Non-black-box Techniques Are Not Necessary for O(1)-Round Non-malleable Protocols

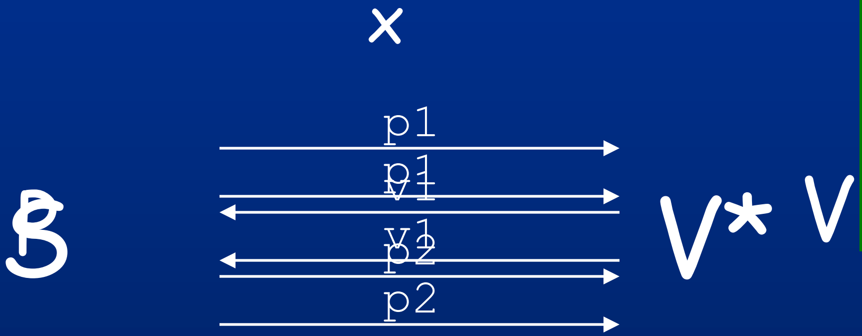
Omkant Pandey

University of California, Los Angeles

(www.cs.ucla.edu/~omkant)

Black-box vs Non-black-box Proofs

(By Ex



Black-box:

Only Oracle access to V*.

$$S^{V*}$$

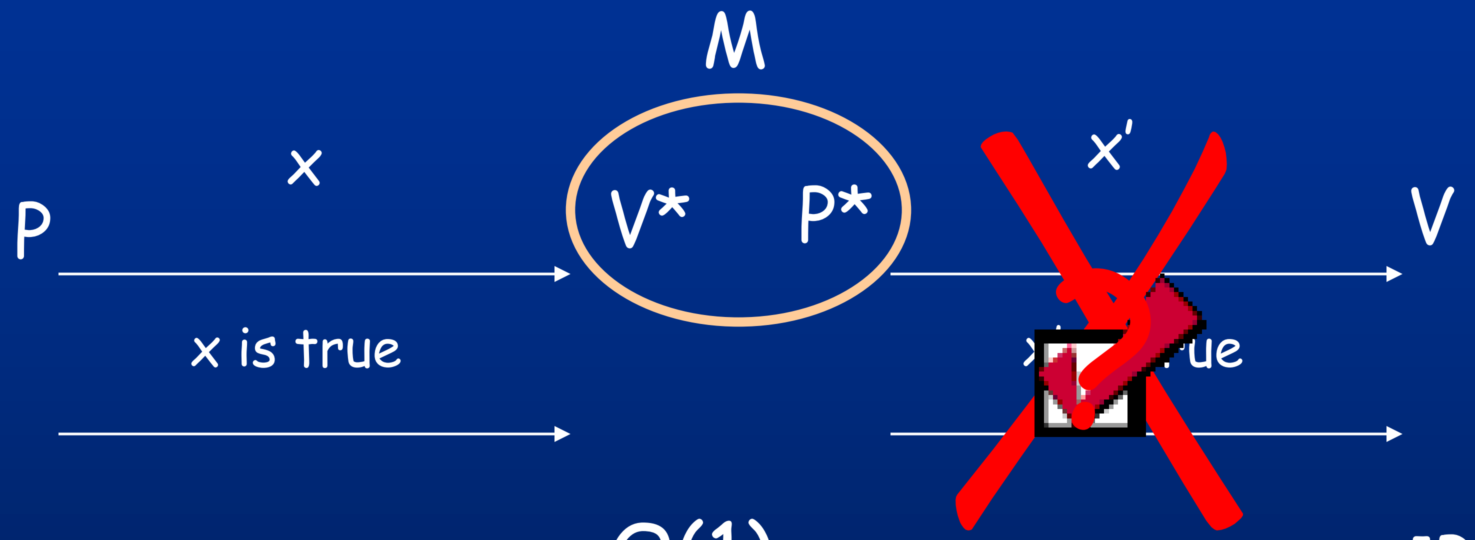
Non-black-box:

Use V* in more ways.

E.g., Code [Barak01].

Non Malleable ZK

[Dolev-Dwork-Naor, 1991]



O(1) [Pan08]

- Black-box NMZK: O(~~log~~ n) -round [~~DDN~~]

- Non-black-box NMZK: O(1) -round [Bar01,Pas04,PR05]

Assumption?

- Gap Discrete Logarithm [MMY06]

$$y=g^x[p] \rightarrow \overset{\mathcal{O}_p}{A_{DL}}$$

- Actual assumption we use is slightly weaker.
- Assumptions of Similar sort used regularly. [OP01a,OP01b]
- In the context of quasi-polynomial simulation [Pas03], have been used before [PS04,MMY06]

Other Results

- Non-interactive Non-malleable Commitments
    - First Construction (in the Plain Model)

- First (Black-box) O(1) –round stand alone MPC with dishonest majority.

- Gap-DL holds in generic group model uncond.

- Paper available on eprint.

Thanks!