Round Complexity of Authenticated Broadcast with Dishonest Majority [FOCS '07]

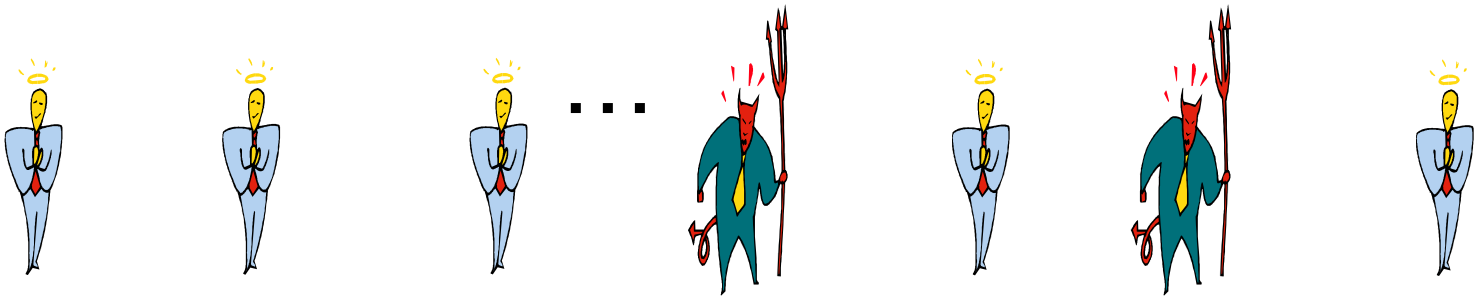
***Juan Garay* (Bell Labs)**
Jonathan Katz (University of Maryland)
Chiu-Yuen Koo (University of Maryland)
Rafail Ostrovsky (UCLA)

Broadcast (aka Byz. agreement) [PSL80, LSP82]

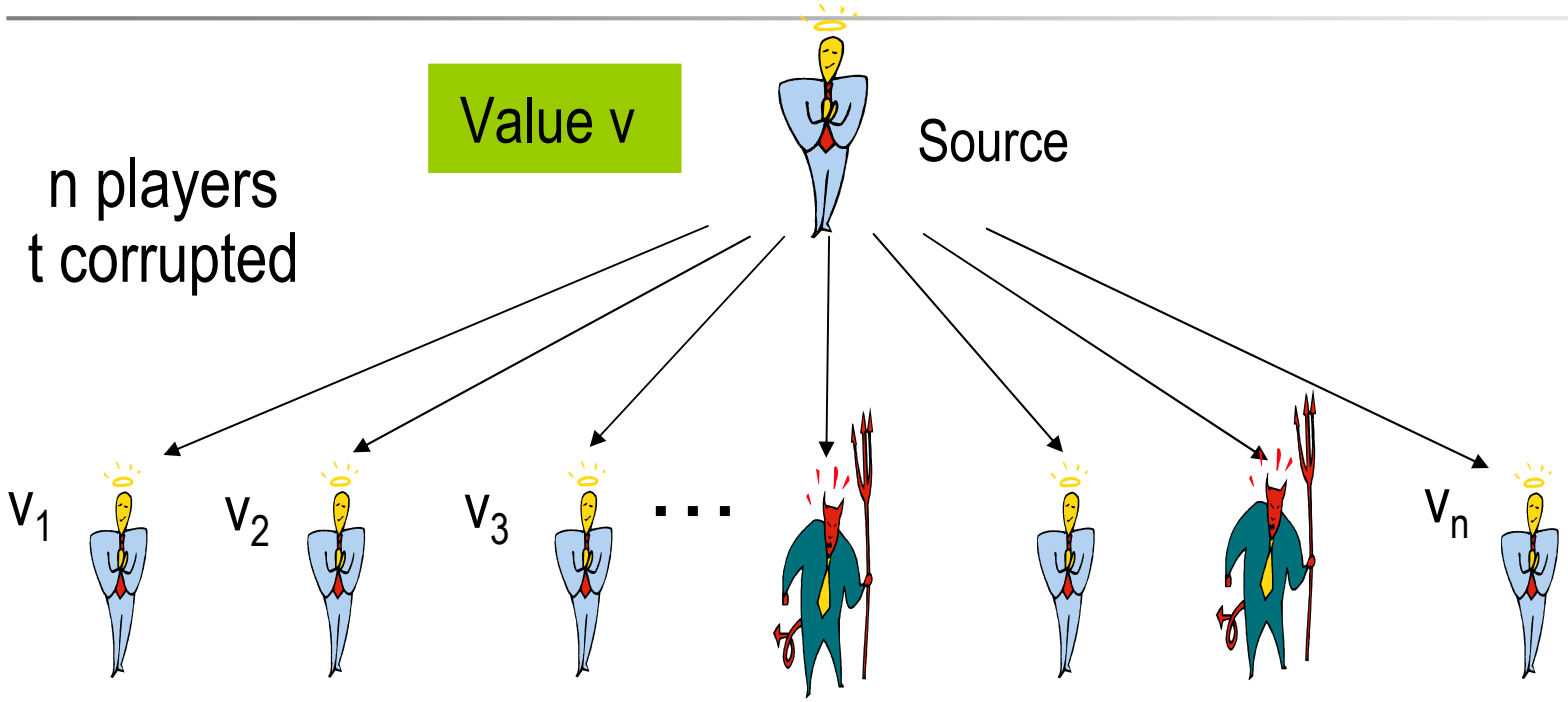
n players
t corrupted

Value v

Source



Broadcast (aka Byz. agreement) [PSL80, LSP82]



Validity: If source is honest, $v_i = v$

Agreement: $v_i = v_j$

Broadcast: Bounds

- Information theoretic:
  - $t < n/3$
  - Rounds $r = t+1$

  [PSL80, … , GM92]
- Computational ("*Authenticated*"): PKI + Signatures
  - $t < n - 1$
  - $r = t+1$

  [PSL80, DS83]

Randomized Broadcast: Bounds

- Information theoretic:
  - t < n/3
  - r = expected O(1)

  [R83, B83, … ,FM88]
- Computational ("*Authenticated*"): PKI + Signatures
  - t < n/2
  - r = expected O(1)

  [CKS00, N02, FG03, KK06]

Randomized Broadcast: Bounds

- Information theoretic:
  - t < n/3
  - r = expected O(1)

  [R83, B83, … ,FM88]
- Computational ("*Authenticated*"): PKI + Signatures
  - t < n/2
  - r = expected O(1)

  [CKS00, N02, FG03, KK06]

$$t \geqq n/2 \ ?$$

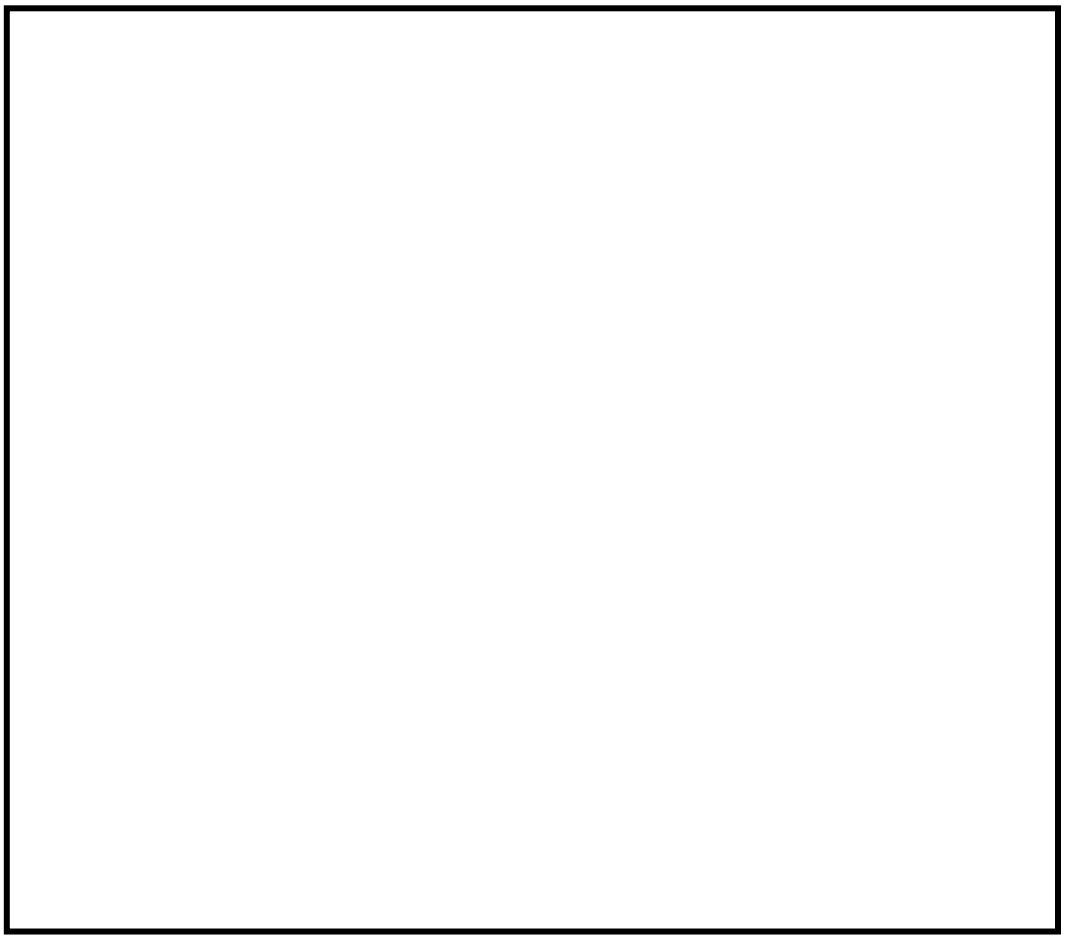
Randomized Broadcast w/ Dishonest Majority

1. Protocol:
   - $t = n/2 + k$
   - r = expected $O(k^2)$
2. Round lower bound:
   - $r = \Omega(n/(n-t))$ for any randomized broadcast protocol

Randomized Broadcast Protocol

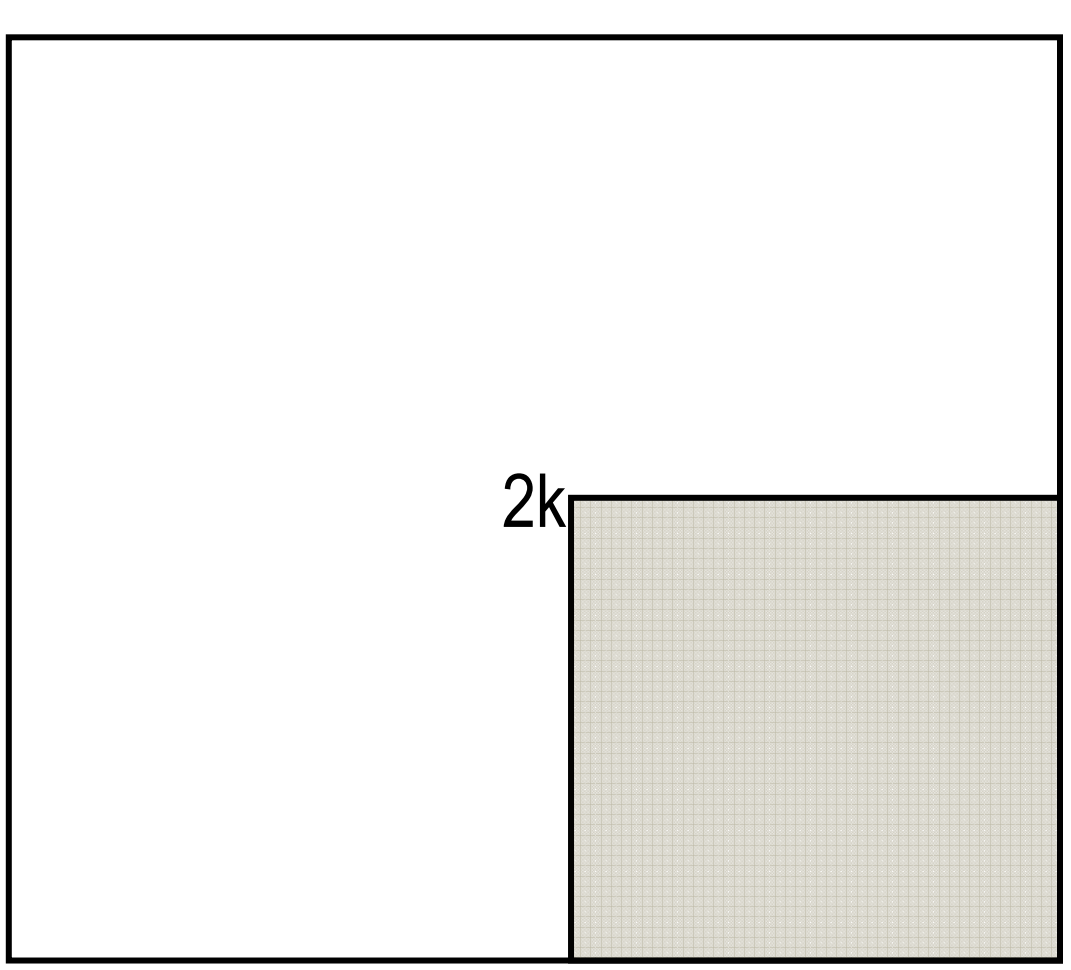
1. Protocol:
   - $t = n/2 + k$
   - $r = \exp. O(k^2)$

n



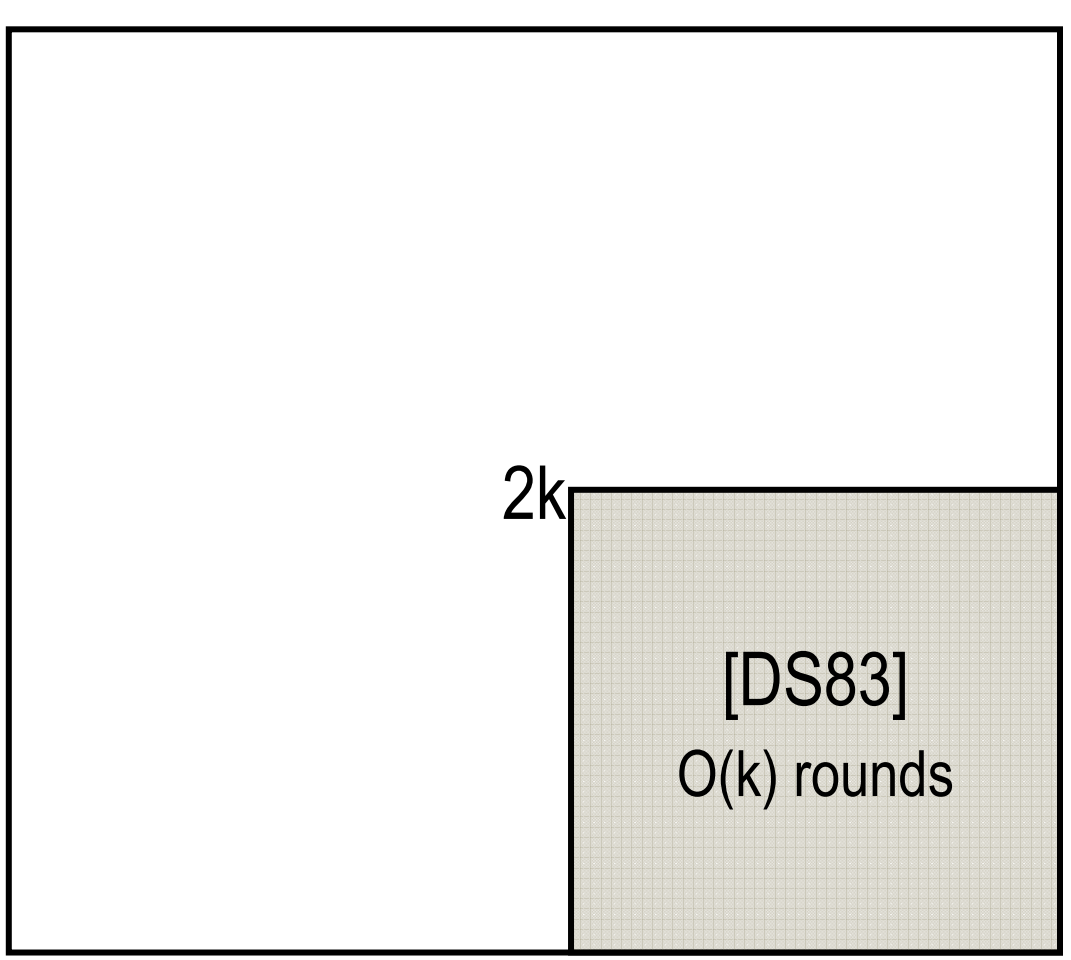
Randomized Broadcast Protocol

1. Protocol:
   - t = n/2 + k
   - r = exp. $O(k^2)$



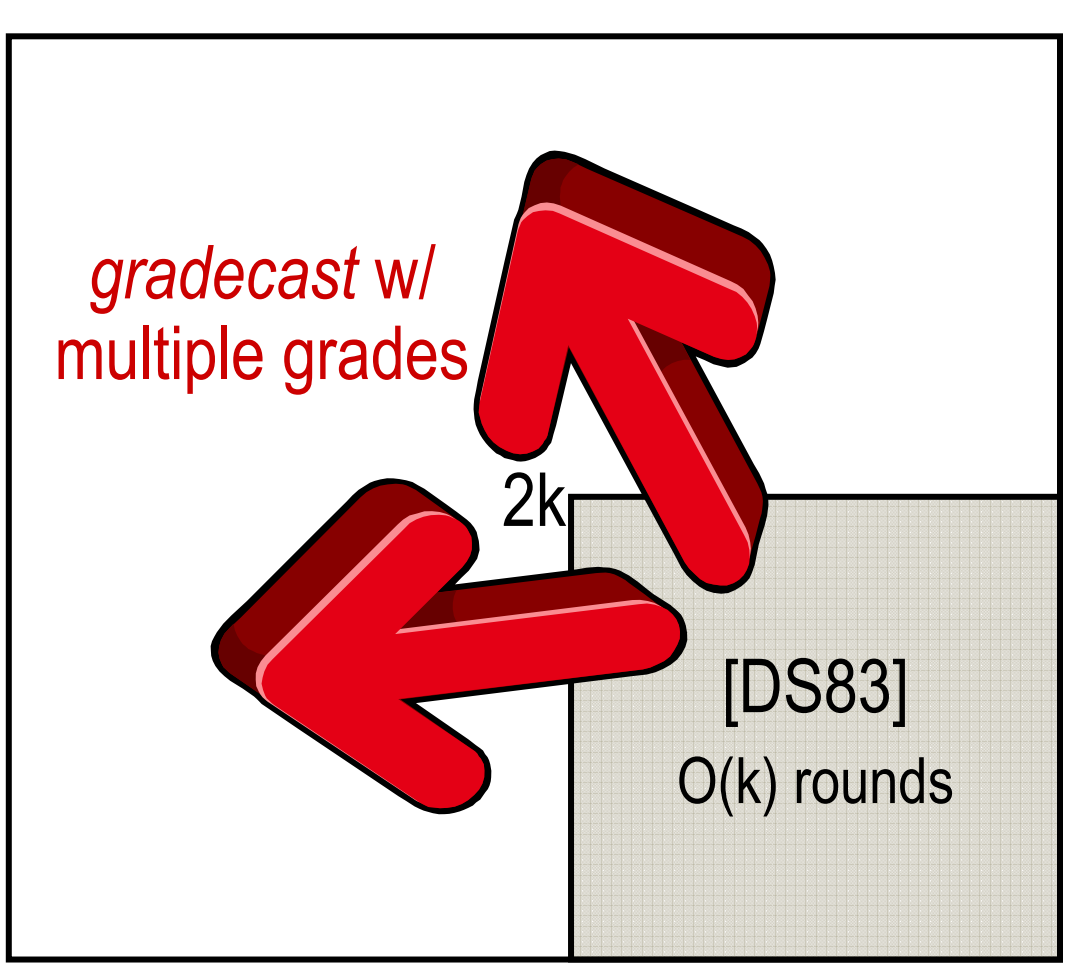
Randomized Broadcast Protocol

1. Protocol:
   - t = n/2 + k
   - r = exp. $O(k^2)$



Randomized Broadcast Protocol

1. Protocol:
   - $t = n/2 + k$
   - $r = \exp. O(k^2)$



Round Complexity of Authenticated Broadcast with Dishonest Majority [FOCS '07]

***Juan Garay* (Bell Labs)**
Jonathan Katz (University of Maryland)
Chiu-Yuen Koo (University of Maryland)
Rafail Ostrovsky (UCLA)