Robust Protocols from Homomorphic-CCA Encryption

Manoj Prabhakaran & Mike Rosulek

University of Illinois, Urbana-Champaign

(to appear in *ASIACRYPT* 2008)

Non-malleable Homomorphic Encryption

- Encryption scheme where:
  - Anyone can change Enc(m) to Enc(f(m)) for certain f's
  - Enc(f(m)) can't be linked to original Enc(m)
  - No other malleabilities
- Construction given in [PR08]
  - message space = G^n
  - transformation space: f(m) = m*r, for all r in some subgroup of G^n

Anonymous Opinion Poll

- Pollster: wants to conduct a poll
- Tabulator: helps pollster collect info
  - not trusted: shouldn't see the results
- Respondents: provide responses
  - don't want responses linked to their identities
  - don't trust each other / tabulator / pollster

Protocol Components:

- Non-malleable homomorphic scheme:
  - Message space: G^2
  - Transformations: (a,b) --> (a,b*r) for known r $\in$ G
  - (Cannot change first component, can't mix-and-match components from 2 ciphertexts, etc)

Protocol

Pollster cannot tell which response came with which r_i

(unlinkability & homomorphic property)

- Pollster:
  - Generate a key pair. Pick random r1
  - Send PK and ri to respondent #i
- Respondent i:
  - send Enc(mi, ri) to tabulator (mi is th
- Tabulator:
  - "rerandomize" 2nd components of ciphertexts
    - multiply by random s1 .. sn $\in$ G, whose product is 1
  - send permutation of resulting ciphertexts to pollster
- Pollster:
  - Decrypt; check product of 2nd components
  - If product preserved, accept 1st components.

The End

- Cool use of non-malleable homomorphic encryption scheme