# Limits on the Power of Cryptographic Cheap Talk

Pavel Hubáček*
Jesper Buus Nielsen
Alon Rosen

*Produced all the good slides

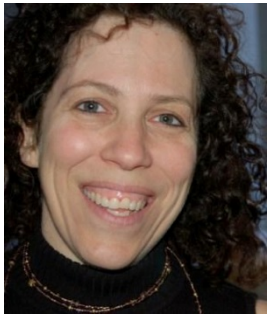
# NE, Nash 1950

| | | | |
|---|---|---|---|
| | 14/3 | 6, 6 | 2, 7 |
| | 14/3 | 7, 2 | 0, 0 |

# CE, Aumann 1974

**Correlated equilibria can pick up more utility!**

Play right!



5>14/3

| | | |
|---|---|---|
| 4 | 6, 6 | 2, 7 |
| 7 | 7, 2 | 0, 0 |

Play top!

# Dodis-Halevi-Rabin 2000

**For any CE, a computational NE achieving the same utility!**

**Bad advice, I abort!**

Cheap Talk

Top!

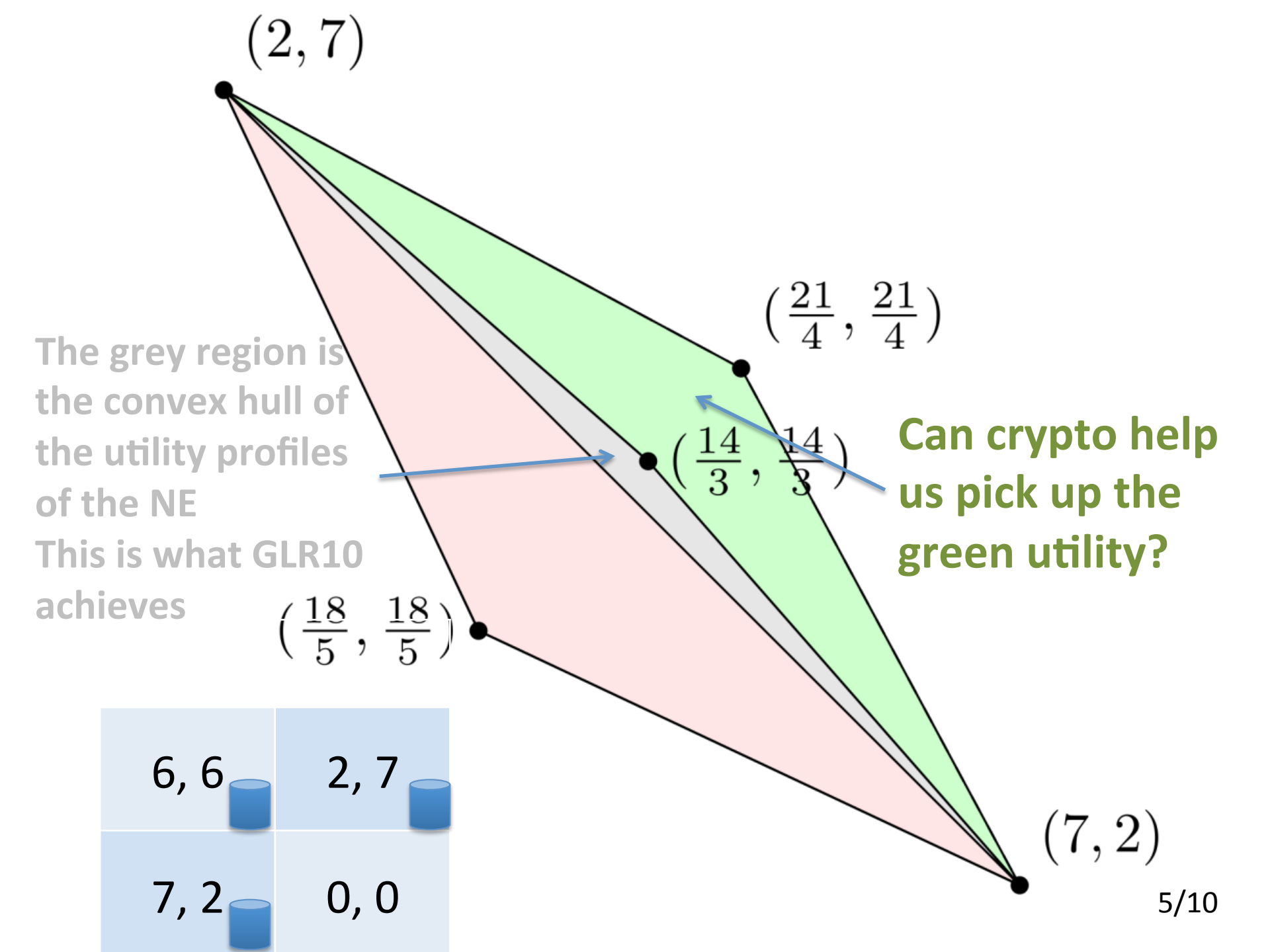
Right!

| | |
|---|---|
| 6, 6 | 2, 7 |
| 7, 2 | 0, 0 |

**MiniMax**

# Gradwohl-Livne-Rosen 2010

- MiniMax might be an empty threat
- First explicit model of **empty threat-free** (ETF) strategy for a cryptographic cheap-talk game
- Gives an ETF strategy for large sub-class of CE


$(2, 7)$
$(\frac{21}{4}, \frac{21}{4})$
$(\frac{14}{3}, \frac{14}{3})$
$(\frac{18}{5}, \frac{18}{5})$
$(7, 2)$
The grey region is the convex hull of the utility profiles of the NE
This is what GLR10 achieves
Can crypto help us pick up the green utility?
6, 6
2, 7
7, 2
0, 0

# Def. 1: NES⊂CE

- A CE is called **NE-Safe** (NES) iff *the residual utility given any advise is at least the utility in the worst NE for the same player*

# Def. 2: ETF$\subset$CE

- A CE **S** for a matrix game **M** is called **ETF** if there exist an ETF strategy for the corresponding cryptographic cheap-talk game for **M** which has the same utility profile as **S**
- *"The utility which we can pick up using cryptographic cheap-talk"*

# Hubáček-N-Rosen 2013

- We identify and define **NES**
  - The NE safe correlated equilibrium
- We prove:
  - **ETF $\subset$ NES**
  - **CE $\not\subset$ NES**
  - **If OT exists then ETF = NES**
  - **If ETF = NES then OT exists**

# ETF

- A strategy is **ETF** if it is a computational NE and neither player has an empty threat
- **Empty threat** of Rabin in strategy **$S=(S_R,S_C)$** :
  *A non-negligible event **E** observable by Canetti and a deviation **D** for Canetti such that:*
  *if Canetti switch to **D** when observing **E**, then in all ETF continuations, following the switch, Canetti gets non-negligibly more utility than if he had stuck to **S***

# ETF $\subset$ NES

- Assume a strategy is not NES for Rabin
- **Event E**: Rabin receives an advice with residual utility lower than her worst NE
- **Deviation D**: Rabin sends her advice + entire view of the protocol to Canetti and then plays according to her worst NE
- **Analysis**: After Rabin reveals her view to Canetti, they essentially only have common randomness, so if the continuation is stable, it is a (convex combination of) NE

# CE $\not\subset$ NES