Utility Dependence in Correct and Fair Rational Secret Sharing

Gilad Asharov

Yehuda Lindell

Bar-Ilan University, Israel

What is Secret Sharing?

- t-out-of-n secret sharing:
  - ***n*** parties wish to share a secret ***s***, such that every subset of ***t*** parties can reconstruct the secret together, but every subset of less than ***t*** parties cannot learn anything about the secret

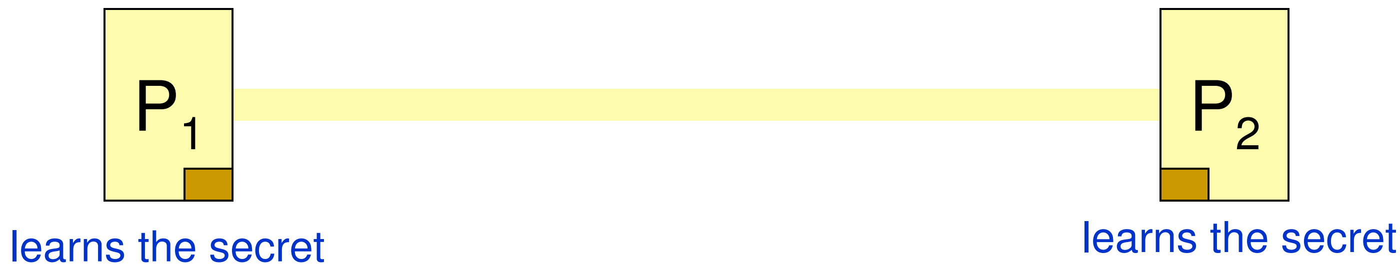
- Two Phases:
  - **Sharing**: A “dealer” creates and sends shares for the ***n*** parties
  - **Reconstruction**: at least ***t*** parties reconstruct the secret (using a reconstruction protocol)

Rational Secret Sharing

- The Goal: to construct a **fair** reconstruction protocol when the parties are **rational**
  - *Fair*: all parties learn the secret
  - *Rational*: all parties have utility functions that they wish to maximize

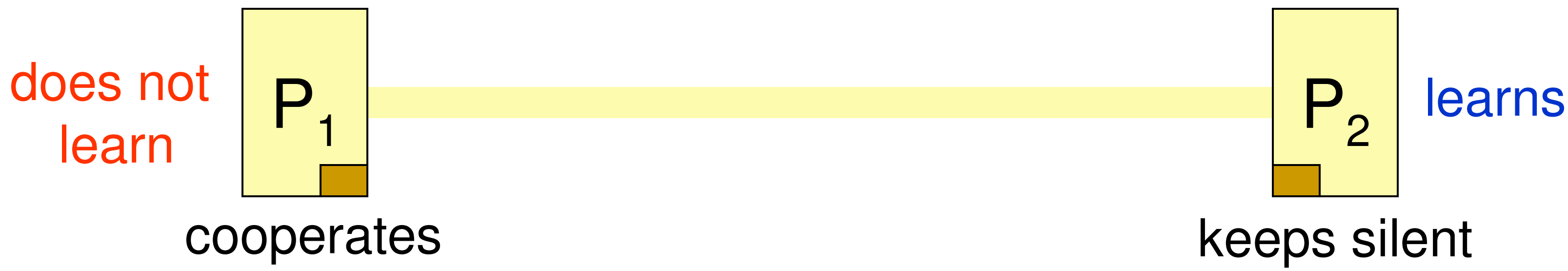
Naive Protocol for Share Reconstruction

- All parties broadcast their shares



The Problem

- A party can not broadcast its share but still learn the secret



- In **rational** secret sharing we assume that:
  - Each party wants to learn the secret
  - Each party prefers to be the only one to learn the secret
- In the naïve reconstruction protocol – no one has incentive to cooperate! [Halpern Teague, STOC 04]

Background – Utilities

- U_i^+ : the utility for party P_i when it alone learns the secret
- U_i : the utility for party P_i when all parties learn the secret
- U_i^- : the utility for party P_i when it does not learn the secret

- Assumptions: for every party it holds that:

$$U_i^+ \geq U_i \geq U_i^-$$

Background – Nash Equilibrium

- **Best Response:**
  is the strategy which produces the most favorable outcome for a player, taking other players' strategies as given

- **Nash Equilibrium:**
  a behavior strategy profile $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ is a *Nash Equilibrium* if for every party i, σ_i is the best response for $\boldsymbol{\sigma}_{-i} = (\boldsymbol{\sigma} \setminus \{\sigma_i\})$
  - $\forall i\ \forall \sigma'_i$: $u_i(\sigma_i, \boldsymbol{\sigma}_{-i}) \geq u_i(\sigma'_i, \boldsymbol{\sigma}_{-i})$
  - There are other solution concepts and stronger equilibriums

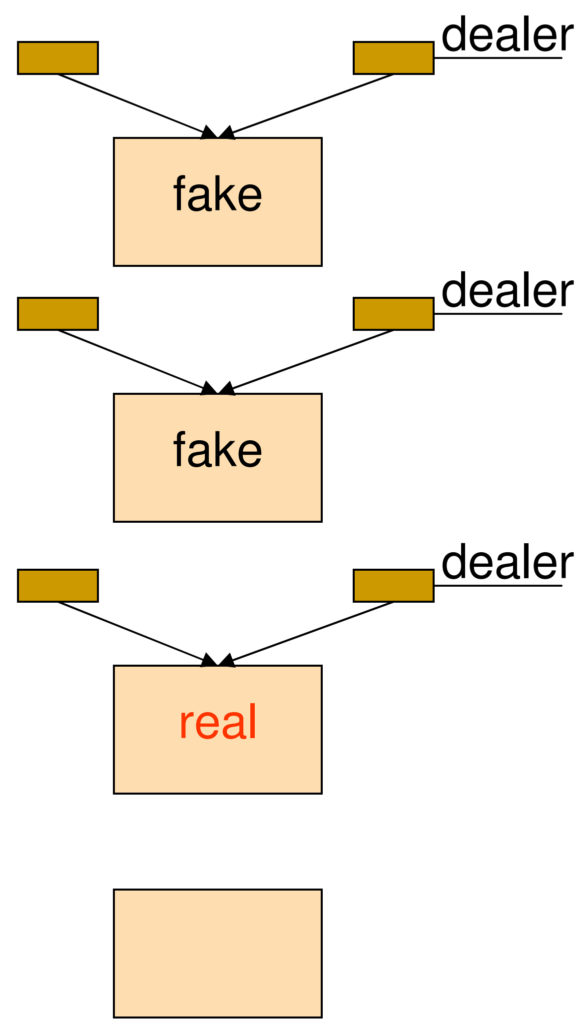
Rational Secret Sharing

- *Rational secret sharing:*
  - There is (at least) a Nash equilibrium on the strategy that instructs all to cooperate and results in all parties learning the secret

  - Thus, the parties' utilities are maximized when they cooperate and all learn the secret
    - When following prescribed strategy, all gain $\mathbf{U_i}$
    - Deviating from the strategy yields an expected utility less than $\mathbf{U_i}$

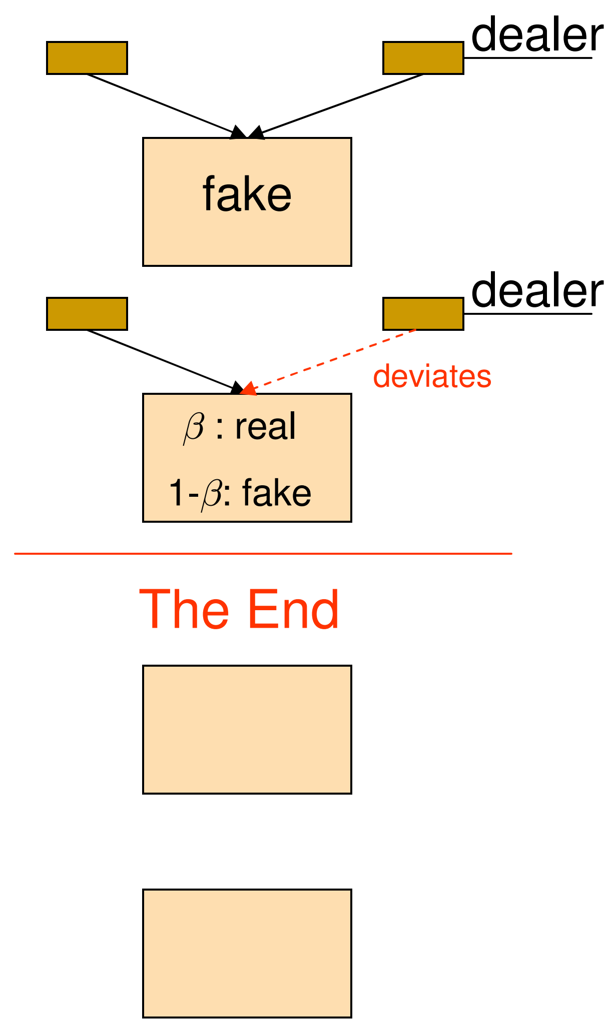
Background – the Gordon-Katz Protocol (simultaneous)

- The dealer at every round chooses shares for the real secret (s) with probability β, and for a fake secret with probability 1-β
- Parties can distinguish between real secret and fake one
- At every round, the parties are supposed to broadcast their shares simultaneously (**C**=cooperate)
- If the reconstructed value is not the real secret, parties continue to the next round



Background – the Gordon-Katz Protocol (simultaneous)

- If a party "deviates" (**D**=deviate=keeps silent), then the game is terminated
- In this case, it can learn the secret alone, but only with probability β
- "deviate" is a risk
  - "Big" β - small risk
  - "Small" β - big risk



The Gordon-Katz Protocol (simultaneous)

- Consider 2-out-of-2 secret sharing, the strategy for both to cooperate is a Nash equilibrium if for every i:

$$u_i(C,C) > u_i(D,C)$$

- The expected utility when deviating (D) is:

$$\beta \cdot U_i^{+} + (1-\beta)\cdot U_i^{-}$$

- Therefore, it should hold that:

$$U_i > \beta \cdot U_i^{+} + (1-\beta)\cdot U_i^{-}$$

- This occurs when: $$\beta < \frac{U_i - U_i^{-}}{U_i^{+} - U_i^{-}}$$

- Observe that the protocol is dependent on the utilities

Utility Dependence

- In reality, the utility of a party may not even be known to itself
- Even if a party knows its own utility, it is unclear how others can learn this value
- Therefore, we don't know how to set the correct β

Our First Question

Is it possible to construct a reconstruction protocol that achieves (at least) Nash Equilibrium for all possible values of utility functions (that fulfill the assumptions)?

*We call such a protocol "**utility independent**"*

Is there a difference between simultaneous and non-simultaneous channels?

Simultaneous vs. Non-Simultaneous

- *Is there a difference between simultaneous and non-simultaneous channels?*

Simultaneous | Non-simultaneous

Our Results

Is it possible to construct a reconstruction protocol that achieves (at least) Nash Equilibrium for all possible values of utility functions (that fulfill the assumptions)?

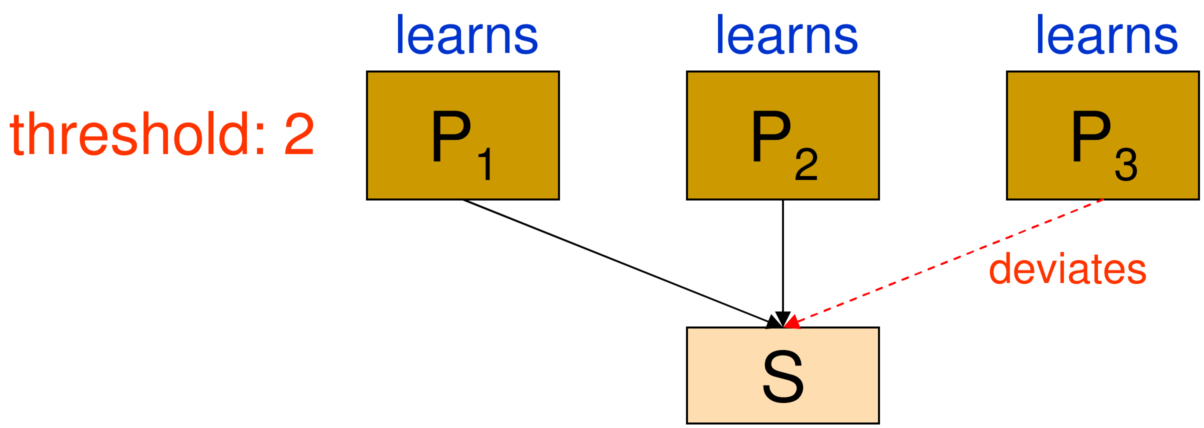
- For 2-out-of-2:
  - NO (both models)
- For t-out-of-n:
  - Coalition of size more than t/2: NO (both models)
  - Coalition of size less then t/2: YES (simultaneous)

Positive Result

- Theorem
  - There exists a multiparty reconstruction protocol that is **independent** of the utility functions of the players and is resilient to coalitions of size less than t/2 (in the simultaneous model)
    - This result does not appear in the proceedings
      - See the full version on **ePrint report 2009/373**
    - Based on an important observation that was made by Lysyanskaya-Triandopoulos (CRYPTO 2006)

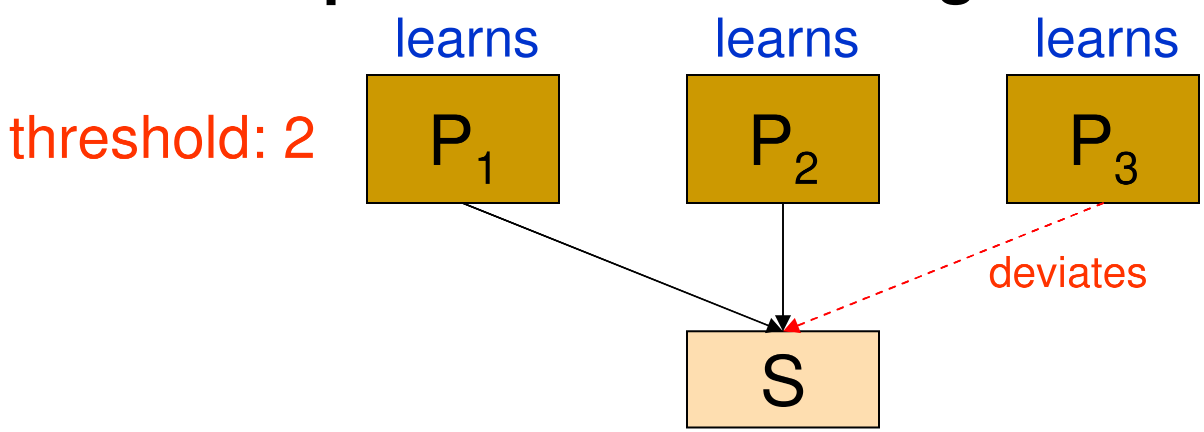
Complete Independence t-out-of-n (simultaneous)

- An additive share helps to achieve fairness
- Consider 2-out-of-3 secret sharing scheme, Naïve protocol
  - All 3 parties participate in the reconstruction phase
- Even if one of the parties does not cooperate, all parties learn the secret



An additive share helps to achieve fairness

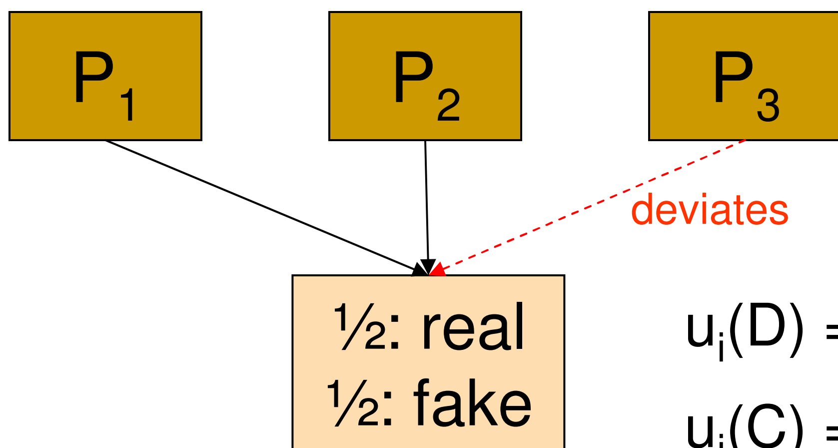
- All cooperating is Nash Equilibrium! [HT, STOC04]
  - Assume that all the other are cooperating:
    - $u_i(C,\mathbf{C}) = U_i$
    - $u_i(D,\mathbf{C}) = U_i$
- But, this Nash Equilibrium is very weak guarantee:
  - Deviating is never worse than cooperating, sometimes even better
  - Cooperating is weakly dominated by deviating
- **The naïve protocol is not enough!**



An additive share helps to achieve fairness

- We need to add some penalty
  - Consider Gordon-Katz protocol, with $\beta = ½$
- Cooperating is still best response
- All cooperating is still in Nash Equilibrium
- Cooperation is not weakly dominated any more

threshold: 2



$u_i(D) = ½\, U_i + ½\, U_i^-$

$u_i(C) = U_i$

Complete Independence t-out-of-n (simultaneous)

- If the number of parties that are participating in the reconstruction phase is greater than the threshold – it is possible to achieve **utility-independent** protocol
  - $t^* > t$ parties in the reconstruction phase

- What about $t^* = t$?
  - What about n-out-of-n secret sharing?

Complete Independence In Multiparty (simultaneous)

- The dealer protocol:
  - Generate a random **r** $\in \{0,1\}^k$
  - Create shares for **r** with threshold **t**
  - Create shares for **s**$\oplus$**r** with threshold **t/2**

- The reconstruction:
  - The parties will reconstruct **r** using the Naïve protocol
    - If anyone deviates – the game is terminated
  - The parties will reconstruct **s**$\oplus$**r** using the Gordon-Katz protocol with β **= ½**

Complete Independence In Multiparty (simultaneous)

- We also showed a “stronger equilibrium”
- We showed that the protocol is resilient to coalitions of size less than t/2

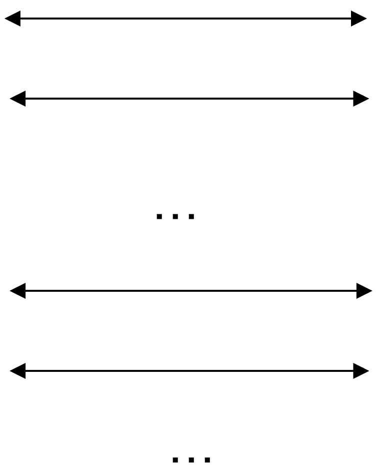
- Using our impossibility result, this protocol is optimal with respect to coalitions

Correctness in Non-Simultaneous Model

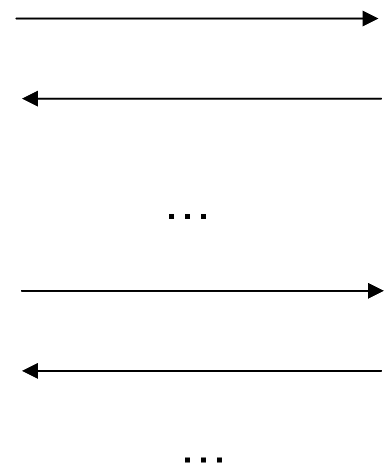
(two party)

Simultaneous vs. Non-Simultaneous

Simultaneous



Non-simultaneous



Correctness in Non-Simultaneous Model

- Kol and Naor [STOC 08] – presented a protocol for the non-simultaneous model
  - In their protocol, a party can cause the other to output an incorrect value (at the expense of not learning)
  - They assumed that parties always prefer to learn and so will not carry out this attack

Correctness in Non-Simultaneous Model

- We added another utility value:
  - U^f – a player does not learn the secret, but causes the other to output a wrong value
  - Kol-Naor assume that $U^f < U$
- We study the setting where U^f may be greater than U

Questions (non-simultaneous)

- *Can we construct a protocol in the non-simultaneous model that works (both parties output correct secret) even if $U^f > U$?*
  - *If the U^f_i values are known, the answer is YES*
  - *We construct a (utility dependent) protocol that solves this problem of correctness (based on the Kol-Naor protocol)*
- *Can we construct a protocol that works for every value of U_i^f ? (it may know the other utilities)*
  - *NO: Dependence on U^f is inherent*
  - *We prove that a "correct" protocol cannot be "fair"*

Conclusion

Blue – Known Results

Red - Open Questions

U^+ is known	U^f is known	Simultaneous	Non-simultaneous
yes	yes	✓	* ✓
yes	**NO**	✓	New ✗ – two party ? – multiparty
NO	yes	New ✗ – two party ✓ – multiparty	New ✗ – two party ? – multiparty
NO	**NO**	New ✗ – two party ✓ – multiparty	New ✗ – two party ? – multiparty

* - our result, based on Kol-Naor protocol


Thank You