Somewhat Non-Committing Encryption and Adaptively Secure Oblivious Transfer

Juan Garay, **Daniel Wichs**, Hong-Sheng Zhou

Oblivious Transfer

- Cornerstone of secure multiparty computation : [Yao82, GMW87,…,CLOS02,…]

- **Usual Approach:** Design a protocol which is secure in the semi-honest setting. Add zero-knowledge proofs to make it secure against malicious adversaries.

- This Thursday: Peikert *et al.* [PVW08] will present the first truly efficient OT protocol which does not follow above paradigm.
  - Malicious adversaries are considered right away – no compiler.
  - Achieves UC security in CRS model.
  - …But only against **static adversaries.**

Adaptively Secure OT

- Adaptive security for OT is hard even in the semi-honest setting.

- Only few known examples of adaptively secure OT [Beaver98, CLOS02]. Little hope of making these efficient in the malicious setting.

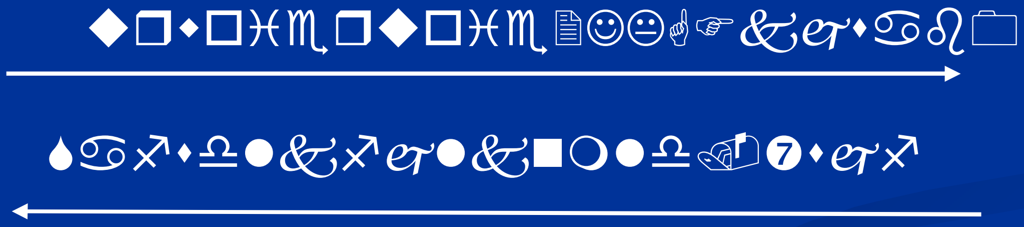
Can we make the new guy adaptive?

- First Observation: With only small modifications, we can make the scheme adaptively secure assuming that all communication is sent over *idealized private channels*.

- Unfortunately, idealized private channels are very expensive to realize! Need to use *non-committing encryption* [CFGN'06] to encrypt entire protocol transcript.
  - Current best protocols require $\Omega(1)$ exponentiations per bit of plaintext!

Non-Committing Encryption [CFGN'96]

- The simulator can run a "fake" encryption protocol and later explain it as an encryption of some arbitrarily chosen plaintext:
  - Simulator fakes a protocol transcript:



  - Later is told to explain this as an encryption of some message m. Needs to produce random coins of sender and receiver so that this looks legitimate.
- For us, this is overkill. Our simulator does not need the ability to lie about all possible choices!

Somewhat Non-Committing Encryption

- Simulator is given *t* messages:
  - (“Vote: Obama”, “Vote: McCain”, “Vote: Nader”)
- Simulator produces a “fake” transcript using these messages.
- Must later be able to explain this transcript as an encryption of any one of the *t* messages.

Conclusions

- Somewhat non-committing encryption can be made significantly more efficient than fully non-committing encryption.
- For messages of size k:
  - Fully Non Committing: $\approx k$ exponentiations.
  - Somewhat Non Committing $\approx t$ exponentiations.
- Using somewhat non-committing encryption, we can modify the Peikert *et al.* scheme to get the first truly efficient adaptively secure bit OT.

Somewhat Non-Committing Encryption and Adaptively Secure Oblivious Transfer

Juan Garay, **Daniel Wichs**, Hong-Sheng Zhou