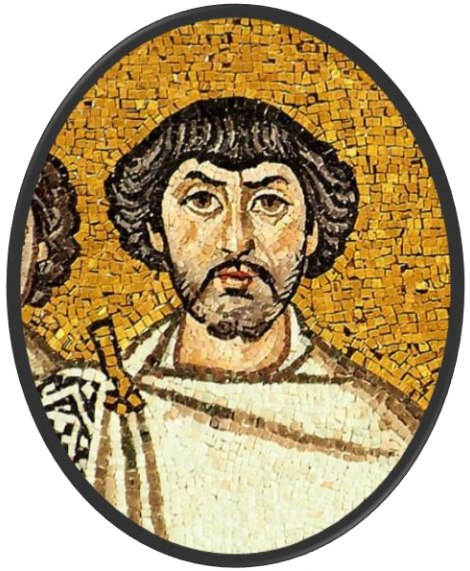
On the Round Complexity of Randomized Byzantine Agreement

Ran Cohen, Iftach Haitner, **Nikolaos Makriyannis**,
Matan Orland & Alex Samorodnitsky



To appear in DISC'19

Technion
Israel Institute of Technology

Randomized BA & Problem Statement

- Each P_i holds input $v_i \in \{0,1\}$.
- Agreement: All honest parties output the same bit.
- Validity: $\exists\ i$ s.t. (honest) P_i outputs v_i.

We prove bounds on the halting probability after 1 or 2 rounds.

Randomized BA & Problem Statement

- Each P_i holds input $v_i \in \{0,1\}$.
- Agreement: All honest parties output the same bit.
- Validity: $\exists\ i$ s.t. (honest) P_i outputs v_i.

We prove bounds on the halting probability after 1 or 2 rounds.

Micali's BA (ITCS'17) halts after 3 rounds with constant probability.

We Show

BA Protocol Security Threshold	Halting Probability in round 1	Halting Probability in round 2
$n/3$	$o(1)$	$1 - \Theta(1)$
$n/4$	$1/2 + o(1)$	$1 - \Theta(1)$

We Show

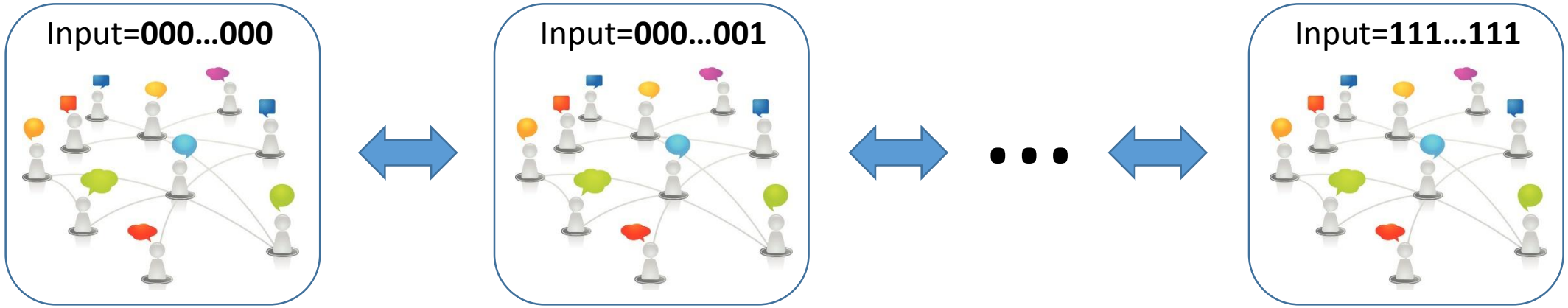
BA Protocol Security Threshold	Halting Probability in round 1	Halting Probability in round 2
$n/3$	$o(1)$	$1 - \Theta(1)$
$n/4$	$1/2 + o(1)$	$1 - \Theta(1)$

For *all** BA protocols and under plausible combinatorial assumption:

BA Protocol Security Threshold	Halting Probability in round 2
$n/3$	$o(1)$
$n/4$	$1/2 + o(1)$

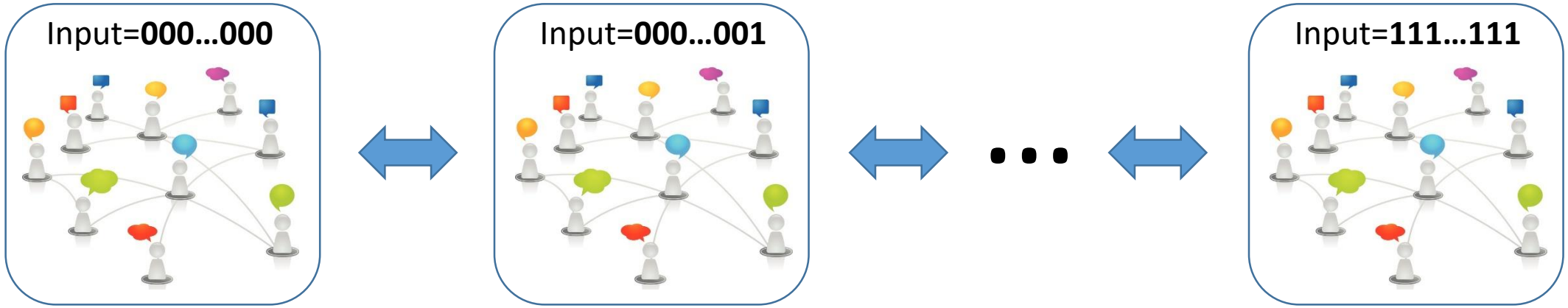
Our Technique

- We follow the classic blueprint for deterministic protocols:



Our Technique

- We follow the classic blueprint for deterministic protocols:



- **However**, for randomized protocols, the above chain fails.

The randomness can be used to distinguish adjacent executions.

Our Technique (cont’d)

- Solution:

  Abort (certain) parties to uncouple randomness from output.

Our Technique (cont'd)

- Solution:

  Abort (certain) parties to uncouple randomness from output.

- Our attack gives rise to an isoperimetric-type inequality.

Unrealistic cases reduce to KKL & Friedgut's junta theorem.

General case is left as open problem.

Thank You!

Available on eprint & arXiv:

https://eprint.iacr.org/2019/868

https://arxiv.org/abs/1907.11329