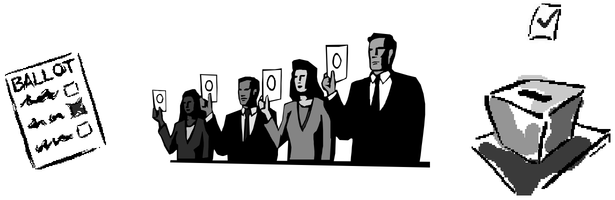
The Current State of Cryptographic Election Protocols

Josh Benaloh
Microsoft Research

So, you want to hold an election …

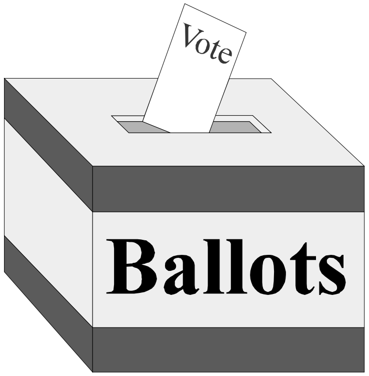


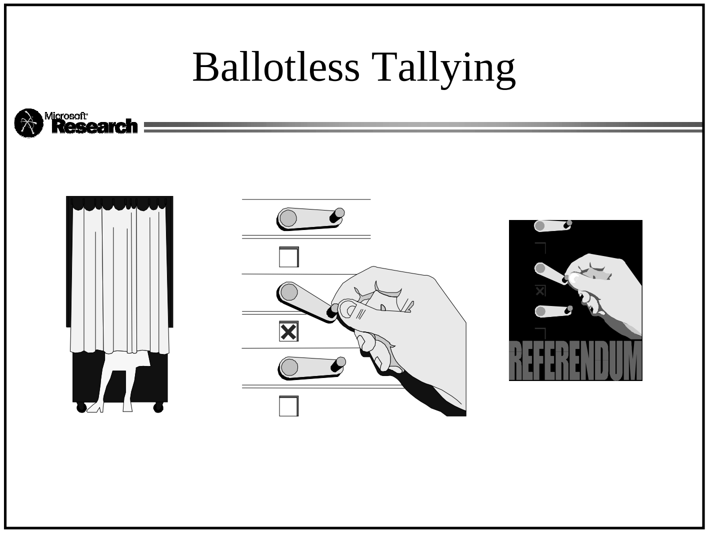
Fundamental Decision

You have essentially two paradigms to choose from …

- Anonymized Ballots
- Ballotless Tallying

Anonymized Ballots

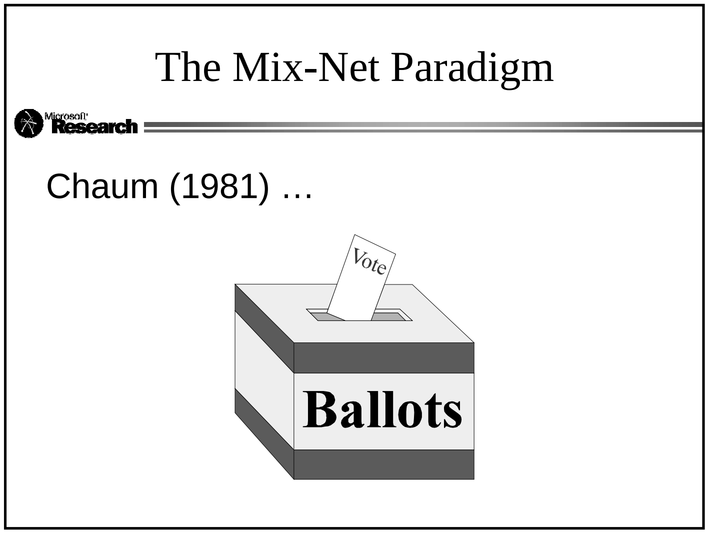




Ballotless Tallying

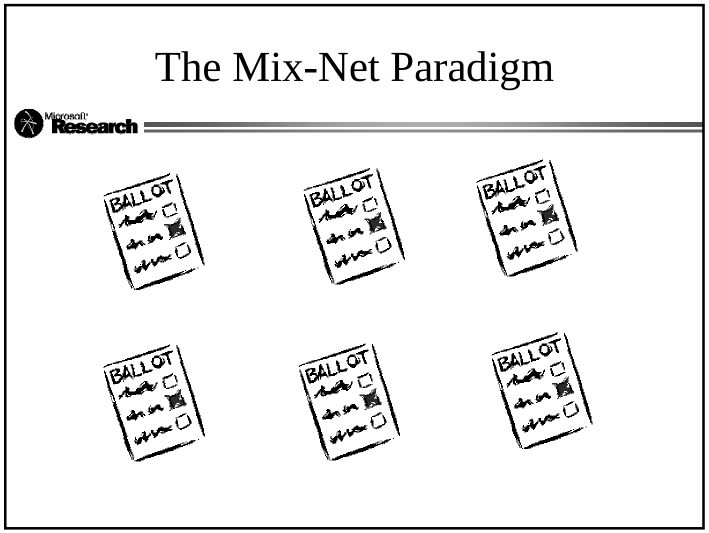
A Fundamental Trade-Off

- Ballots simplify write-ins and other “non-standard” options.
- Non-standard options can compromise privacy.

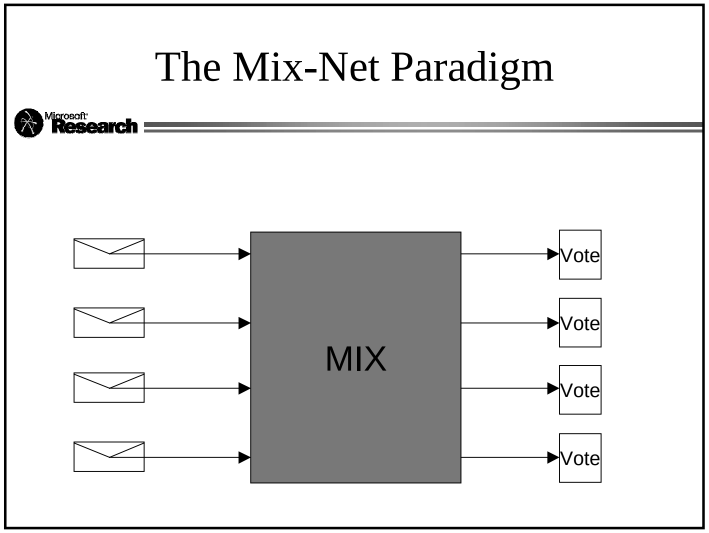


The Mix-Net Paradigm

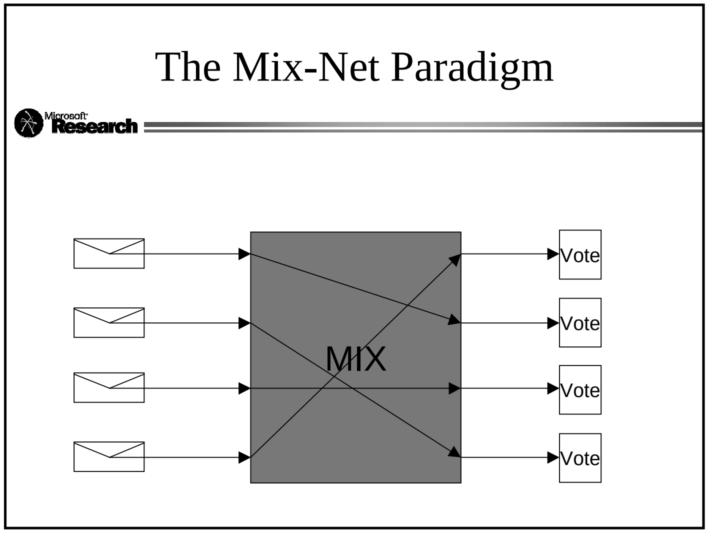
Chaum (1981) …



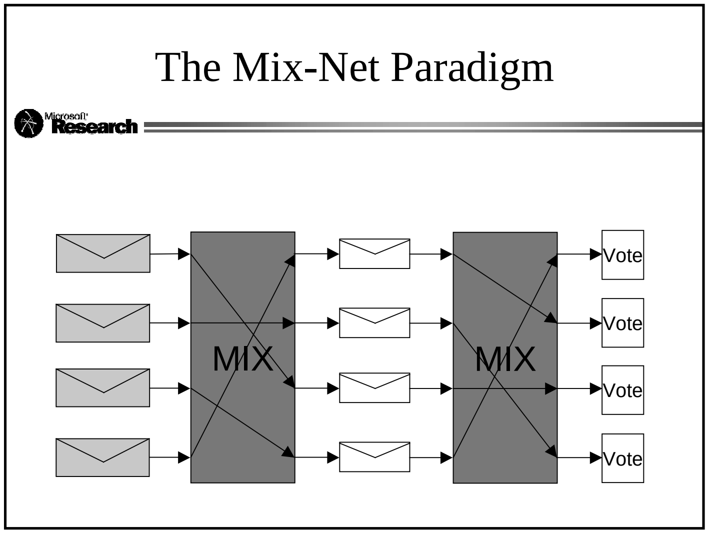
The Mix-Net Paradigm



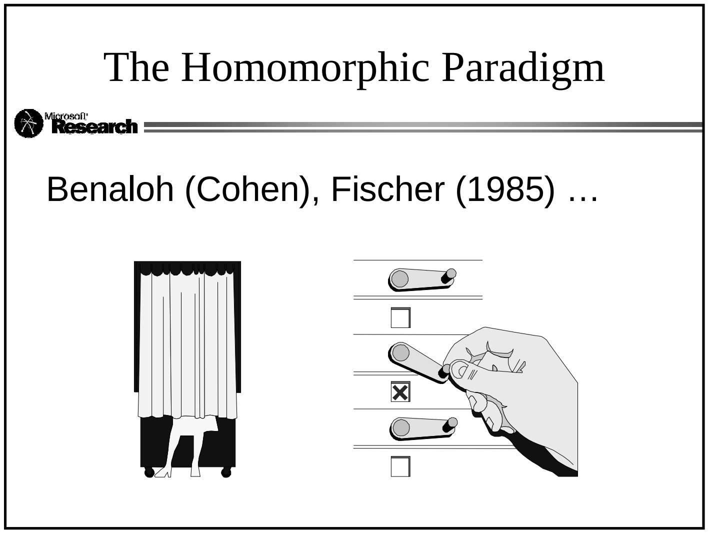
The Mix-Net Paradigm



The Mix-Net Paradigm

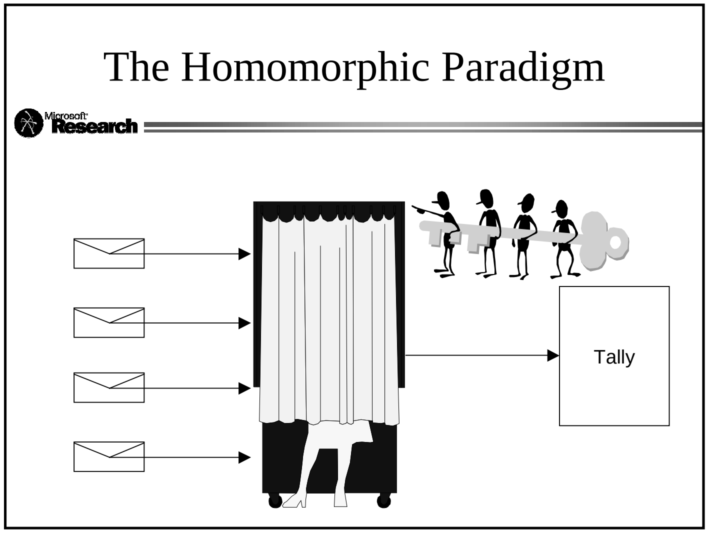


The Mix-Net Paradigm

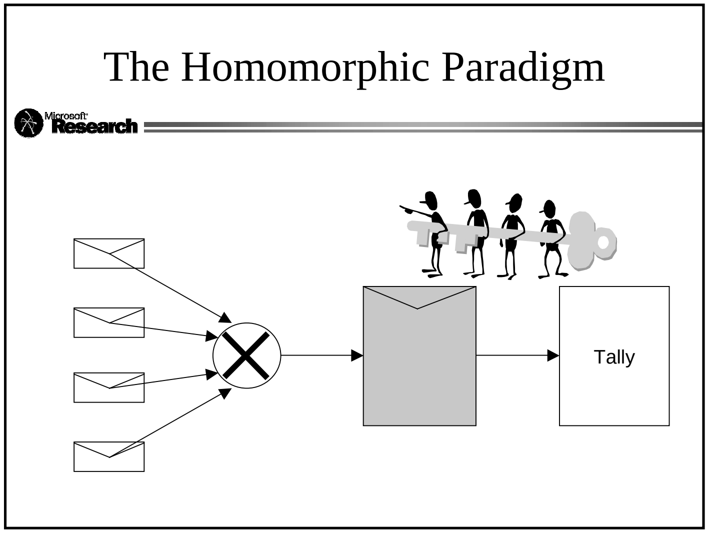


The Homomorphic Paradigm

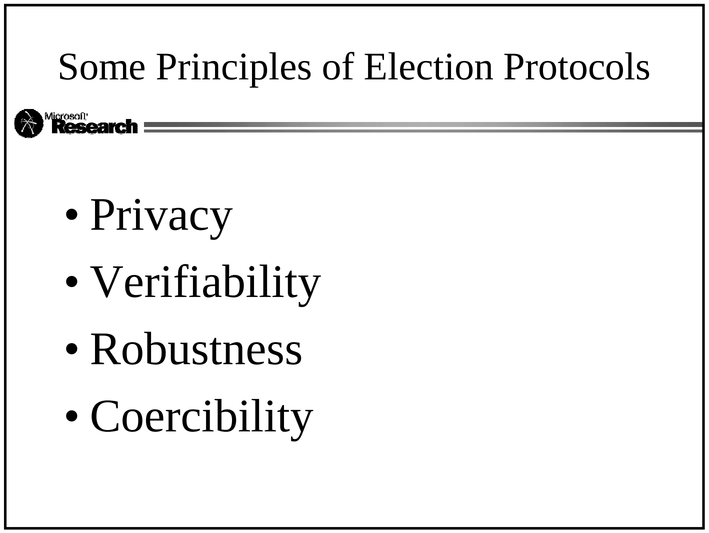
Benaloh (Cohen), Fischer (1985) …



The Homomorphic Paradigm

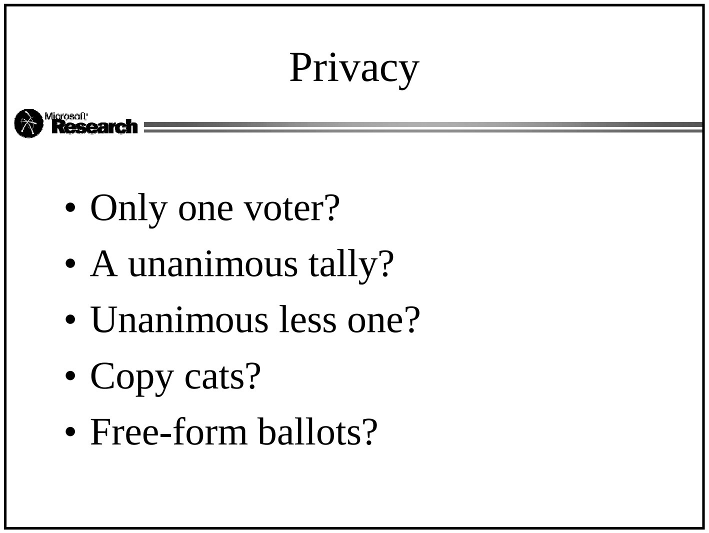


The Homomorphic Paradigm



Some Principles of Election Protocols

- Privacy
- Verifiability
- Robustness
- Coercibility



Privacy

- Only one voter?
- A unanimous tally?
- Unanimous less one?
- Copy cats?
- Free-form ballots?

Verifiability

- By single trusted party?
- By trusted committee?
- By each voter?
- By observers?

Robustness

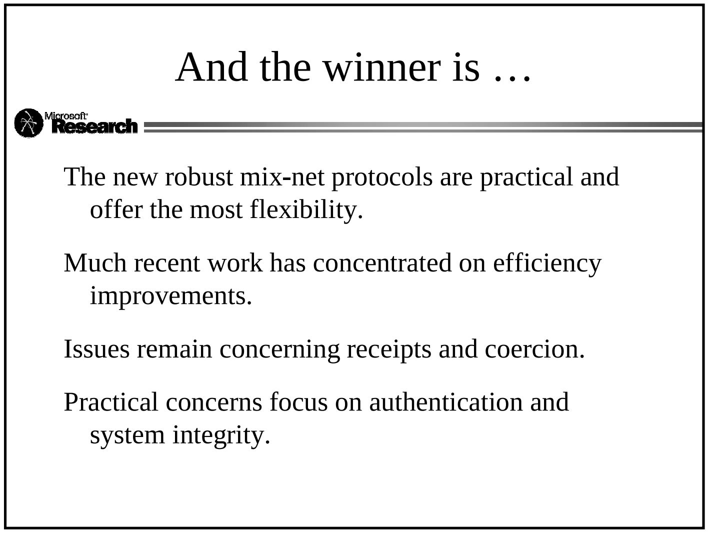
- Against faulty/malicious voter?
- Against faulty/malicious trustee?
- At what cost to privacy?

Coercibility

- Before the vote?
- During the vote?
- After the vote?
- By trustee, voter, or observer?
- Free-form ballots?

Some of the Authors

- Mix-Net: Chaum, Fujioka, Okamoto, Ohta, Pfitzmann, Waidner, Park, Itoh, Kurosawa, Michels, Horster, Sako, Kilian, Abe, Hirt, Jakobsson, Juels, Rivest, Furukawa, Neff, Golle, Zhong, Boneh
- Homomorphic: Benaloh, Fischer, Yung, Tuinstra, Sako, Kilian, Franklin, Cramer, Gennaro, Schoenmakers, Hirt, Kiayias



And the winner is …

The new robust mix-net protocols are practical and offer the most flexibility.

Much recent work has concentrated on efficiency improvements.

Issues remain concerning receipts and coercion.

Practical concerns focus on authentication and system integrity.