4. If $\mathbf{c^* = c_i = 1}$, player $\mathbf{P_i}$ broadcast his share. There are 3 possibilities:
   a. If all shares are revealed, the secret is recovered and the **protocol ends**.
   b. If **c* = 1** and **0 or 2** shares are revealed, players **terminate the protocol**.
   c. In any other cases, the dealer and players proceed to the **next round**.

Socio-Rational Secret Sharing

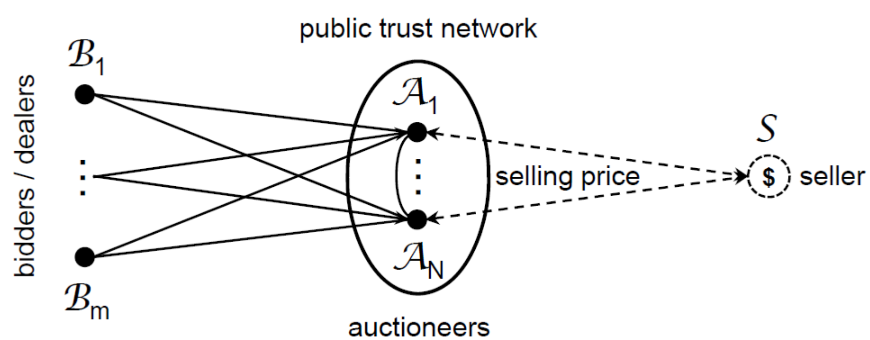
- **Motivation:** we would like to consider a repeated secret sharing game where players enter into a long-term interaction for executing an unknown number of independent secret sharing schemes.

- **Contribution:** a public trust network is constructed to incentivize players to be cooperative, i.e., they can then gain extra utilities. In other words, players avoid selfish behaviors due to the social reinforcement of the trust network.

Application in Repeated Games

- **Sealed-Bid Auctions:** consider a repeated secret sharing game.

  1. Bidders select **"n"** out of **"N"** auctioneers based on their reputation.
  2. Each bidder then acts as an independent dealer and shares his bid.
  3. Auctioneers simulate a secure MPC protocol to define the outcome.
  4. In the last round of the MPC, they need to recover the selling price.



✓ Only auctioneers who learn (report) the selling price are rewarded.

✓ At the end of each game, the reputation of each auctioneer is updated.

Our Construction in Nutshell

- **Utility Estimation Function:** is used by a rational foresighted player.

decision making

  - ✓ Estimation of the future gain/loss due to the trust adjustment (virtual).
  - ✓ Learning the secret at the current time (real).
  - ✓ The number of other players learning the secret at the moment (real).

$

- **Prominent Properties:** our solution

  - ✓ Has a single reconstruction round.
  - ✓ Provides a stable solution concept.
  - ✓ Is immune to rushing attack.
  - ✓ Prevents the players to abort.

despite all the existing protocols

Utility Assumption

➤ **Rational vs Socio-Rational Secret Sharing:** $l_i(\boldsymbol{a}) \in \{0,1\}$ whether P_i has learned the secret or not, and let $\delta(\boldsymbol{a}) = \sum_i l_i(\boldsymbol{a})$

Socio-Rational:

$$l_i(\boldsymbol{a}) = l_i(\boldsymbol{a}') \text{ and } \mathcal{T}_i^{\boldsymbol{a}}(p) > \mathcal{T}_i^{\boldsymbol{a}'}(p) \Rightarrow u_i(\boldsymbol{a}) > u_i(\boldsymbol{a}').$$

Rational:

$$l_i(\boldsymbol{a}) > l_i(\boldsymbol{a}') \Rightarrow u_i'(\boldsymbol{a}) > u_i'(\boldsymbol{a}').$$

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

1. The first preference illustrates that whether P_i learns the secret or not, he prefers to stay reputable.

2. The second assumption means P_i prefers the outcome in which he learns the secret.

3. The third one means P_i prefers the outcome in which the fewest number of other players learn the secret.

Utility Computation

- **Sample Function:** which satisfies our utility assumptions.

$$\underbrace{\omega_i(\boldsymbol{a}) = 3/(2 - \mathcal{T}_i^{\boldsymbol{a}}(p)) \qquad \mathcal{T}_i^{\boldsymbol{a}}(p) \in [-1, +1]}_{\omega_i \in [1\,,\,3]} \qquad \tau_i(\boldsymbol{a}) = \mathcal{T}_i^{\boldsymbol{a}}(p) - \mathcal{T}_i^{\boldsymbol{a}}(p-1)$$

assume P_i has contributed in two consecutive periods ***p*** and ***p-1***

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

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

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

Ω = $100

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

Protocol: Socio-Rational SS

1. Sharing Phase:

Non-reputable	Newcomer	Reputable
$P_i \in \mathcal{B} \Rightarrow \mathcal{T}_i(p) \in [-1, \beta)$	$P_i \in \mathcal{N} \Rightarrow \mathcal{T}_i(p) \in [\beta, \alpha]$	$P_i \in \mathcal{G} \Rightarrow \mathcal{T}_i(p) \in (\alpha, +1]$

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:

%10 %30 %60

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

2. The dealer then initiates a secret sharing scheme by selecting a polynomial $f(x) \in \mathbb{Z}_q[x]$ of degree t 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.

Protocol: Socio-Rational SS

2. Reconstruction Phase:

Action Profile: $\mathcal{A} \stackrel{\text{def}}{=} \mathcal{A}_1 \times \cdots \times \mathcal{A}_N$

Reputation Profile: $\mathcal{T} \stackrel{\text{def}}{=} \mathcal{T}_1 \times \cdots \times \mathcal{T}_N$

Three Actions: $\mathcal{A}_i = \{\mathcal{C}, \mathcal{D}, \perp\}$

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 $f(i)$.

consider the current and a few games further

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 $u'_i : \mathcal{A} \mapsto \mathbb{R}$ at the end of the reconstruction phase according to the outcome. **only consider the current game**

4. Finally, the reputation values $\mathcal{T}_i$ of all players are publicly updated according to each player's behavior and the trust function $\mathcal{T} : \mathcal{A}_i \mapsto \mathbb{R}$.

Comparison

- **(2,2)-Socio-Rational Secret Sharing:** despite rational secret sharing, Cooperation is always the best strategy even if the other party defects.

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

- **Utility Comparison:** where $\mathcal{U}^+ > \mathcal{U} > \mathcal{U}^- > \mathcal{U}^{--}$

P_1 \ P_2	Cooperation	Defection
Cooperation	$\mathcal{U},\mathcal{U}$	$\mathcal{U}^{--},\mathcal{U}^+$
Defection	$\mathcal{U}^+,\mathcal{U}^{--}$	$\mathcal{U}^-,\mathcal{U}^-$

(2,2)- Secret Sharing with Selfish Players

P_1 \ P_2	Cooperation	Defection
Cooperation	$\mathcal{U}^+,\mathcal{U}^+$	$\mathcal{U},\mathcal{U}^-$
Defection	$\mathcal{U}^-,\mathcal{U}$	$\mathcal{U}^{--},\mathcal{U}^{--}$

(2,2)- Socio-Rational Secret Sharing

Intuition and Motivation

Reputation is a key point for having a successful social collaboration

Rational players should have a long-term vision as reputable persons or companies gain more profit all the time

Thank You Very Much

More Resources:

- ✓ Nojoumian M. and Stinson D. R., Socio-Rational Secret Sharing as a New Direction in Rational Cryptography, *3rd Conference on Decision and Game Theory for Security (GameSec)*, Springer LNCS 7638, pp. 18-37, Budapest, Hungary, 2012.
- ✓ Nojoumian M., Novel Secret Sharing and Commitment Schemes for Cryptographic Applications, *PhD Thesis, David R. Cheriton School of Computer Science, U of Waterloo, Canada*, 2012.
- ✓ Nojoumian M. and Stinson D. R., Social Secret Sharing in Cloud Computing Using a New Trust Function, *10th IEEE Annual Conference on Privacy, Security and Trust (PST)*, pp. 161-167, Paris, France, 2012.
- ✓ Nojoumian M., Stinson D. R., and Grainger M., Unconditionally Secure Social Secret Sharing Scheme, *IET Information Security (IFS)*, vol. 4, issue 4, pp. 202-211, 2010.
- ✓ Nojoumian M. and Stinson D. R., Brief Announcement: Secret Sharing Based on the Social Behaviors of Players, *29th ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 239-240, Zurich, Switzerland, 2010.
- ✓ Nojoumian M. and Lethbridge T. C., A New Approach for the Trust Calculation in Social Networks, *3rd International Conference on E-Business (ICE-B)*, pp. 257-264, Setubal, Portugal, 2006.