Adaptively Secure UC Constant Round MPC Protocols

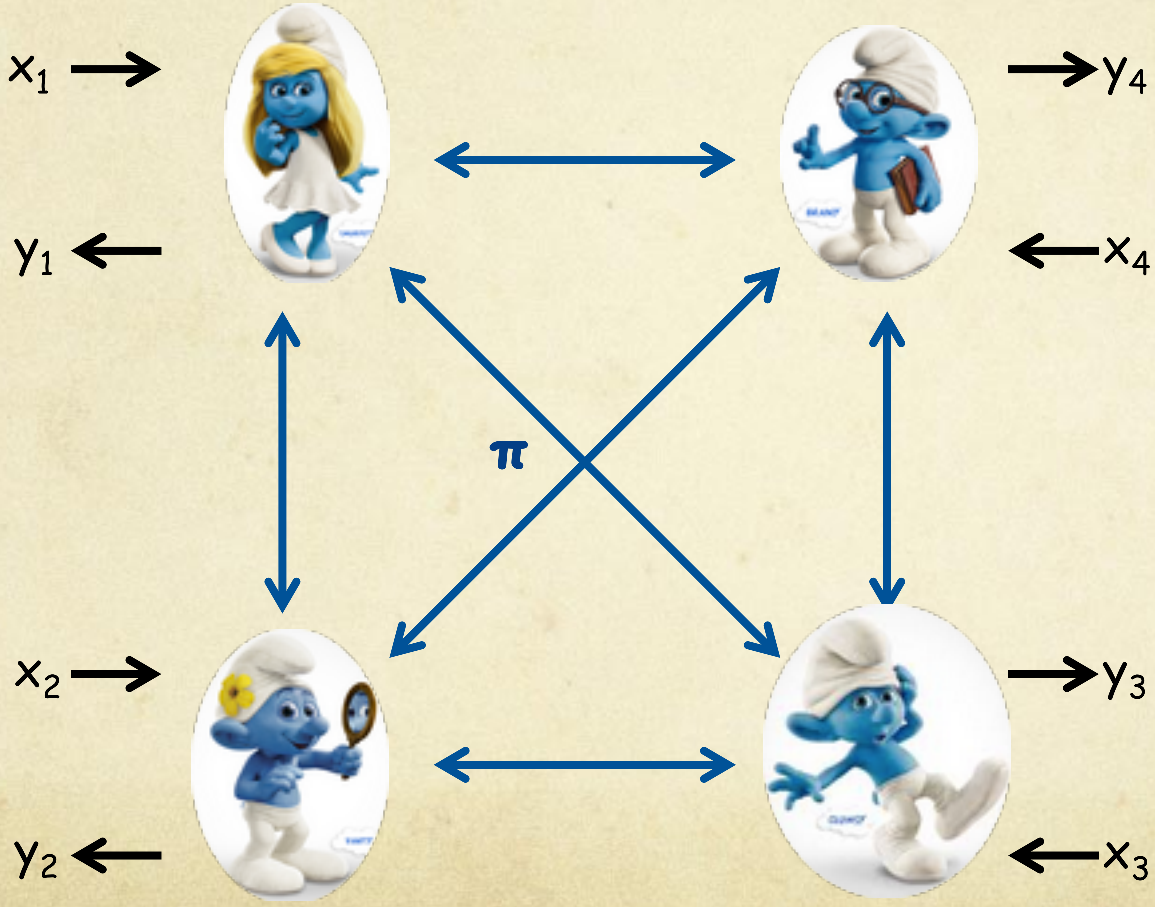
Ivan Damgård, Aarhus University

Antigoni Polychroniadou, Aarhus University

Vanishree Rao, UCLA

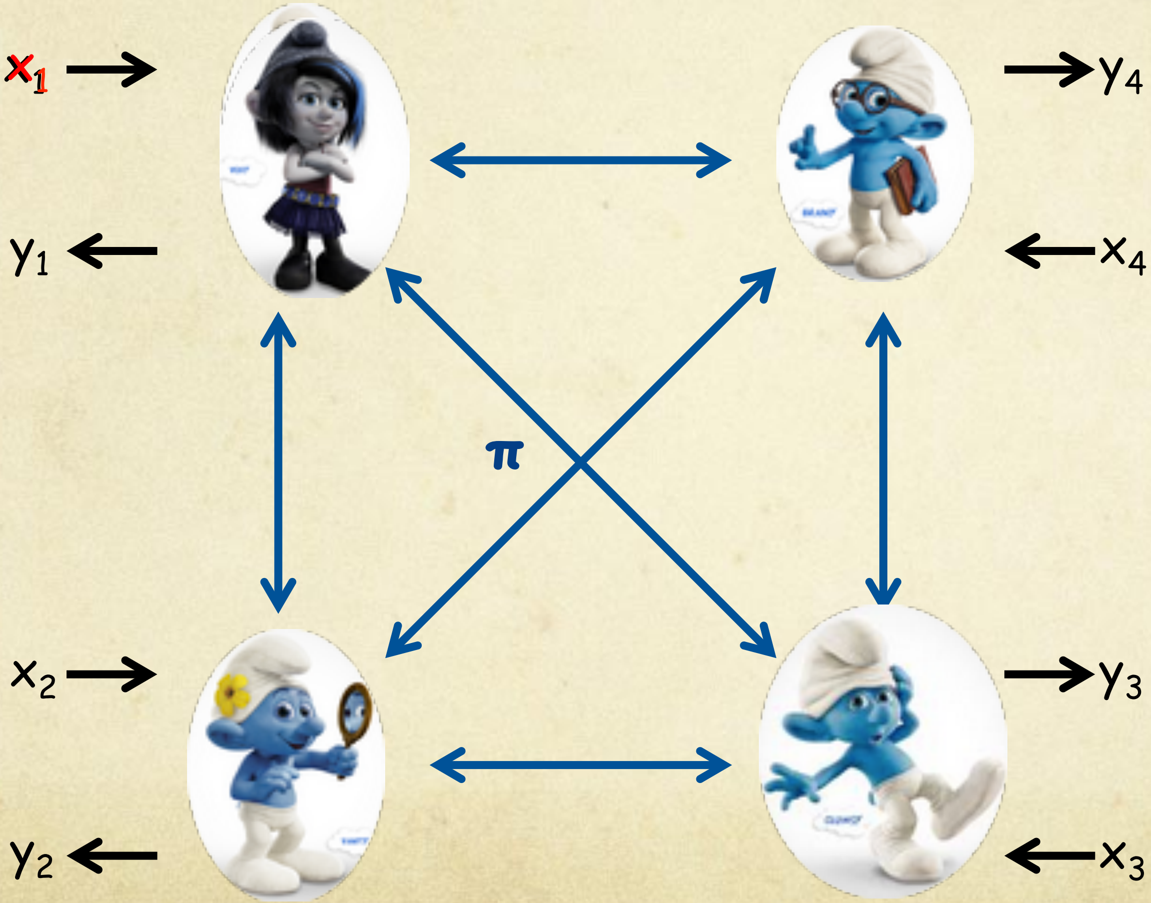
The MPC problem

$f(x_1, x_2, x_3, x_4) = (y_1, y_2, y_3, y_4)$



The MPC problem

$f(x_1, x_2, x_3, x_4) = (y_1, y_2, y_3, y_4)$



Adversary:

Passive or Active

Static or Adaptive

Unbounded or PPT

Adaptive security

Dishonest majority

“Low” Communication complexity

Constant number of rounds

- ✓ Adaptive security
- ✓ Dishonest majority
- ✓ “Low” Communication complexity
- ✓ Constant number of rounds

Known Results (Emphasis on Round Efficiency and majority)

Information theoretic setting

- [BGW88]: Unconditionally and adaptively secure. **Not** constant round.

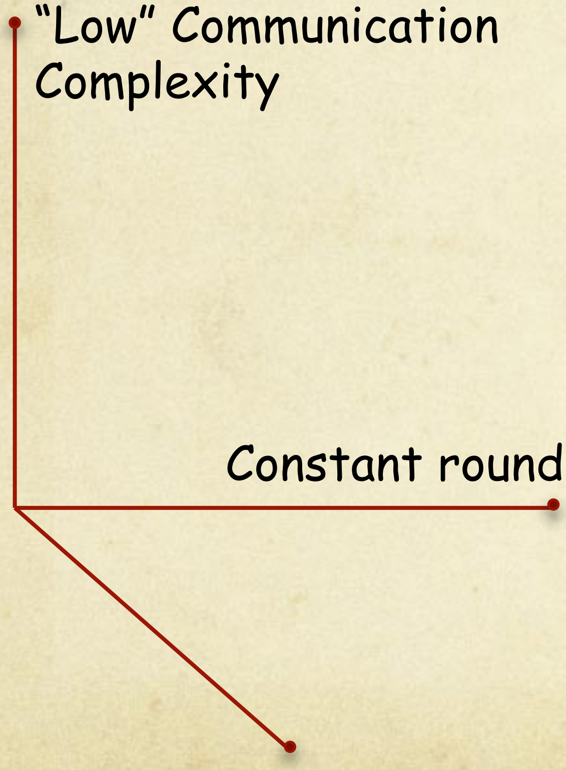
Known Results in UC (Emphasis on Round Efficiency)

Cryptographic setting

- Yao's garbled circuits for 2 parties (constant round but not adaptive)
- *Constant Round*: Protocols based on FHE [G09], [AJLTVW12] (not adaptive)

Comparison of protocols on a cube

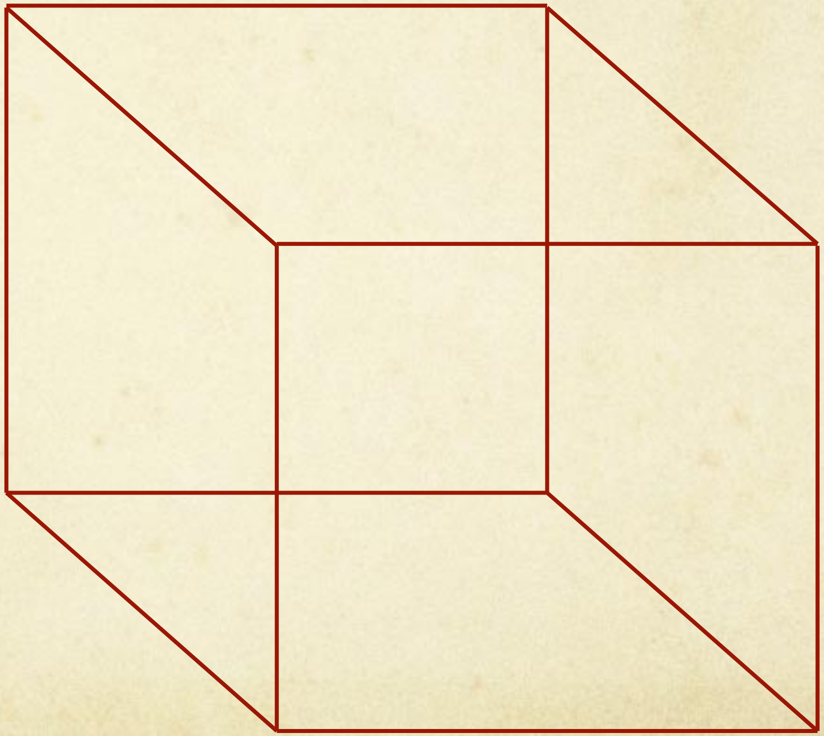
Static Schemes based on FHE: [G09], [AJLTVW12]



"Low" Communication Complexity

Constant round

Dishonest Majority



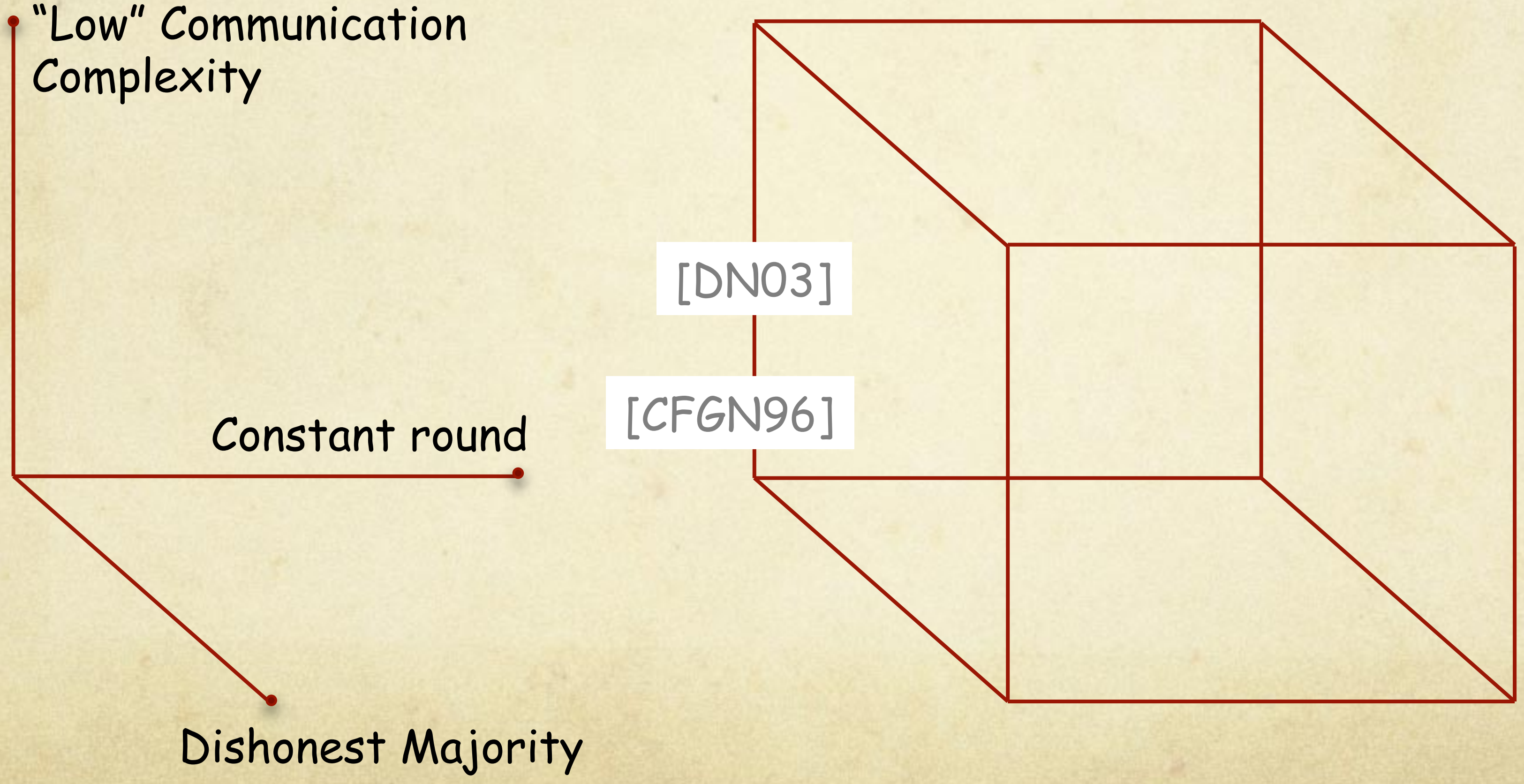
Known Results in UC (Emphasis on Round Efficiency)

Cryptographic setting

- Yao's garbled circuits for 2 parties (constant round but not adaptive)
- *Constant Round*: Protocols based on FHE [G09], [AJLTVW12] (not adaptive)
- *Adaptive security*: [CFGN96] and Protocols based on additively HE [DN03] (not constant round and only for honest majority)

Comparison of protocols on a cube

Static Schemes based on FHE: [G09], [AJLTVW12]



"Low" Communication Complexity

Constant round

Dishonest Majority

[DN03]

[CFGN96]

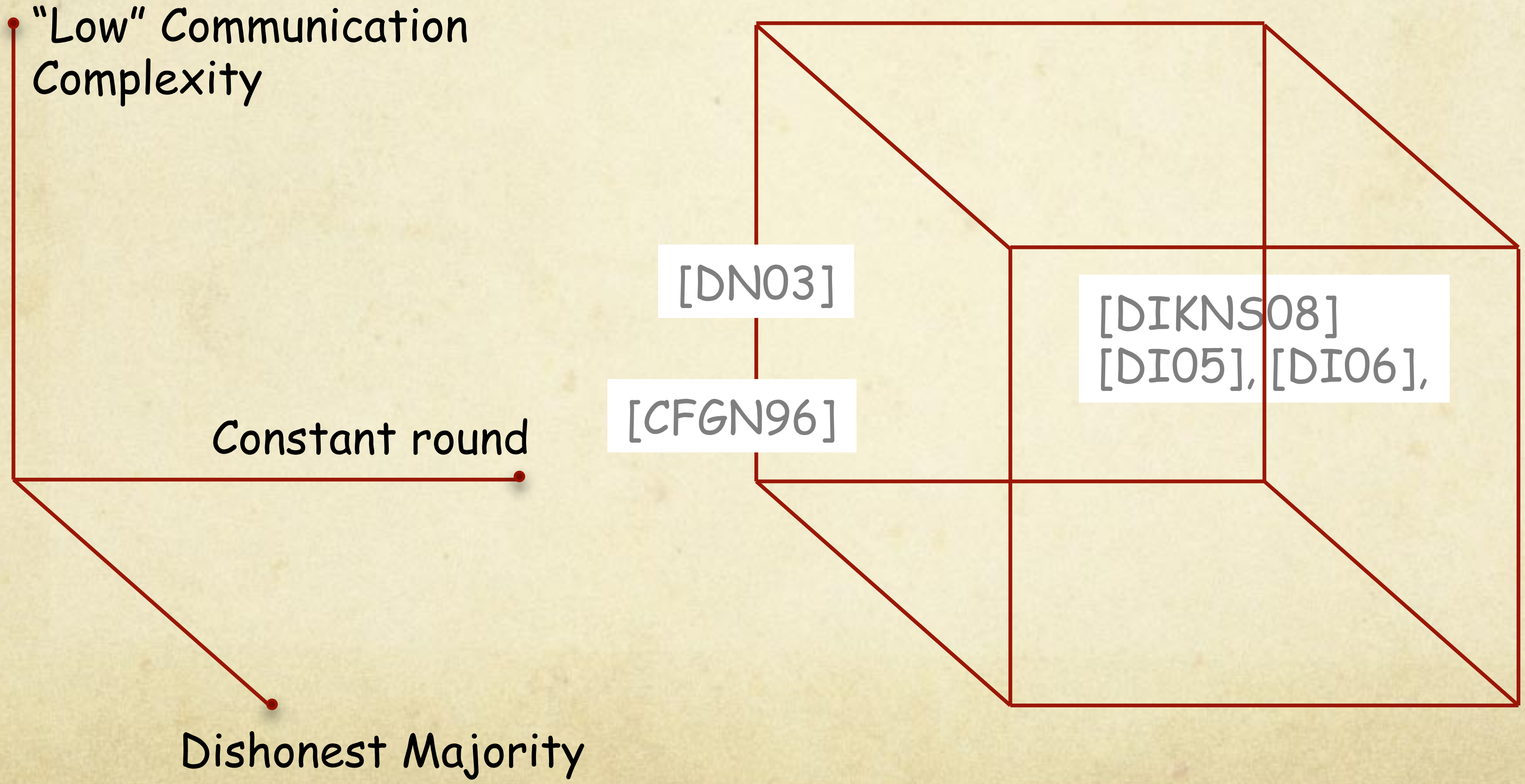
Known Results in UC (Emphasis on Round Efficiency)

Cryptographic setting

- Yao's garbled circuits for 2 parties (constant round but not adaptive)
- *Constant Round*: Protocols based on FHE [G09], [AJLTVW12] (not adaptive)
- *Adaptive security*: [CFGN96] and Protocols based on additively HE [DN03] (not constant round and only for honest majority)
- *Constant round & Adaptive security*: [DI05], [DI06], [DIKNS08], [IPS08]: use an unconditionally secure protocol to compute, for instance, a Yao garbled circuit, that is then used to compute the desired function in constant round.

Comparison of protocols on a cube

Static Schemes based on FHE: [G09], [AJLTVW12]



"Low" Communication Complexity

Constant round

Dishonest Majority

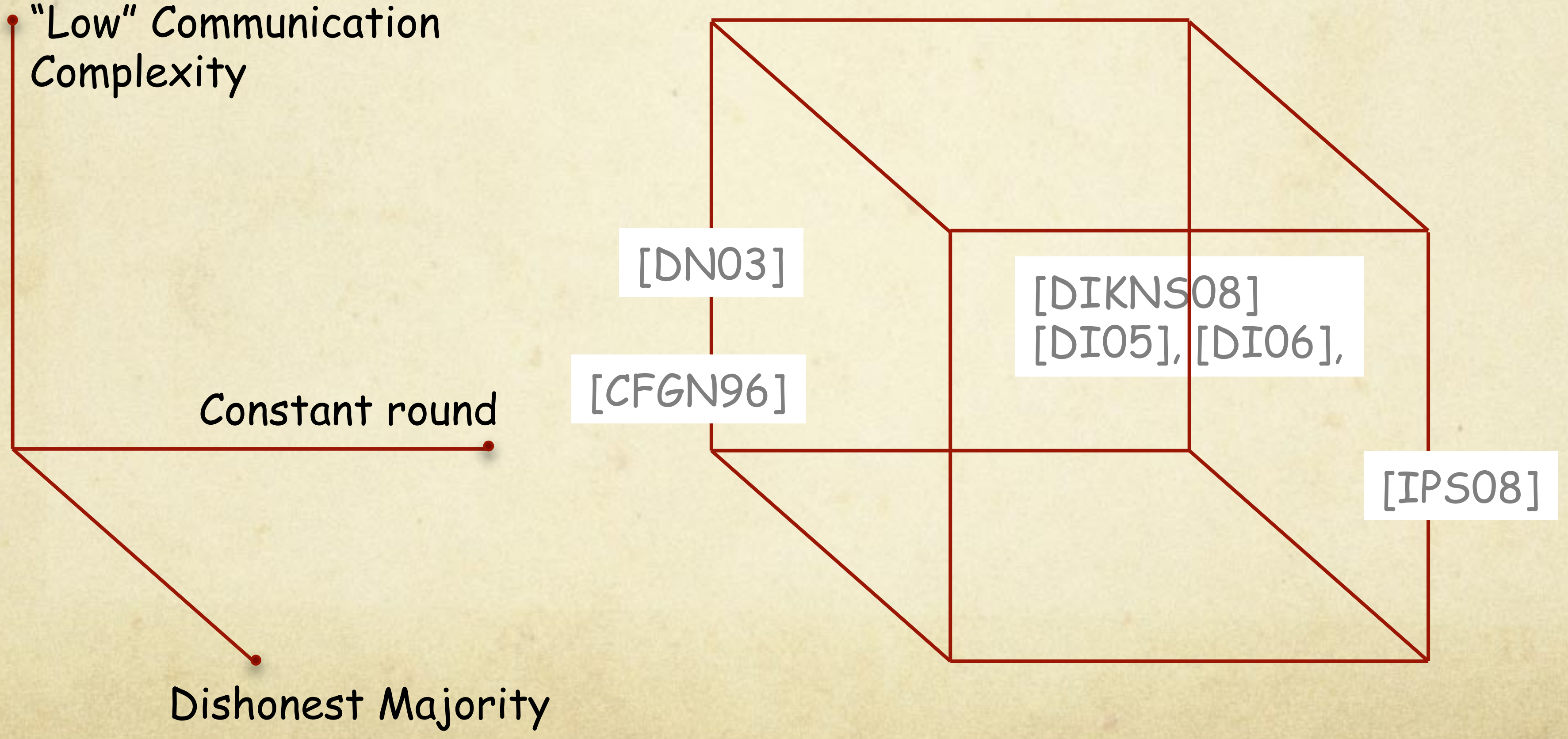
[DN03]

[CFGN96]

[DIKNS08]
[DI05], [DI06],

Comparison of protocols on a cube

Static Schemes based on FHE: [G09], [AJLTVW12]



"Low" Communication Complexity

Constant round

Dishonest Majority

[DN03]

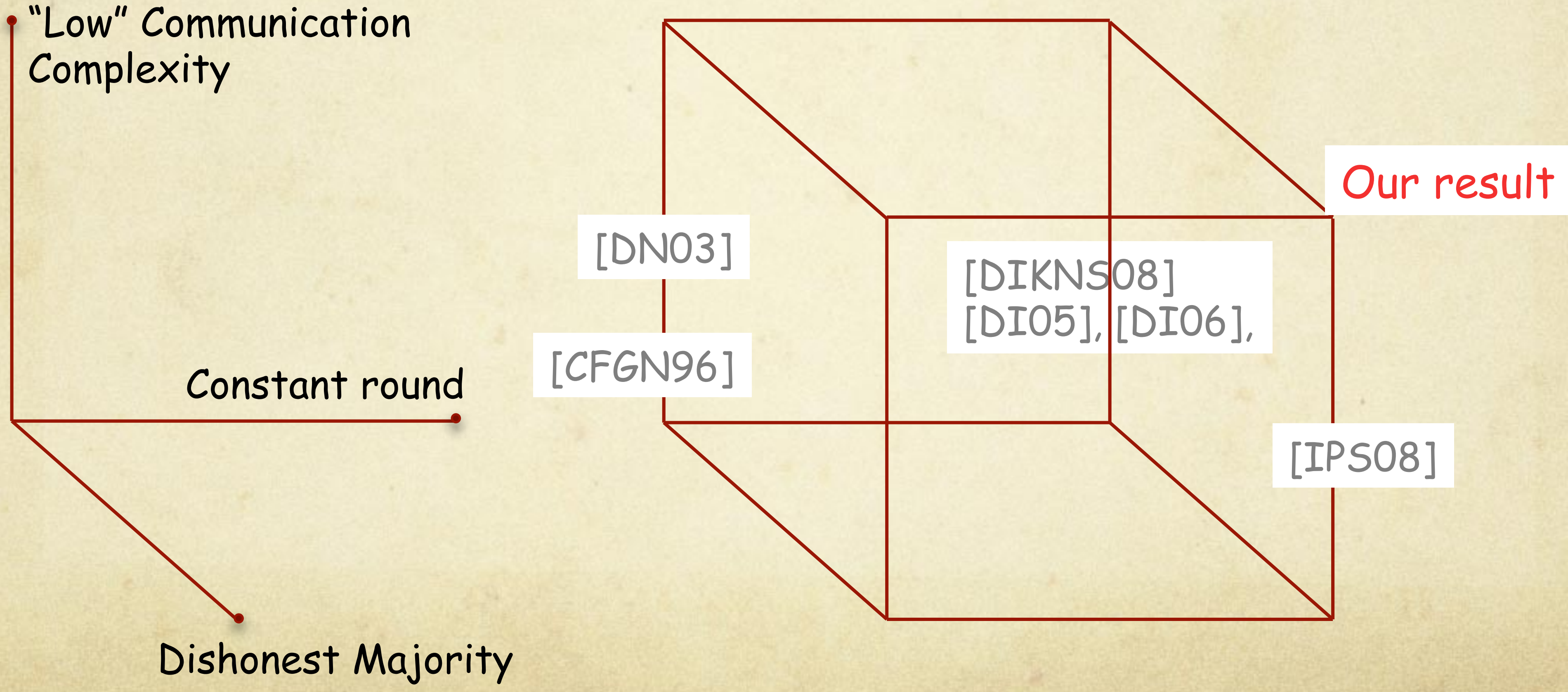
[CFGN96]

[DIKNS08]
[DI05], [DI06],

[IPS08]

Comparison of protocols on a cube

Static Schemes based on FHE: [G09], [AJLTVW12]



"Low" Communication Complexity

Constant round

Dishonest Majority

[DN03]

[CFGN96]

[DIKNS08] [DI05], [DI06],

[IPS08]

Our result

Our Result

An adaptively secure UC MPC protocol with dishonest majority and a constant number of rounds.

Our Model:

n Parties

Broadcast Channel

r-round protocol, where r is constant

Adversary *Adv*:

- PPT (Cryptographic setting)
- Active
- Adaptive

Dishonest Majority in UC (≤n-1) ⇒ set up assumption

Thank you!