lec 19

Socio-Rational Secret sharing (SRS)

Similar to Rational SS, players are selfish. In addition, players have concern about their future gain/loss & the secret sharing game is played repeatedly for an unknown # of rounds.

(a) A long-term utility considering future games.

(b) An actual utility in the current game.

1. Estimation of future gain/loss due to trust/repatation adjustmeat (virtual utility).
2. learning the secret in the curreat round.
3. the # of other players learning the secret in the curreat round.

rational secret sharing

Clarity → * As a consumer, if you buy something today (cooperation: los $u), you receive a significat discount from the producer (reward $U) on your next purchase.

* As a producer, if you use low-grade materials to save money (defect: gain $v), you lose many of your consumers (penalize $V) in coming years.

---

utility assumption of SRS

$* l_i^{\vec{a}} \in \{0, 1\}$ (0: not learning the secret; 1: learning the secret)

$* \delta^{\vec{a}} = \sum_{i \in \text{players}} l_i^{\vec{a}}$

√√ A. $l_i^{\vec{a}} = l_i^{\vec{a'}}$ and $T_i^{\vec{a}} > T_i^{\vec{a'}}$

√ B. $l_i^{\vec{a}} > l_i^{\vec{a'}} \Longrightarrow u_i^{\vec{a}} > u_i^{\vec{a'}}$

√ C. $l_i^{\vec{a}} = l_i^{\vec{a'}}$ and $\delta^{\vec{a}} < \delta^{\vec{a'}} \Longrightarrow u_i^{\vec{a}} > u_i^{\vec{a'}}$

$\Longrightarrow u_i^{\vec{a}} > u_i^{\vec{a'}}$

Utility Computation / sample function.

First parameter: $\omega_i^{\vec{a}} = \frac{3}{2 - \tau_i^{\vec{a}}}$ ← current time

Second parameter: $\tau_i^{\vec{a}} = T_{i\,(p)}^{\vec{a}} - T_{i\,(p-1)}^{\vec{a}}$ ← previous time

$$-1 \leq \tau_i^{\vec{a}} \leq +1 \longrightarrow +1 \leq \omega_i^{\vec{a}} \leq +3$$

Third parameter: Ω unit of utility ($100)

$$\begin{cases} A: -\frac{|\tau_i^{\vec{a}}|}{\tau_i^{\vec{a}}} * \omega_i^{\vec{a}} * \Omega, & \text{where } \frac{|\tau_i^{\vec{a}}|}{\tau_i^{\vec{a}}} = \begin{cases} +1 & \text{if } a_i = C \\ -1 & \text{if } a_i = D \end{cases} \\ B: l_i^{\vec{a}} * \Omega, & \text{where } l_i^{\vec{a}} \in \{0, 1\} \\ C: \frac{l_i^{\vec{a}}}{g^{\vec{a}} + 1} * \Omega, & \text{where } g^{\vec{a}} = \sum l_i^{\vec{a}} \end{cases}$$

actual utility

a: actions

$$\rightarrow u'^{\vec{a}} = f_2\left(l_i^{\vec{a}} * \Omega\right) + f_3\left(\frac{l_i^{\vec{a}}}{g^{\vec{a}} + 1} * \Omega\right)$$

long-term utility function $\rightarrow u^{\vec{a}} = f_1\left(\frac{|\tau_i^{\vec{a}}|}{\tau_i^{\vec{a}}} * \omega_i^{\vec{a}} * \Omega\right) + u'^{\vec{a}}$

assumption: $f_1 \gg f_2 \geq f_3 \geq 1$ → weights of equations in the utility functions

Socio-Rational secret sharing game: $\Gamma = (\mathcal{A}_i, T_i, u_i, u'_i)$

- $\mathcal{A}_i$: set of actions
- T_i: set & rep?
- u_i: long-term (current game & future games)
- u'_i: actual (current game)

(a) set of actions: $\mathcal{A}_i = \{C, D, \perp\}$

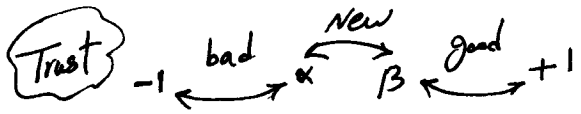
- C: cooperation or revealing share
- D: defection or not revealing share
- $\perp$: not participation

(b) $T_i(\varphi) = T_i(\varphi - 1)$ if $a_i = \perp$

(c) long-term utility function $u_i : \mathcal{A} \times T_i \longmapsto \mathbb{R}$ ($\mathcal{A}$: action profile)

(d) actual utility function $u'_i : \mathcal{A} \longmapsto \mathbb{R}$

SRS protocol



Secret sharing

1. Let ϕ be the current probability distribution over players' types (Bad, newcomers, good). The dealer selects n out of N players where $n \leq N$ based on this non-uniform probability distribution.

$N = 30$ $\alpha_1 \rightarrow n = 5$

$\alpha_2 \rightarrow n = 7$

⋮

2. The dealer initiates a (t,n)-ss scchem by selecting $f(a)$ of degree $t-1$, where $f(0) = \alpha_1$. Subsequently, he sends shares $f(i)$ to P_i for "n" selected players and then leaves the scheme.

Secret Recovery

1. Each selected player P_i computes his long-term utility function u_i and select an action, i.e., reveal or not-reveal his share $f(i)$.
2. If enough shares are revealed, the poly $f(a)$ is reconstructed through Lagrange Interpolation formula & secret is recovered.
3. Each selected player receives his utility $\tilde{u}_i$ (real payoff) at the end of the recovery phase according to outcome.
4. Finally, repatation values T_i of all players are publicly updated according to each player's behaviour & the trust function.

Two-player Socio-Rational secret sharing game

$$u_i^{(C,C)\vec{a}} > u_i^{(C,D)\vec{a}} > u_i^{(D,C)\vec{a}} > u_i^{(D,D)\vec{a}}$$

p_i cooperates — p_i defects

p_1 \ p_2	C	D
C	U, U	U^-, U^+
D	U^+, U^-	~~U, U~~

→ NE

(2,2)-SS with selfish players

$$U^+ > U > U^- > U^{--}$$

p_1 \ p_2	C	D
C	~~U^+, U^+~~	U, U^-
D	U^-, U	U^{--}, U^{--}

NE