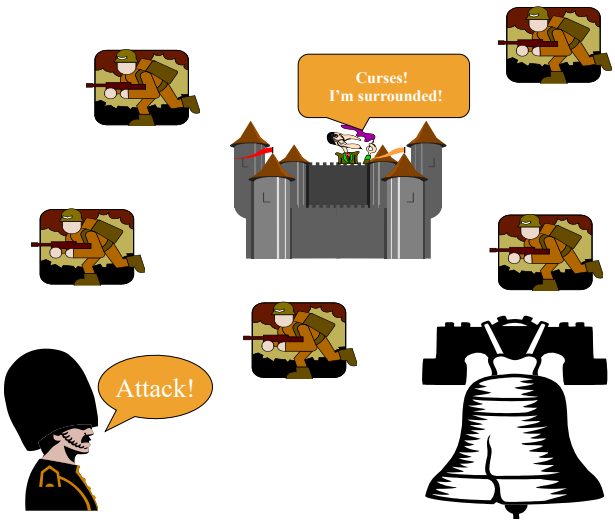
BYZANTINE AGREEMENT

68

68

Byzantine Agreement



69

69

Byzantine Agreement

- Suppose 3 generals (A,B,C), one of whom may be traitor
- General A knows he's loyal
- Take majority vote?
- But traitor may be saying different things to A and other loyal general
- Lower bound: Need at least 4 generals if 1 traitor
- Generally: Need 3f+1 processors if f are faulty

70

70

Byzantine Agreement

- Assume wlog general sending orders to lieutenants
- Give commanders ability to sign their messages
- Assume no more than f failures, and f+2 commanders

71

71

Protocol

- Round 1:
  - General broadcasts his order (true or false) to all lieutenants
- Round *i*, for loyal commander:
  - Consider any *messages* with i-1 signatures received in previous round
  - Record any *orders* signed by the general
  - Commander adds his signature to each *message*, and broadcasts result to all other processes
  - Repeat this round f times for total f+1 rounds

72

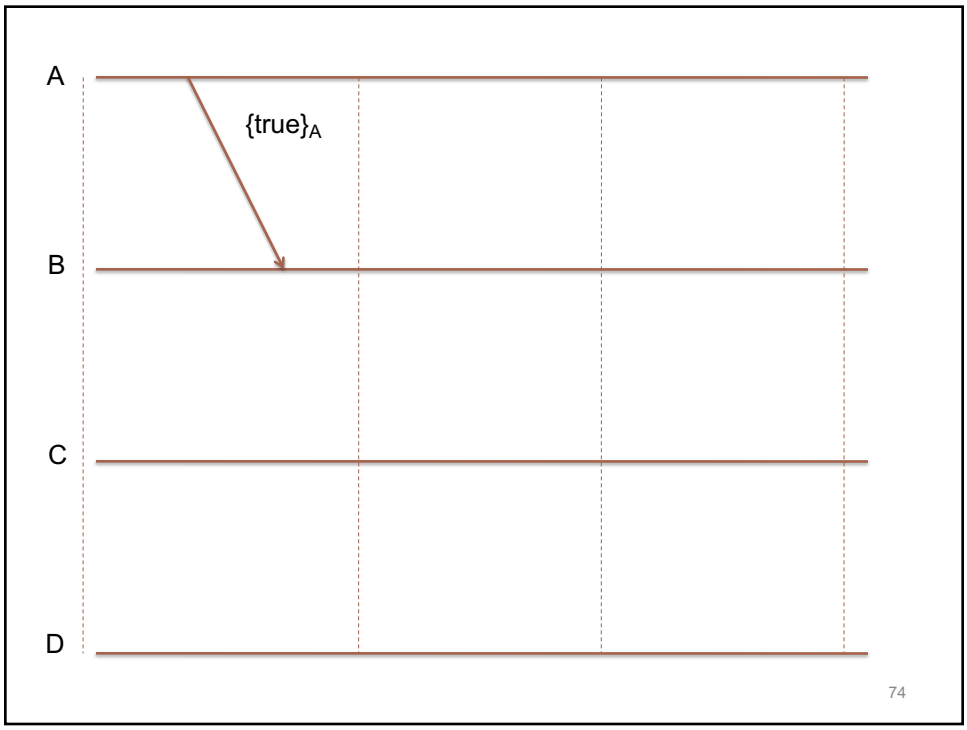
72

Protocol

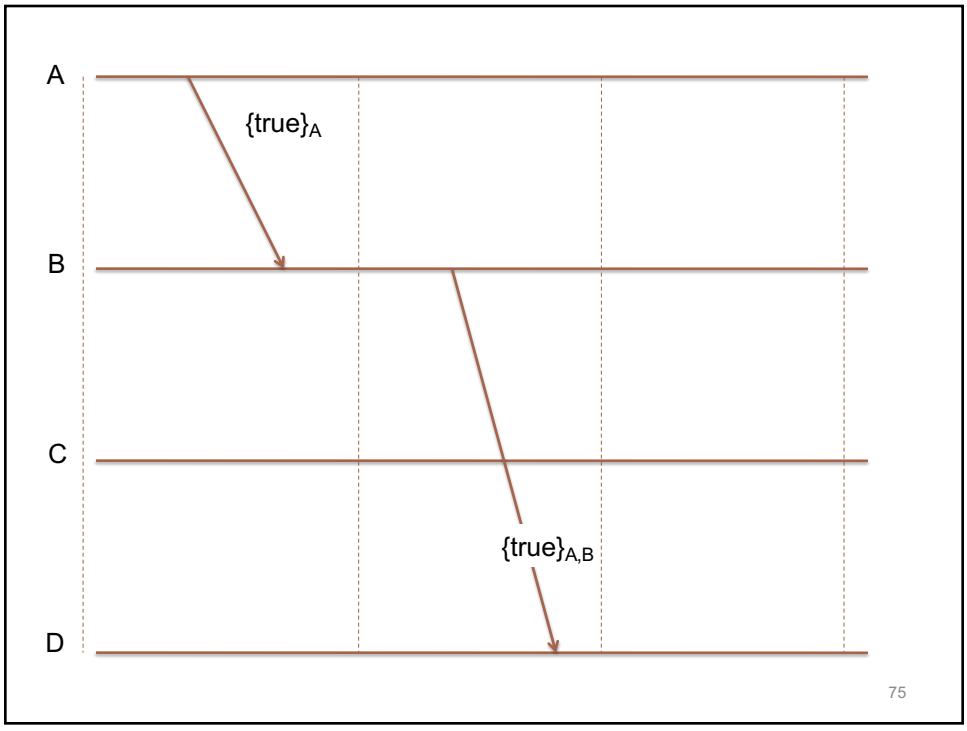
- After f+1 rounds, each loyal commander considers the orders he has recorded:
  - If empty, or conflicting orders, then choose default decision
  - If exactly one order, then execute that order

73

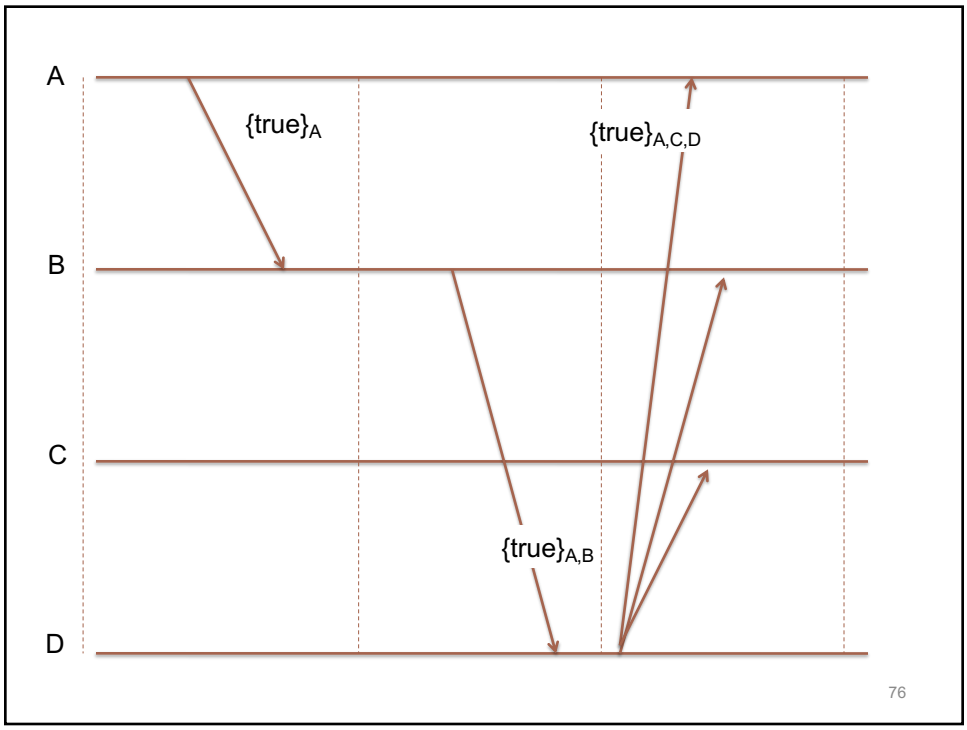
73



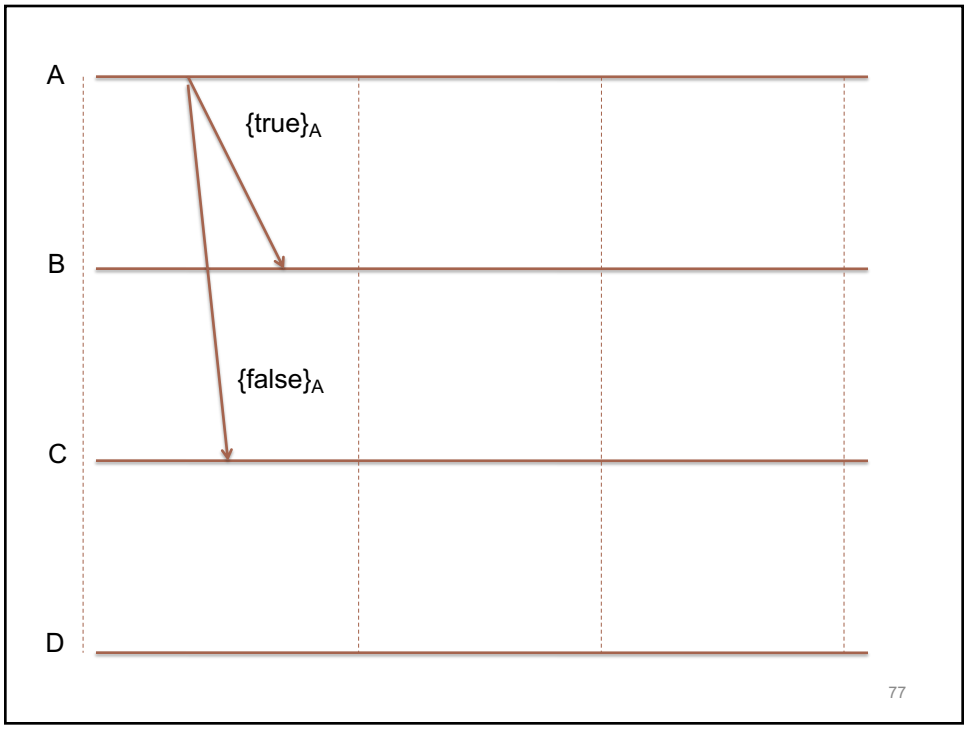
74



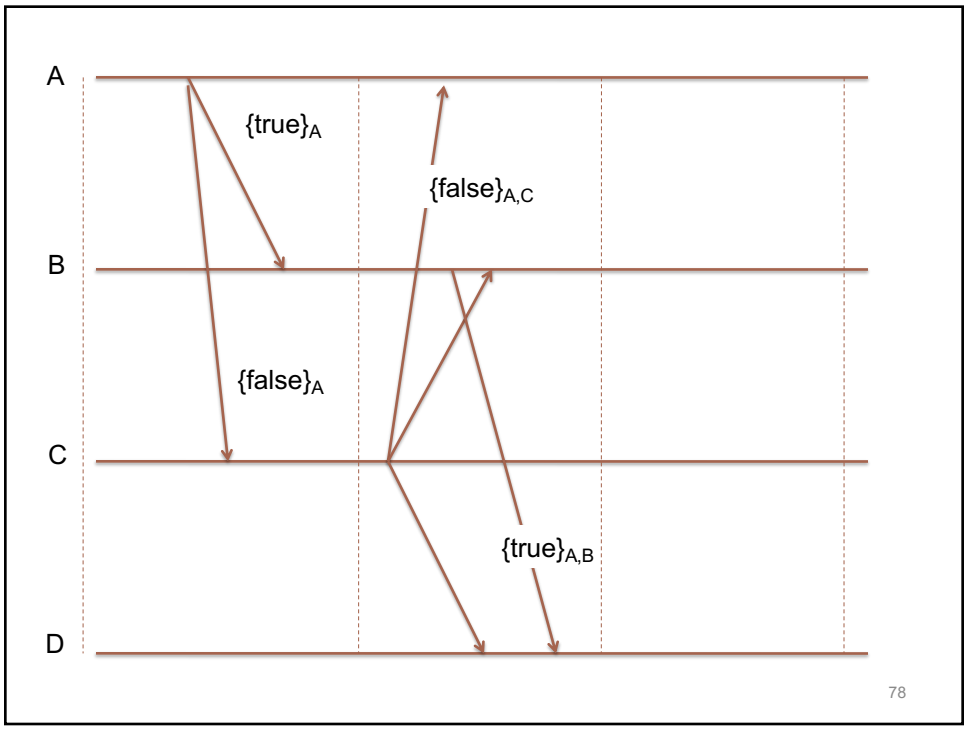
75



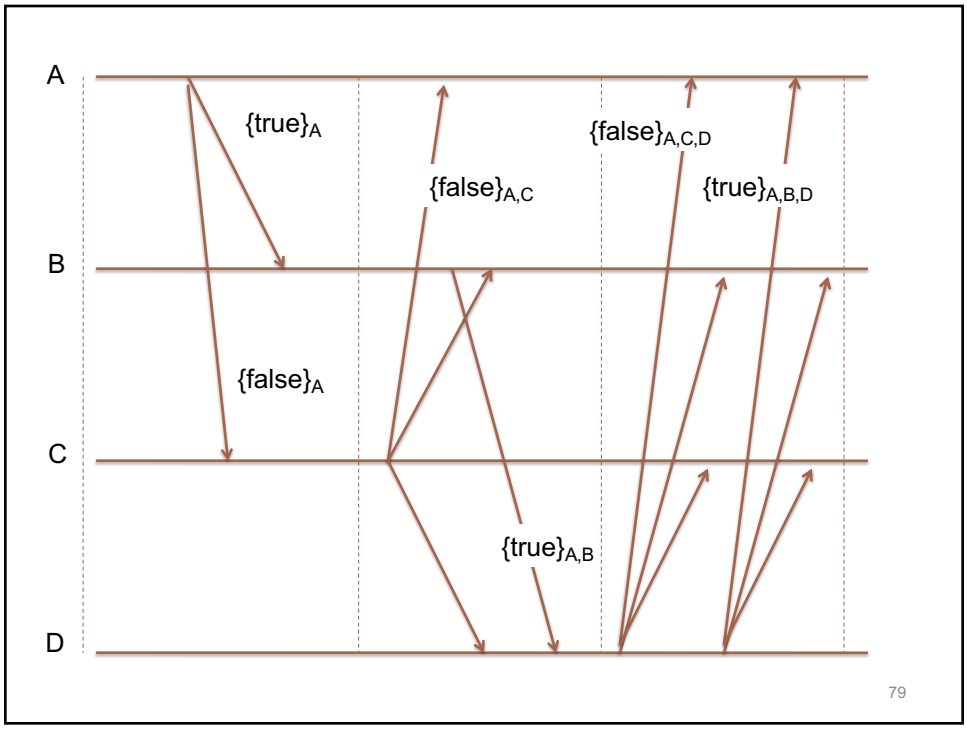
76



77


A
B
C
D
{true}A
{false}A,C
{false}A
{true}A,B
78

78


A
B
C
D
{true}A
{false}A,C
{false}A,C,D
{true}A,B,D
{false}A
{true}A,B
79

79

Why does this work?

- Suppose general is loyal
  - Broadcasts order in first round
  - But lieutenants do not know if he is loyal
  - Therefore run for f more rounds
- Disloyal general would:
  - Relay conflicting orders via disloyal lieutenants
  - Orders delivered to loyal lieutenants in last round
  - But protocol requires f+1 rounds, f+1 signatures
  - So orders relayed through at least one loyal lieutenant

80

80

Observations

- Complexity of protocol:
  - $O(N^2)$ messages on each round!
  - All Byzantine protocols are expensive
- Rabin: randomized protocols
  - Each process has a form of coin available to it
  - Can flip coin in each round
  - With randomness, very rapid agreement "with high probability" in very little time

81

81