Expected Constant Round Byzantine Broadcast under Dishonest Majority

Jun Wan (junwan@mit.edu)
Hanshen Xiao (hsxiao@mit.edu)
Elaine Shi (runting@gmail.com)
Srini Devadas (devadas@csail.mit.edu)

Byzantine Broadcast [Lamport et al. 82]

- A set of users aim to reach consensus, one of them is the designated sender.
- The sender is given an input bit $b \in \{0, 1\}$
  - *Consistency*: all honest users must output the same bit; and
  - *Validity*: all honest users output the sender's input bit if the sender is honest.

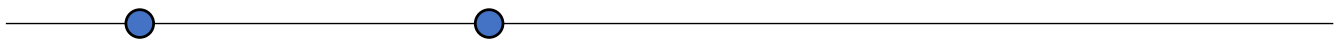
Background and Previous Work

- Synchronous, assume trusted cryptographic setup
- [Dolev and Strong, 83]: no deterministic protocol can achieve Byzantine Broadcast within $f + 1$ rounds, where f is the number of corrupted users.
- Focus on randomized protocols

Previous work

- Honest majority: expected constant rounds protocols exist (even under adaptive adversary) [Katz and Koo 09, Abraham et al. 19].
- Dishonest majority:

Garay et al., 07	*Fitz et al. 09*
$O((2f-n)^2)$	$O((2f-n))$

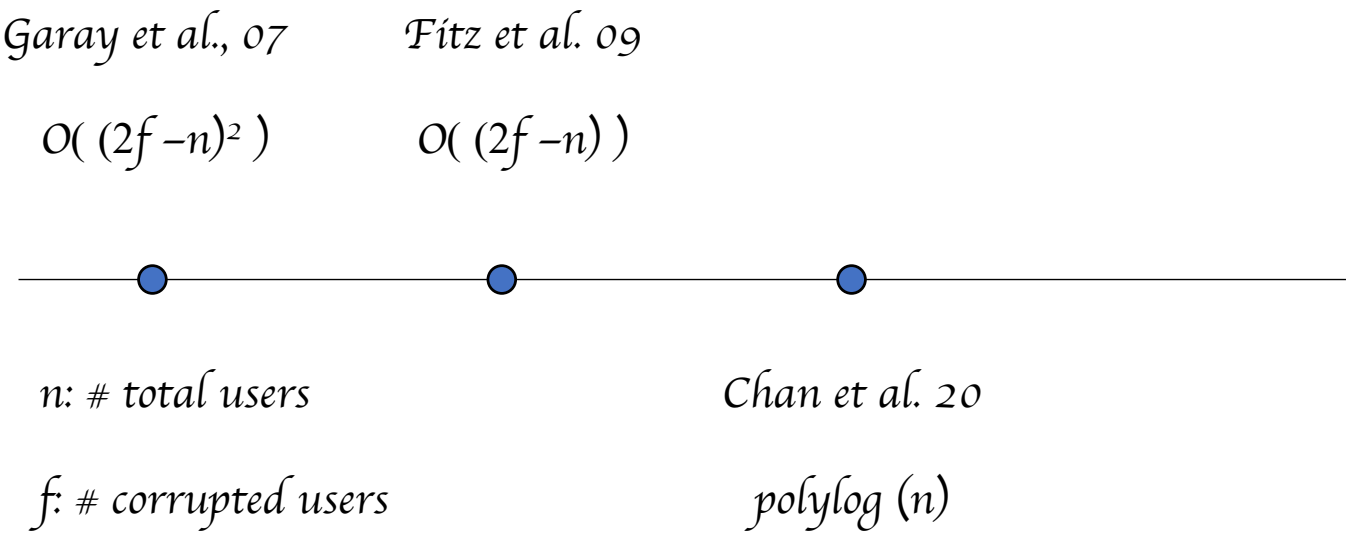


n: # total users

f: # corrupted users

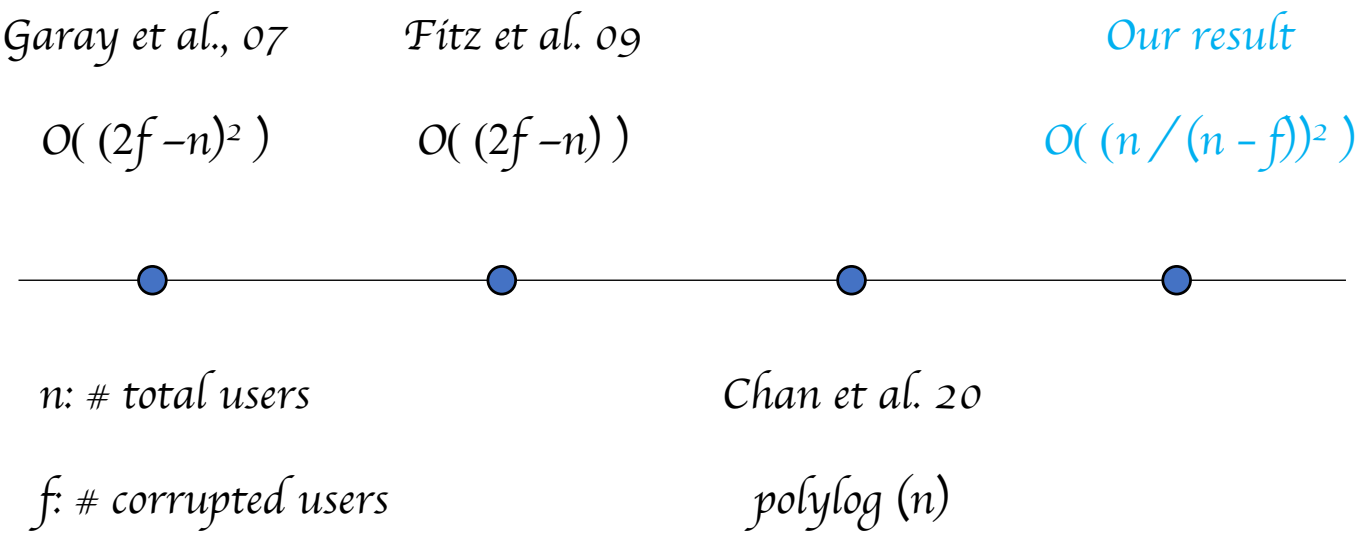
Previous work

- Honest majority: expected constant rounds protocols exist (even under adaptive adversary) [Katz and Koo 09, Abraham et al. 19].
- Dishonest majority:



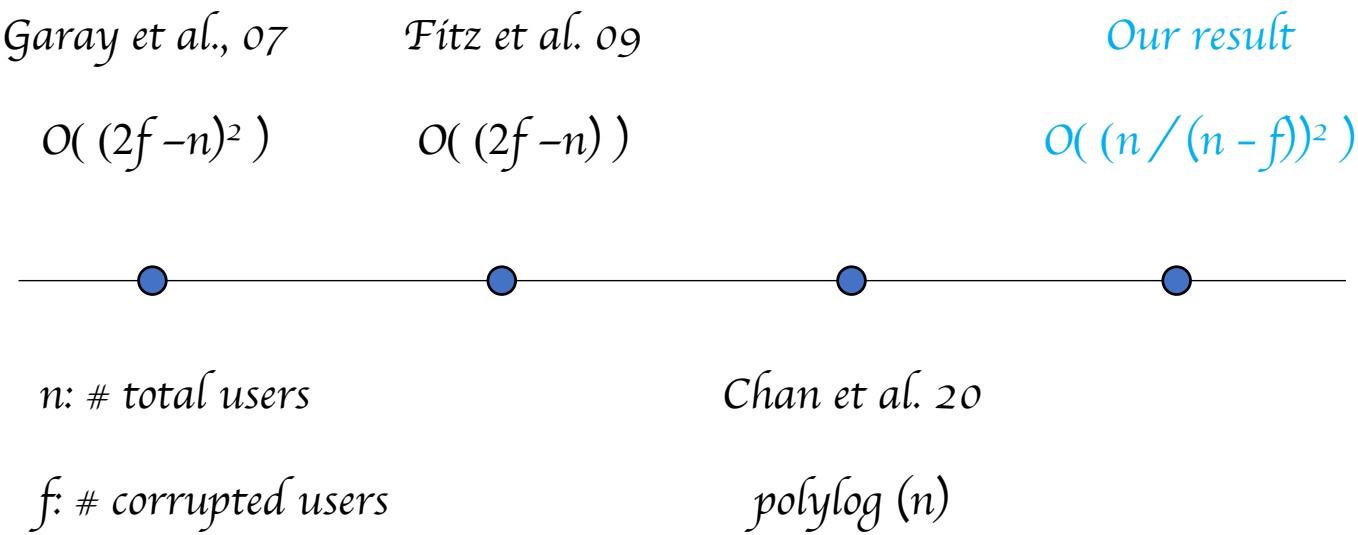
Previous work

- Honest majority: expected constant rounds protocols exist (even under adaptive adversary) [Katz and Koo 09, Abraham et al. 19].
- Dishonest majority: can we also achieve expected constant round complexity?



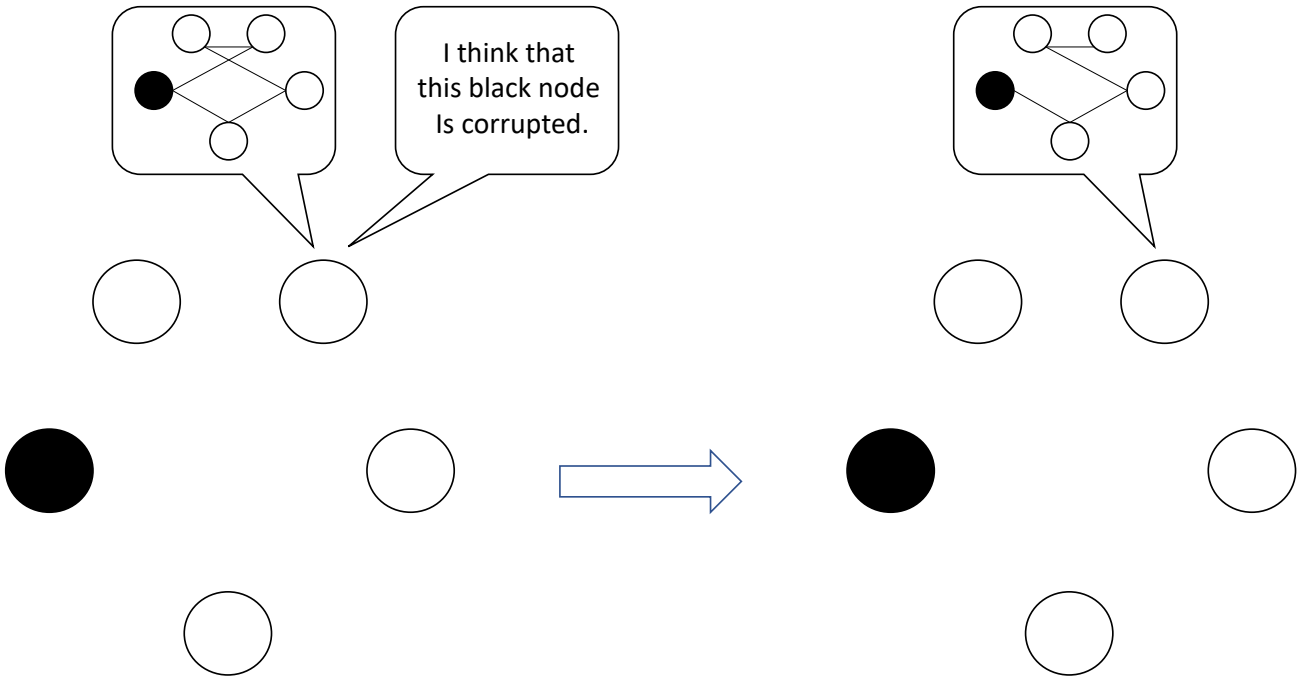
Our results

- Round complexity: $\Theta((n/(n-f))^2)$.
- Tolerates adaptive adversary: cannot erase messages already sent upon corrupting the user



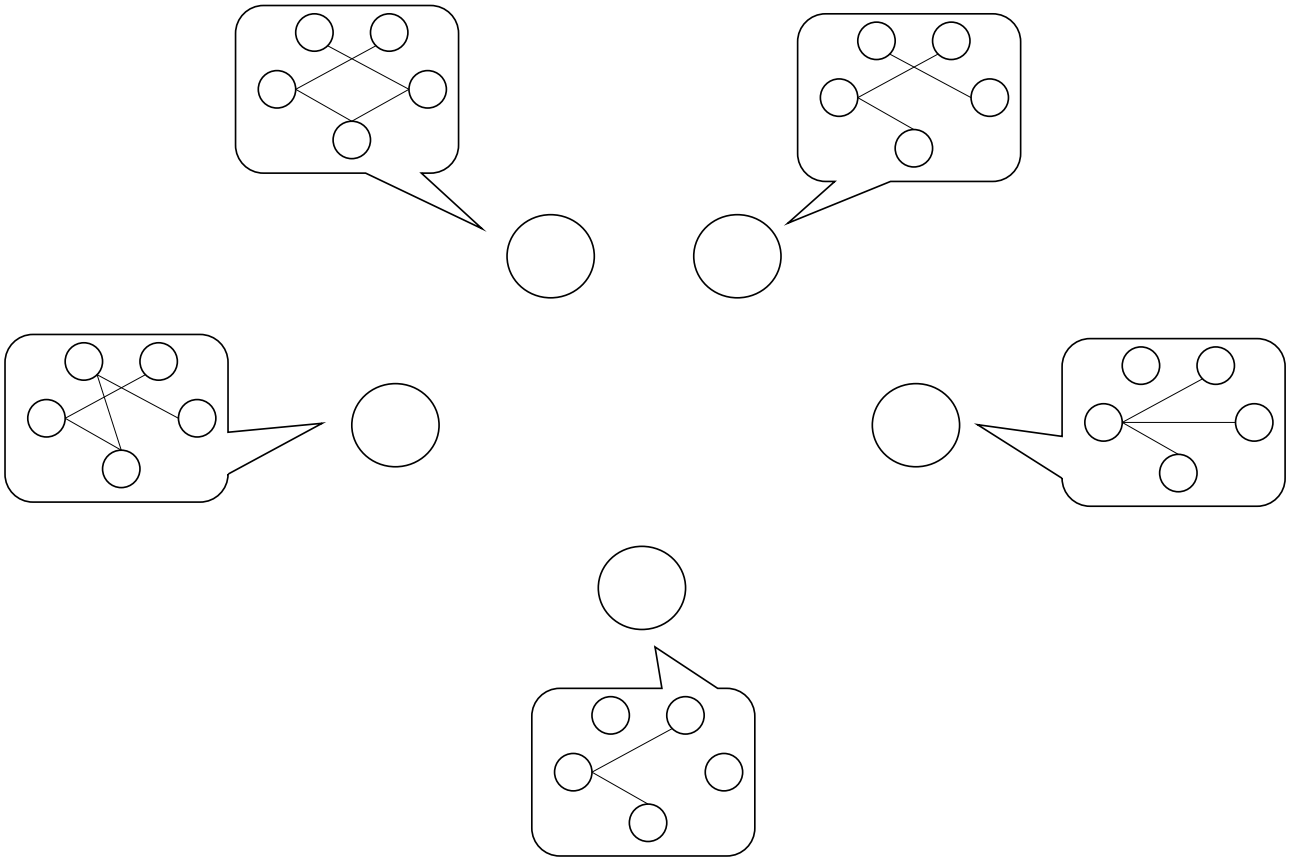
Novelty and new techniques

- Use a new graph idea: the trust graph.



Novelty and new techniques

- Use a new graph idea: the trust graph.



Novelty and new techniques

- Use a new graph idea: the trust graph.
- Build a new primitive and bootstrap full consensus from this weaker primitive, similar to gradecast.

Thank you

- Future work: strongly adaptive adversary
- See details of the paper on Eprint