Bonn-Aachen International Center for Information Technology
Cryptography and Game Theory — Raekow, Ziegler
IPEC Winter 2012

Scribe(s): David Möller — Lecture 13, Date: 22.03.2012

1 Lecture 7

1.1 Secret Sharing and GT

We have a safe:

- loot from bank robbery
- only a subset of the initial robbers can open the safe
- each robber receives $\frac{loot}{numberofpresentrobbers}$ as their share
- special lock: everybody enters their shares at the same time.
- if $t+1$ shares are entered the safe opens.

Each robber wants:

1. correctness: learn the correct secret
2. exclusivity: as few as possible of the other players learn correct result.

Note: these preferences are natural in MPC and Secret Sharing.
Move MPC and Secret Sharing from good | bad players to rational players.

1.2 Broadcast Problem

A dealer D holds a message m. D and a number of participating player can be corrupted. Can honest player receive a common msg m'. If D is honest $m' = m$.

Protocol for $n = 4$, 1 corrupt [Pears, Shostak, Lamport 1986]

- Each player sends a msg m_i to all tho other players.
- Each player tells all the other players what they received. If a player i has evreceived no input from player j, he picks a random value.
- Each player i takes the majority of the values he received for j to be the correct one.

In general: BC is impossible if $n < 3t + 1$, where t is the number of players.

	D	C
D	(4, 4)	(0, 5)
C	(5, 0)	(2, 2)

1.3 Iterated prisoners dilemma

Payoffs of single rounds are combined as the overall outcome. Number of rounds should be unknown. (Because elsewise always playing C would be best!)

"'Tit for Tat"' is the best strategy, which means playing the last action your opponent played.

1.4 Secret Sharing

Need $t + 1$ players to reconstruct secret.

Theorem [Halpern, Teague 2005] Rational players that value correctness first, exclusivity second will never broadcast their share. P_1: if $\geq t$ other players broadcast $\rightarrow P_1$ can reconstruct the secret if $< t$ other players broadcast $\rightarrow P_1$ cannot reconstruct the secret

P_1 has no incentive in both cases to broadcast his share. If exactly t other players sent shares P_1 can reconstruct secret and P_i's that sent their shares cannot reconstruct secret.

So not sending share weakly dominates sending the share.

Similar problem as in iterated Prisoners' dilemma, where the number of rounds is known.

Theorem [Halpern, Teague 2005] Given a secret sharing scheme with known upper bound on the running time for reconstruction always results in each player doing nothing.

Example (MPC) for rational players:

P_1	P_2	P_3	xor	$\bar{P_1}$xorP_2xorP_3
0	0	0	0	1
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	0

Player 2 and 3 don't know the secret, but Player 1 does!

Def.: Non-cooperatively computable functions. Functions for which it is a Nash Equilibrium to submit the true input and to believe the outcome of the function are called non-cooperatively computable.

Goal: Construct a secret sharing scheme, where it is not predictable, when the game ends.

Construction: Assume that we have a mechanism, where each player must reveal the result after a round of his coin toss to the other players.

1. Everyone tosses a coin: if heads then send share else don't send.
2. Reveal the coin
3. If everone learned the secret or if s.o. is cought cheating abort else redistribute shares with now polynomial and return to 1.

Analysis: Let $n = 3$, 3 out of 3 secret sharing Say P_1 withholds his share, although he had heads

- lucky if P_2 and P_3 sent their shares
- if P_2 and P_3 do not sent their shares then the protocol is aborted. P_1 does not learn the secret.

$Pr[$ getting cought and not learning $s] = \frac{3}{4}$ $Pr[$ learning s when no one else does $] = \frac{1}{4}$
So as long as $\frac{1}{4} \cdot u_1$ (only P_1 learning secret) + $\frac{3}{4} \cdot u_1$ (no one leans secret) $< u_1$ (everyone learning)
So P_1 has no incentive to cheat.