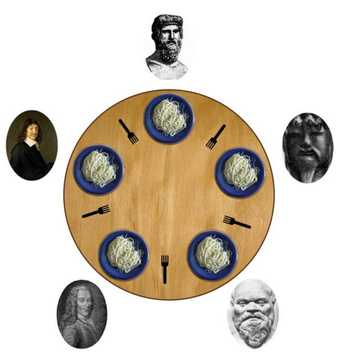
Microsoft Research TechFest 2011 the & in R&D

Nuggets of Randomness

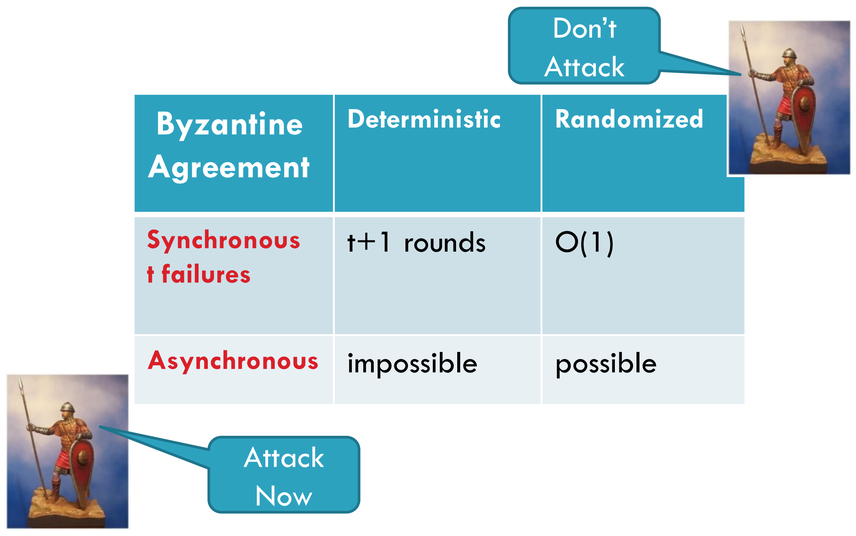
Cynthia Dwork, Omer Reingold (MSR-SVC,{dwork,omreing}@microsoft.com)

1 In Distributed Computing

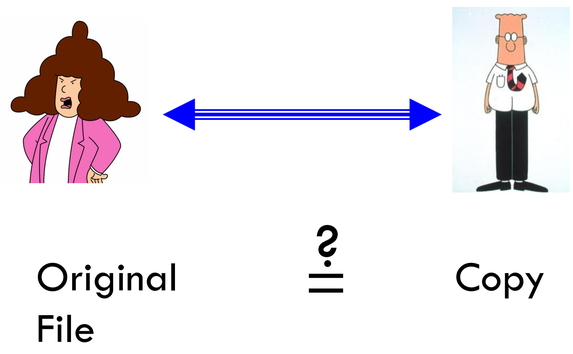
Dining Philosophers: breaking symmetry



Byzantine Agreement	Deterministic	Randomized
Synchronous t failures	t+1 rounds	O(1)
Asynchronous	impossible	possible



2 Randomness Saves Communication



- Deterministic: need to send the entire file!
- Randomness in the Sky: O(1) bits (or log in 1/error)
- Private Randomness: Logarithmic number of bits (*derandomization*).

3 In Cryptography

Private Keys: no randomness - no secrets and no identities

Encryption: two encryptions of same message with same key need to be different

Randomized (interactive) Proofs: Give rise to wonderful new notions: Zero-Knowledge, PCPs, …





4 Random Walks and Markov Chains

- When in doubt, flip a coin:
- Explore graph: minimal memory
- Page Rank: stationary distribution of Markov Chains
- Estimating size of Web
- Simulations of Physical Systems
- …

5 Shake Your Input

- Communication network (n-dimensional cube)

  Every deterministic routing scheme will incur exponentially busy links (in worse case)

  To send a message from x → y:
  select node z at random, send x → z → y.

  Now: O(1) expected load for every edge

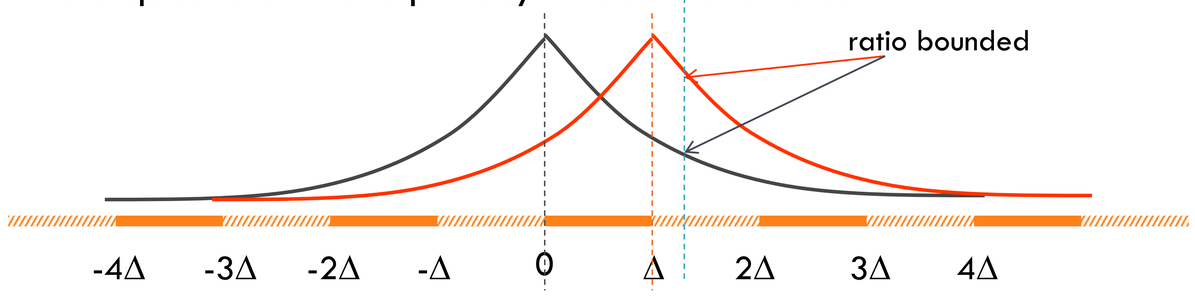


- Another example – randomized quicksort
- Smoothed Analysis: small perturbations, big impact

6 In Private Data Analysis

Hide Presence/Absence of Any Individual

How many people in the database have the BC1 gene?
Add random noise to true answer distributed as Lap(Δ/ε)
More questions? More privacy? Need more noise.



Booth 101 Demo 245

Microsoft Research

Microsoft