From Few to Many Faults

A. Constantinescu, M. Dufay, **A. Paramonov**, R. Wattenhofer

ETH zürich

Plan

- Problem definition
  - Consensus on its own (binary, strong validity)
  - Three major time models
- Message complexity
  - Dolev-Reischuk
  - Optimistic
  - Decouple n and t
- Results
  - Optimal in synchrony
  - Optimal in partial synchrony
  - Almost optimal in asynchrony
- Technical highlights
  - Expanders!!!

Consensus

- *n* parties, up to *t* malicious

Consensus

- *n* parties, up to *t* malicious
- Parties propose 0 or 1

Consensus

- *n* parties, up to *t* malicious
- Parties propose 0 or 1
- Strong validity: If all honest parties propose *v,* then *v* must be decided

Consensus

- *n* parties, up to *t* malicious
- Parties propose 0 or 1
- Strong validity: If all honest parties propose *v,* then *v* must be decided

Synchrony	Partial Synchrony	Asynchrony
Δ	Δ after GST	eventually

Communication complexity

- Dolev-Reischuk[1]: $\Omega(n^2)$

[1] Dolev, D., & Reischuk, R. (1985). Bounds on information exchange for Byzantine agreement. Journal of the ACM (JACM), 32(1), 191-204.

Communication complexity

- Dolev-Reischuk[1]: $\Omega(n^2)$
- But in fact…
  $\Omega(f^2)$! f - the actual number of faults in a given run

[1] Dolev, D., & Reischuk, R. (1985). Bounds on information exchange for Byzantine agreement. Journal of the ACM (JACM), 32(1), 191-204.

Communication complexity

- Dolev-Reischuk[1]: $\Omega(n^2)$
- But in fact…
  $\Omega(f^2)$! f - the actual number of faults in a given run

Common: f = t = n/3

[1] Dolev, D., & Reischuk, R. (1985). Bounds on information exchange for Byzantine agreement. Journal of the ACM (JACM), 32(1), 191-204.

Communication complexity

- Dolev-Reischuk[1]: $\Omega(n^2)$
- But in fact…
  $\Omega(f^2)$! f - the actual number of faults in a given run

Common: $f = t = n/3$

This work: $f \ll t \ll n/3$

[1] Dolev, D., & Reischuk, R. (1985). Bounds on information exchange for Byzantine agreement. Journal of the ACM (JACM), 32(1), 191-204.

Why consider algorithms for $t \ll n/3$?

System A: $t = 1000$, $n = 3001$

System B: $t = 1000$, $n = 10{,}000$

Why consider algorithms for $t \ll n/3$?

System A: t = 1000, n = 3001

System B: t = 1000, n = 10,000

$$n^2 = 100t^2$$

Results

	Communication	**Resilience**
	Synchrony	
This paper	$\mathcal{O}(n + tf)$	$t < \frac{n}{2}$
Spiegelman et al. [2]	$\Omega(n + tf)$	Any

[2] Spiegelman, A. (2020). In search for an optimal authenticated byzantine agreement. arXiv preprint arXiv:2002.06993.

Results

	Communication	**Resilience**
Synchrony		
This paper	$\mathcal{O}(n + tf)$	$t < \frac{n}{2}$
Spiegelman et al. [2]	$\Omega(n + tf)$	Any
Partial Synchrony		
This paper	$\mathcal{O}(n + t \cdot f)$	$t < n/3$

[2] Spiegelman, A. (2020). In search for an optimal authenticated byzantine agreement. arXiv preprint arXiv:2002.06993.

Results

	Communication	Resilience
Synchrony		
This paper	$\mathcal{O}(n + tf)$	$t < \frac{n}{2}$
Spiegelman et al. [2]	$\Omega(n + tf)$	Any
Partial Synchrony		
This paper	$\mathcal{O}(n + t \cdot f)$	$t < n/3$
Asynchrony		
This paper	$\mathbb{E}(\mathcal{O}((n + t^2) \cdot \log n))$	$t < n/3$
This paper	$\mathbb{E}(\Omega(n + t^2))$	Any

[2] Spiegelman, A. (2020). In search for an optimal authenticated byzantine agreement. arXiv preprint arXiv:2002.06993.

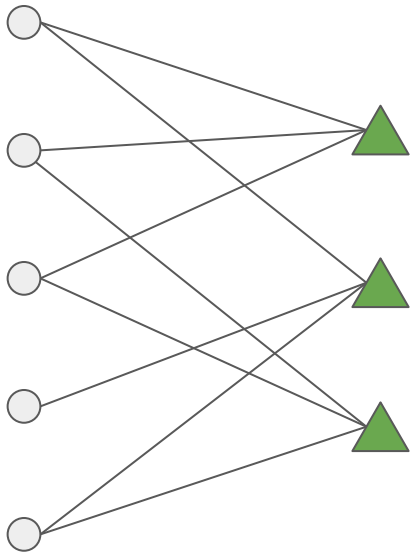
Technical Highlight

Bipartite Expander

Parties Committees

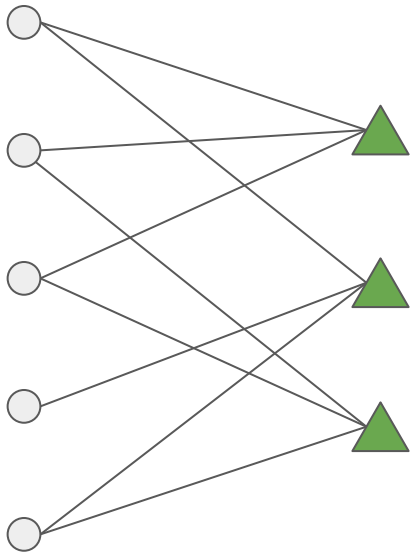
Bipartite Expander

Parties Committees



Bipartite Expander

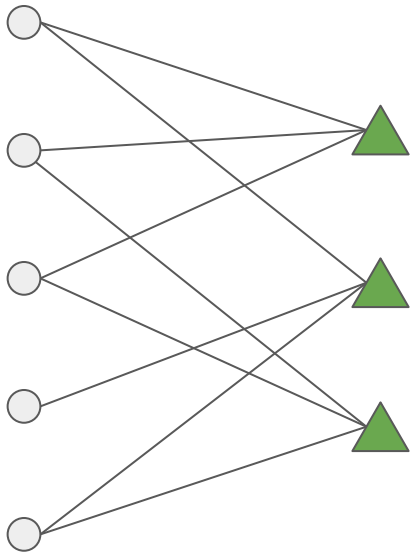
Parties Committees



1. Few committees

Bipartite Expander

Parties Committees

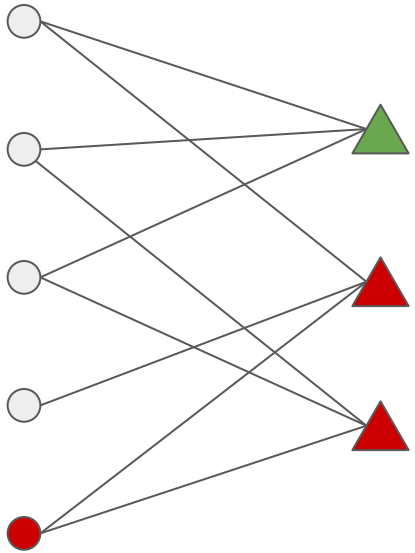


1. Few committees

2. One partie in a tiny fraction of committees

Bipartite Expander

Parties Committees



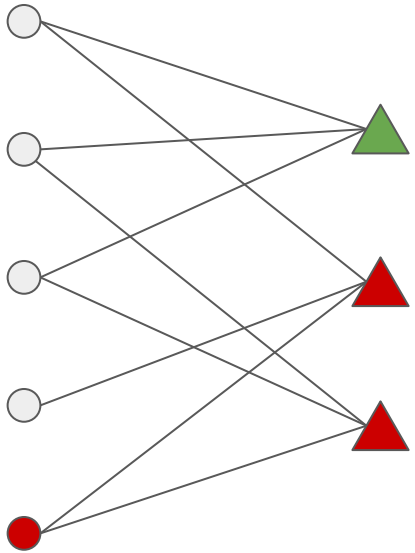
1. Few committees

2. One partie in a tiny fraction of committees

Committee is compromised if it
has at least *1* byzantine.

Bipartite Expander

Parties Committees



1. Few committees

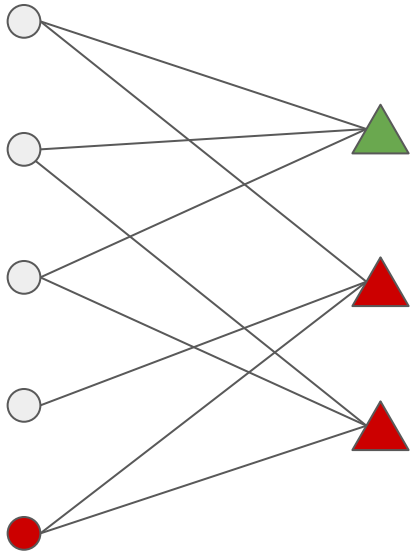
2. One partie in a tiny fraction of committees

Committee is compromised if it
has at least *1* byzantine.

3. Most of the honest parties belong to a non-compromised committee

Bipartite Expander

Parties Committees



Thank you!

1. Few committees

2. One partie in a tiny fraction of committees

Committee is compromised if it has at least *1* byzantine.

3. Most of the honest parties belong to a non-compromised committee