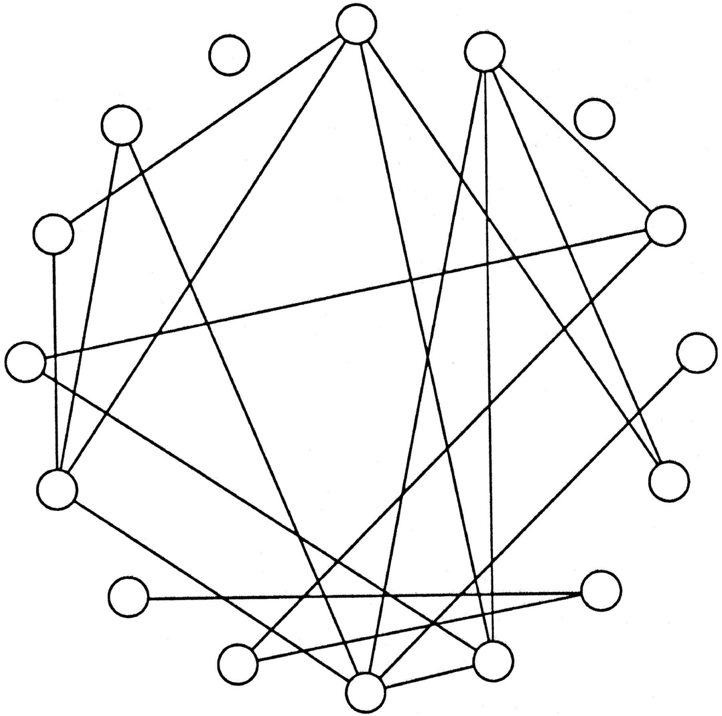
Communication Complexity of Byzantine Broadcast

Linda Chen
Mentor: Jun Wan

All-to-all Communication in Random Graphs

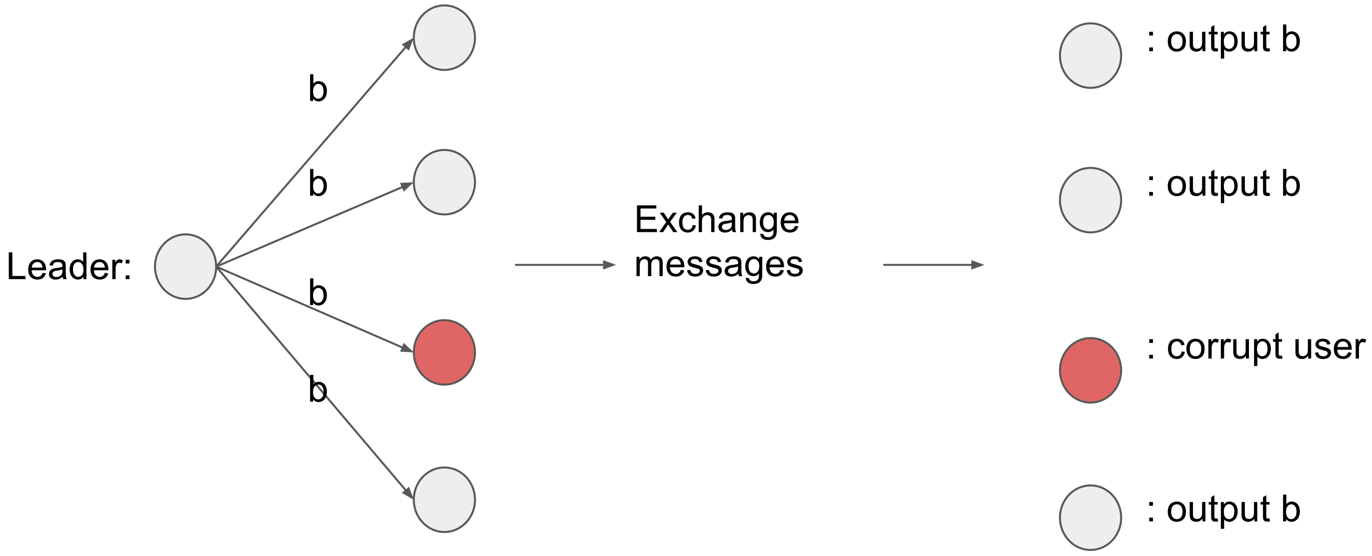
Analysis of:

- Round complexity
- Communication complexity



Byzantine Broadcast

- n users, f corrupted
- Honest users must agree on b



Properties of Byzantine Broadcast

Consistency: all honest users agree

Validity: if the leader is honest, all honest users output the leader's bit

Liveness: all honest users will eventually terminate

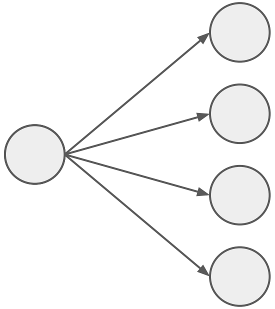
Round Complexity of Byzantine Broadcast

For each epoch:

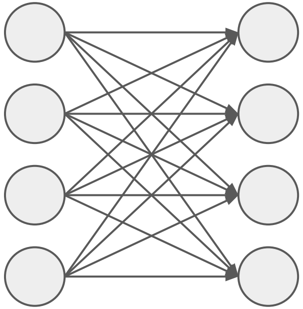
- **Propose (d-1 rounds)**: leader sends input bit to other users
- **Vote (d-1 rounds)**: users exchange their proposed bit
- **Commit (d rounds)**: if a user received enough votes, output the proposed bit and exchange commit messages

Terminate: if a user receives enough commit messages, terminate

Communication Complexity of Byzantine Broadcast



$O(n)$

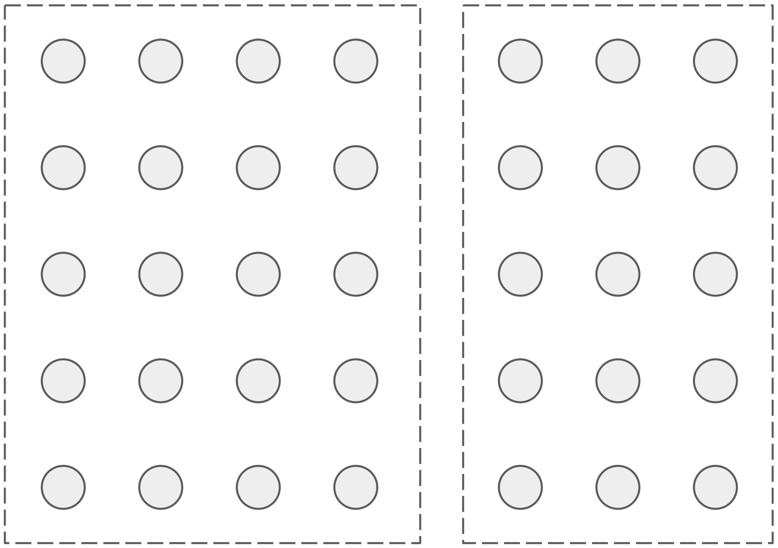


$O(n^2)$

Previous work: $O(n^2)$ lower bound

Our goal: $O(n^3)$ lower bound for dishonest majority

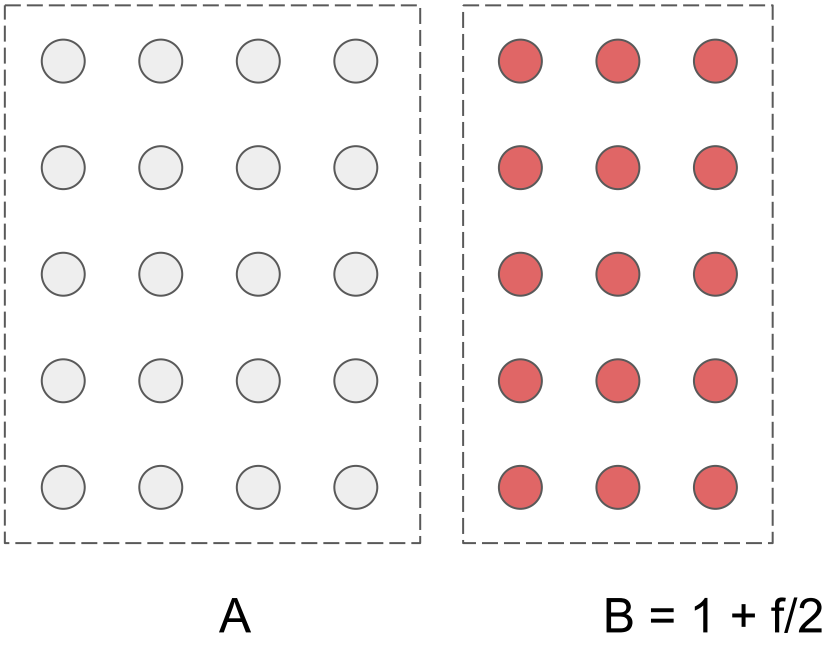
Dolev and Reischuk: $O(n^2)$ lower bound



A

B = 1 + f/2

Scenario 1

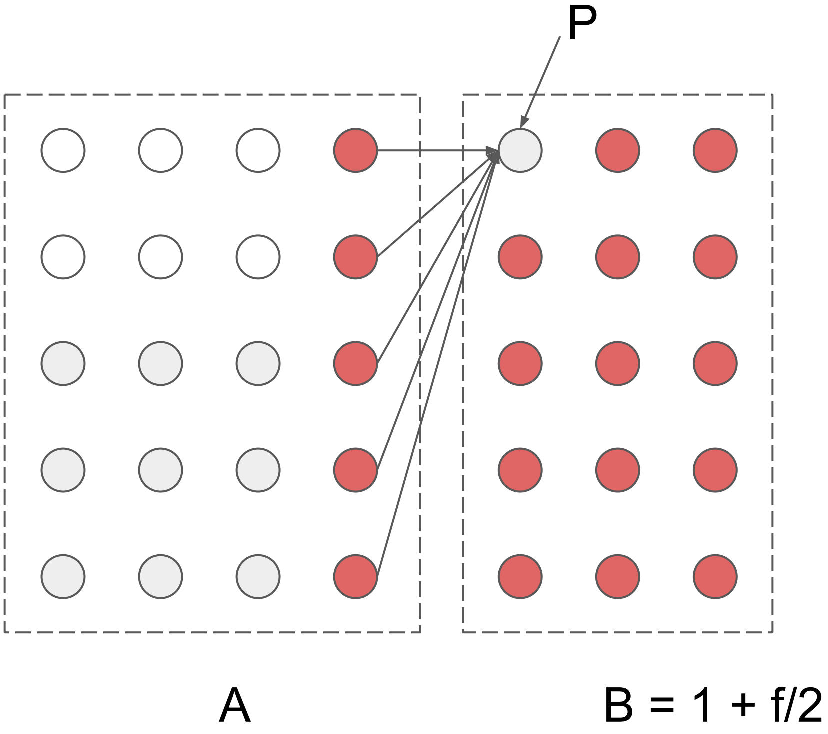


Adversary corrupts B

All users in B:

- Ignore first f/2 messages from A
- Do not send messages to each other

Scenario 2



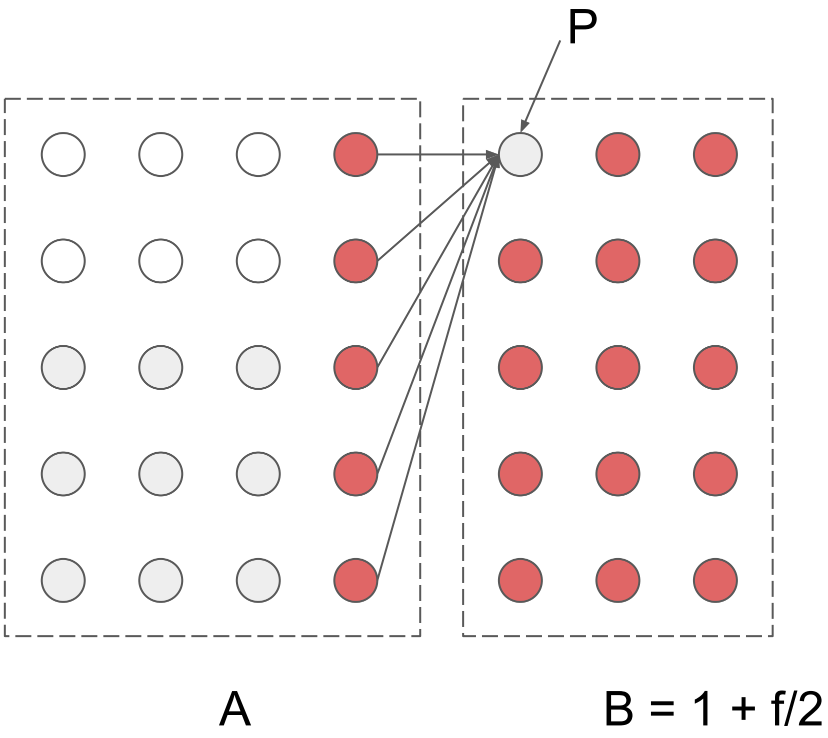
Adversary corrupts:

- All users in B except P
- All users in A that send to P

Communication complexity $<(f/2)^2$:

- $P \in B$ receives $<(f/2)$ messages

Scenario 2



Honest users in A:

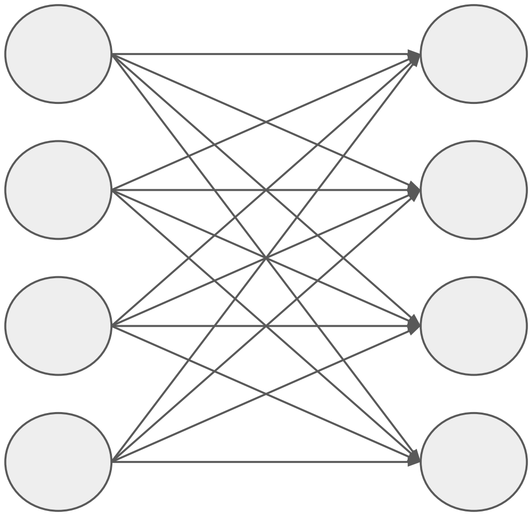
- Same as scenario 1
- Will commit on leader's bit

P:

- Receives no messages
- May commit on different bit

Possible $O(n^3)$ CC

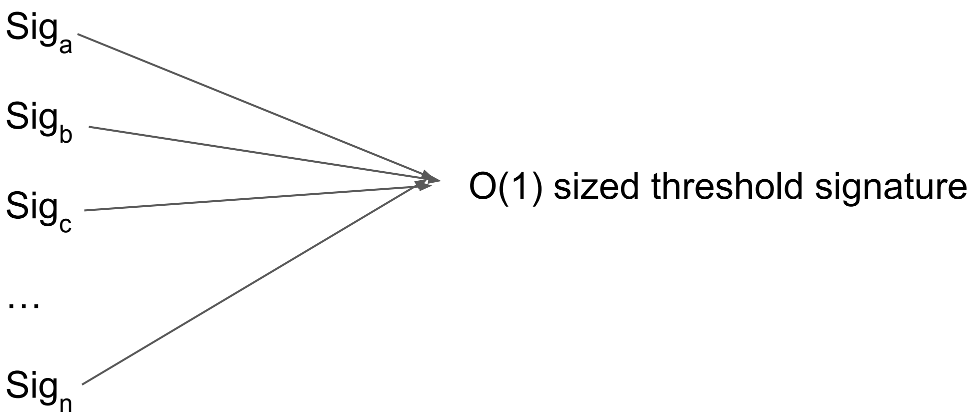
- O(n) users need to relay O(n) messages to O(n) other users



Each edge = O(n) size

Momose and Ren: $O(n^2)$ for Honest Majority

- **Threshold signatures**: combine multiple messages into a single message
- O(n) users send O(1) sized messages to O(n) users



Momose and Ren: $O(n^2)$ for Honest Majority

Without threshold signatures:

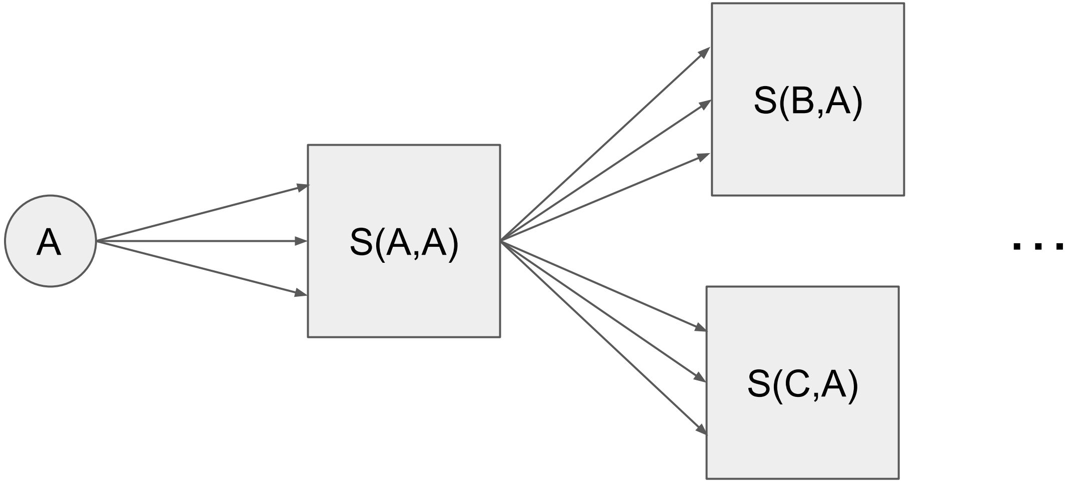
- Requires $f \leq (\frac{1}{2} - \varepsilon)n$
- **Expander graph** where any set of $2\varepsilon n$ users is connected to at least $(1-2\varepsilon)n$ users, where *degree is constant*
- $O(n)$ users propagate $O(n)$ sized messages to $O(1)$ users

Our Goal: $O(n^3)$ lower bound for dishonest majority

Method 1

A’s relay graph G_A:

S(i, A) = set of users that received A’s vote from i



Method 1

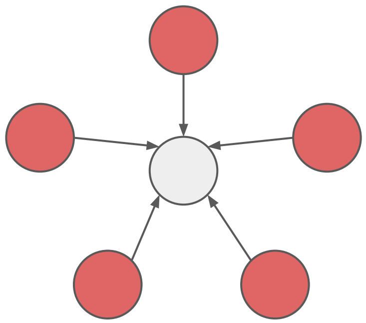
$\sum_i$ (# of edges in G_i) = communication complexity

If communication complexity = $O(n^{3-\varepsilon})$

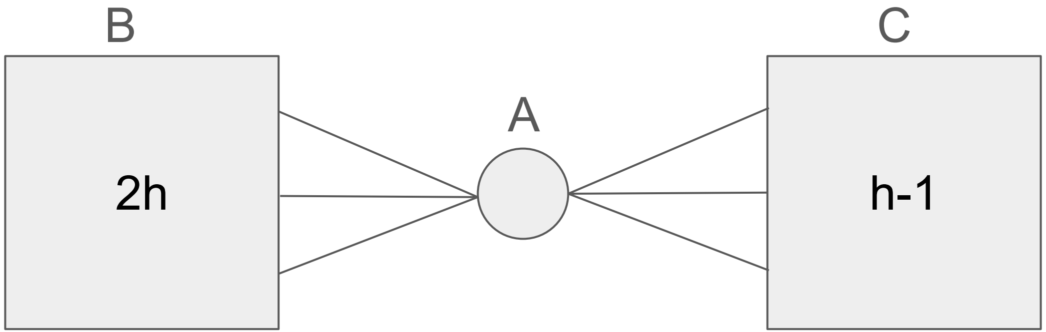
⇒ G_A has less than $n^{2-\varepsilon}$ edges

⇒ average degree = $n^{1-\varepsilon}$

⇒ $f / n^{1-\varepsilon} = n^{\varepsilon}$ don't receive A's vote



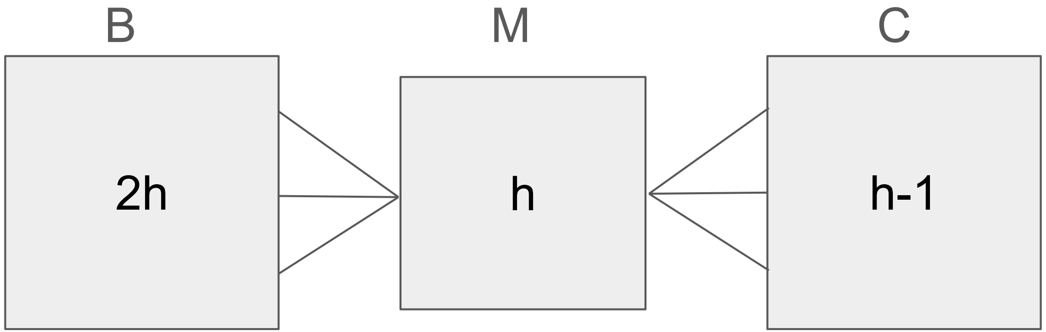
Method 2



A must relay at least O(n) votes from C to at least O(n) users in B

A has $O(n^2)$ communication complexity

Method 2



Users in M do not know how many users are in M

Every user in M: $O(n^2)$ communication complexity

Total: $O(n^3)$ communication complexity

Acknowledgments

- Mentor: Jun Wan
- MIT PRIMES program

Thank you for listening!