A New Non-Malleable Commitment Scheme

Vipul Goyal, Silas Richelson, Alon Rosen, Margarita Vald
Non-Malleability

$C \xrightarrow{\text{Com}(m)} M \xrightarrow{\text{Com}(m')} R$

$M$ wins if $m'$ and $m$ are related.
Non-Malleable Commitment (NMC)

• Useful primitive with many applications
  – Protocol composition, constant round MPC, NMZK,...

• Long history beginning with [DDN91]:
  – [DDN91], [Bar02], [Pas04], [PR05], [LPV08], [PW10], [Wee10], [LP11], [Goy11], [GLOV12], ...

• Recently Lin, Pass [LP11] & Goyal [Goy11] provide:
  – constant round NMC from OWF!
Our Work

- **Theorem 1**: Assume OWF exist. Then there is a 4-round NMC scheme.

- **Theorem 2**: Assume OWF exist. Then there is a 4-round NMZK argument for any L in NP.
• Will appear at FOCS '14.

• Find it on eprint!