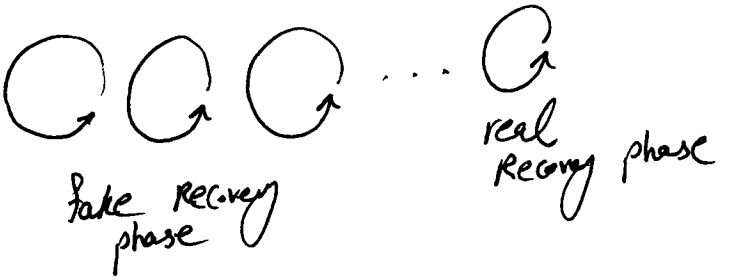
lec 17

Rational Secret sharing

(#) The protocol proceeds in a sequence of iterations where only one iteration is the real secret recovery phase (i.e., last iteration) and the rest are just fake iterations for trapping selfish players.



(#) At the end of each iteration, the protocol either terminates (due to the observation of selfish behavior or cooperation for secret recovery) or it proceeds to the next iteration.

(#) In any given iteration, players do not know whether the current round is the real recovery phase (where a player may gain more utility by being silent and not sending his share to others) or just a test/fake recovery round.

(#) For the sake of simplicity, we assume we only have three players & threshold is also 3

(#) It works for (t,n)-SS scheme as well.

RSS

1. In each round, the dealer initiates a fresh secret sharing scheme where each player P_i receives $f(i)$. This fresh SS encodes just one unique secret α.

2. During an iteration, each p_i flips a biased coin $c_i \in \{0,1\}$ where $pr[c_i=1]=f$.

3. players compute $c^* = \oplus c_i$ by a secure MPC without revealing c_i-s

4. Now c^* is known to everyone. If $c^*=c_i=1$, P_i broadcast his share. we then have:

   (4.1) If three shares are revealed, the secret is recovered & the protocal ends.

   (4.2) if $c^*=1$ and no share or two shares are revealed, players terminate the protocol.

   (4.3) In any other case, the dealer & players proceed to the next round (1).

Drawbacks:
- the protocol may terminate without recovering α.
- the dealer must be in the scheme at the secret recovery phase.

(#) P_1, P_2 are cooperative

P_3 wants to deviate ⟶ he may deviate in "coin-tossing" or in "revealing" his share.

rows	c_1	c_2	c_3	c^*	revealed shares
1	∅	∅	∅	∅	—
(2)	∅	∅	1	1	$f(3)$
3	∅	1	∅	1	$f(2)$
4	∅	1	1	∅	—
5	1	∅	∅	1	$f(1)$
6	1	∅	1	∅	—
7	1	1	∅	∅	—
(8)	1	1	1	1	$f(1), f(2), f(3)$

private — public

Secure MPC

(a) It's not advantageous for P_3 to bais c_3 to be ∅ with higher probability, since, when $c_3 = ∅$, either no share or one share is revealed.

(b) It's also not advantageous for P_3 to bais c_3 to be 1 with a higher probability, since, when $c_3 = 1$, either no share, or one share or all shares are revealed. This may lead to an early secret recovery but it does not have any effect on the utility of P_3.

(c) if $c_3 = \emptyset$ or $c^* = \emptyset$ (rows 1, 3, 4, 5, 6, 7), then there is no incentive for p_3 to deviate since, in all these cases, he is supposed not to reveal his share.

(d) if $c_3 = 1$ and $c^* = 1$ (row 2 & 8 in the table), then player p_3 is supposed to reveal his share. We have two posibilities:

1 $c_1 = 1$ & $c_2 = 1$, which occurs with the following probability:

$$\Pr[c_1 = 1 \wedge c_2 = 1 \mid c_3 = 1 \wedge c^* = 1] = \frac{\Pr[c_1 = 1 \wedge c_2 = 1 \wedge c_3 = 1]}{\Pr[c_3 = 1 \wedge c^* = 1]}$$

$$= \frac{f * f * f}{\underbrace{(1-f)(1-f)f}_{\text{row 2}} + \underbrace{f^3}_{\text{row 8}}}$$

$$= \boxed{\frac{f^2}{(1-f)^2 + f^2}}$$

2 $c_1 = \emptyset$ & $c_2 = \emptyset$, which occurs with the following probability:

$$\Pr[c_1 = \emptyset \wedge c_2 = \emptyset \mid c_3 = 1 \wedge c^* = 1] = \frac{\Pr[c_1 = \emptyset \wedge c_2 = \emptyset \wedge c_3 = 1]}{\Pr[c_3 = 1 \wedge c^* = 1]}$$

$$= \frac{(1-f)(1-f)f}{\underbrace{(1-f)(1-f)f}_{\text{row 2}} + \underbrace{f^3}_{\text{row 8}}}$$

$$= \boxed{\frac{(1-f)^2}{(1-f)^2 + f^2}}$$

Therefore, if P_3 deviates by not revealing his share, either he is going to be the only player who learnes the secret or the protocol ends & he never learnes the secret.

$u^+ \longrightarrow P_3$ is the only player who learnes the secret

$u^- \longrightarrow$ utility for each P_i if no one learnes the secret

$u \longrightarrow$ utility for each P_i if all three players learn the secret

$$u^+ > u > u^-$$

Therefor, a rational P_3 will cheat only if:

$$u^+ \underbrace{\left(\frac{f^2}{(1-f)^2+f^2}\right)}_{P_1 \& P_2 \text{ reveal}} + u^- \underbrace{\left(\frac{(1-f)^2}{(1-f)^2+f^2}\right)}_{P_1 \& P_2 \text{ not reveal}} > u$$

If we assign an appropriate value to f, based on players utility function, such that the above inequality is ~~not~~ satisfied, then P_3 has no incentive to deviate/cheat, when $c_3 = 1$ & $c^* = 1$.