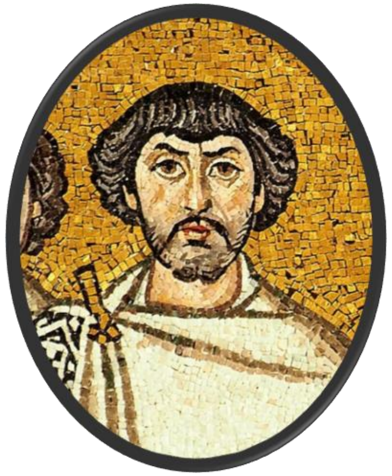
On the Round Complexity of Randomized Byzantine Agreement

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

DISC'2019



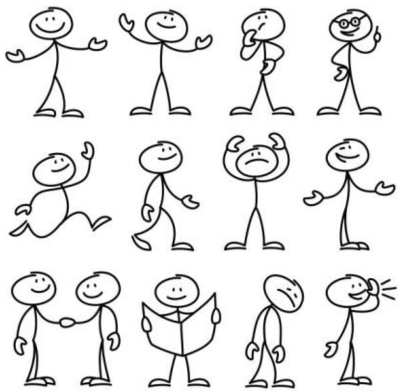
TECHNION
Israel Institute
of Technology

TEL AVIV UNIVERSITY

Definition of Byzantine Agreement (BA)

[Pease-Lamport-Shostak'80, Lamport-Shostak-Pease'82]

- 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.



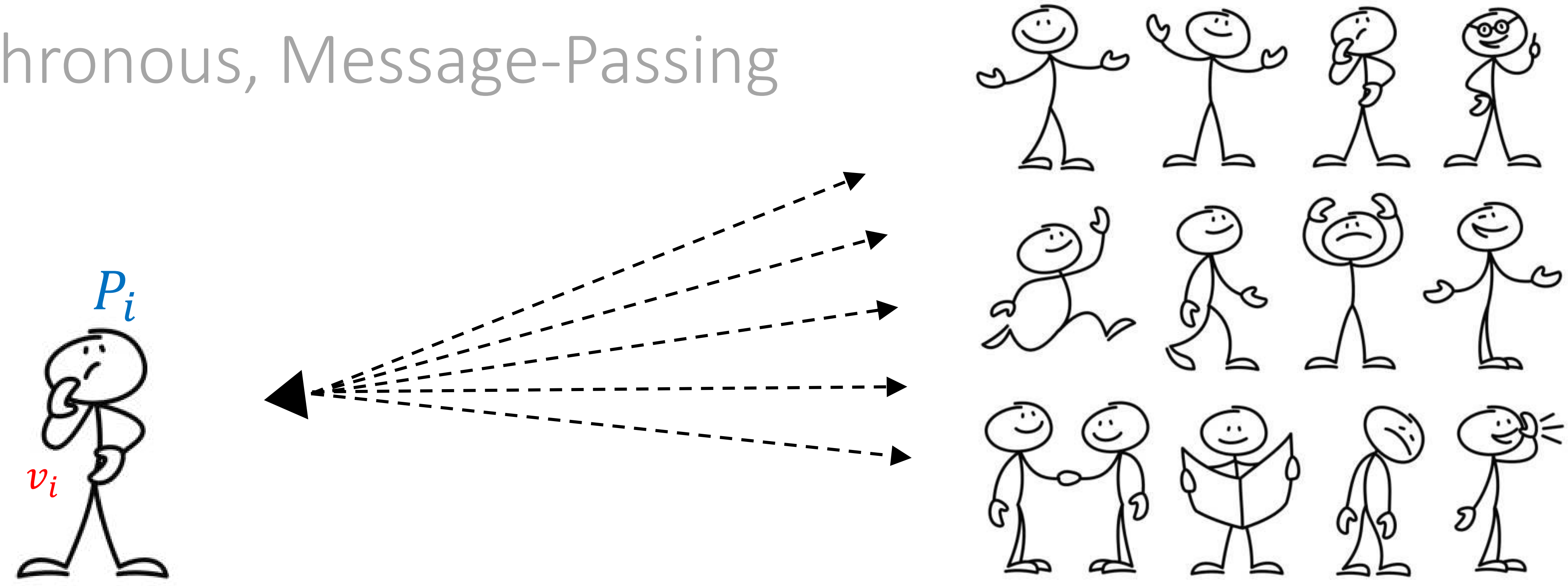
BA is very closely related to **Broadcast**

Sender sends a message to many receivers s.t. all receivers agree on the message

- ➢ Fault-tolerant distributed systems
- ➢ Cryptography (Multi-Party Computation)
- ➢ Blockchain (Cryptocurrencies)

Model

Synchronous, Message-Passing



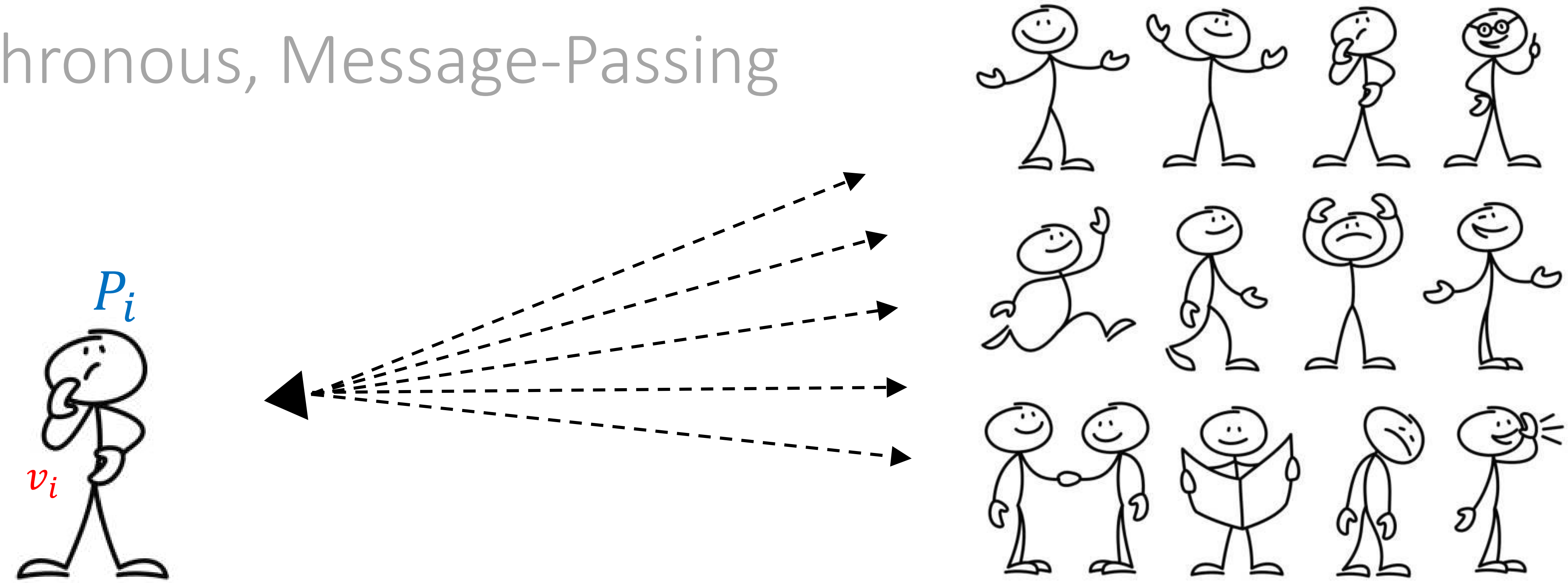
- Parties are connected in a point-to-point network with *synchronous rounds*.

  Round := every party sending a message to all other parties.

- Allow Setup (e.g. Digital signatures, PKI).

Model

Synchronous, Message-Passing



Problem Statement:

What is the minimal number of (expected) rounds needed to reach Byzantine Agreement?

When facing t-out-of-n corrupted players.

Previous Results

Synchronous, Message-Passing

t = security threshold

Deterministic protocols:

- $\#\text{Rounds} = t + 1$ [Lamport-Shostak-Pease’82 , Dolev-Strong’83, Garay-Moses’93]
- $\#\text{Rounds} \geq t + 1$ [Fischer-Lynch’82, Dolev-Strong’83]

Randomized protocols:

- Constant-round impossibility
  [Chor-Merritt-Shmoys’85, Karlin-Yao’84]
- Expected constant-round BA
  [BenOr’83, Rabin’83, Feldman-Micali’88, Katz-Koo’06, Micali’17]
  [Micali-Vaikuntanathan’17, Abraham-Devadas-Dolev-Nayak-Ren’18]
  [Abraham-Chan-Dolev-Nayak-Pass-Ren-Shi’19]

Our Work

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

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

We Show

For every BA resilient against $t = n/3$ corruptions

Halting Probability in round 1	Halting Probability in round 2
$o(1) \approx 0$	$1 - \Theta(1) \ll 1$

Under plausible combinatorial assumption:

Halting Probability in round 2
$o(1) \approx 0$

Outline

1. Adversarial Model
   Local Consistent Adversaries
2. Our Attack(s)
   i. 1^{st} round halting
   ii. 2^{nd} round halting

Adversarial Model

Adversarial Model

Locally Consistent Adversaries

- Efficient (PPTM) limited to the following adversarial behavior
  i. Adversary corrupts a subset of parties
  ii. Corrupted parties may send conflicting inputs to honest parties
  iii. Adversary may abort (some corrupted parties) at any given round

Adversary may **not**
- Manipulate randomness
- Lie about (honest) incoming messages

Adversarial Model

Locally Consistent Adversaries

- Efficient (PPTM) limited to the following adversarial behavior
  i. Adversary corrupts a subset of parties
  ii. Corrupted parties may send conflicting inputs to honest parties
  iii. Adversary may abort (some corrupted parties) at any given round
- We show lower bounds via locally consistent attacks

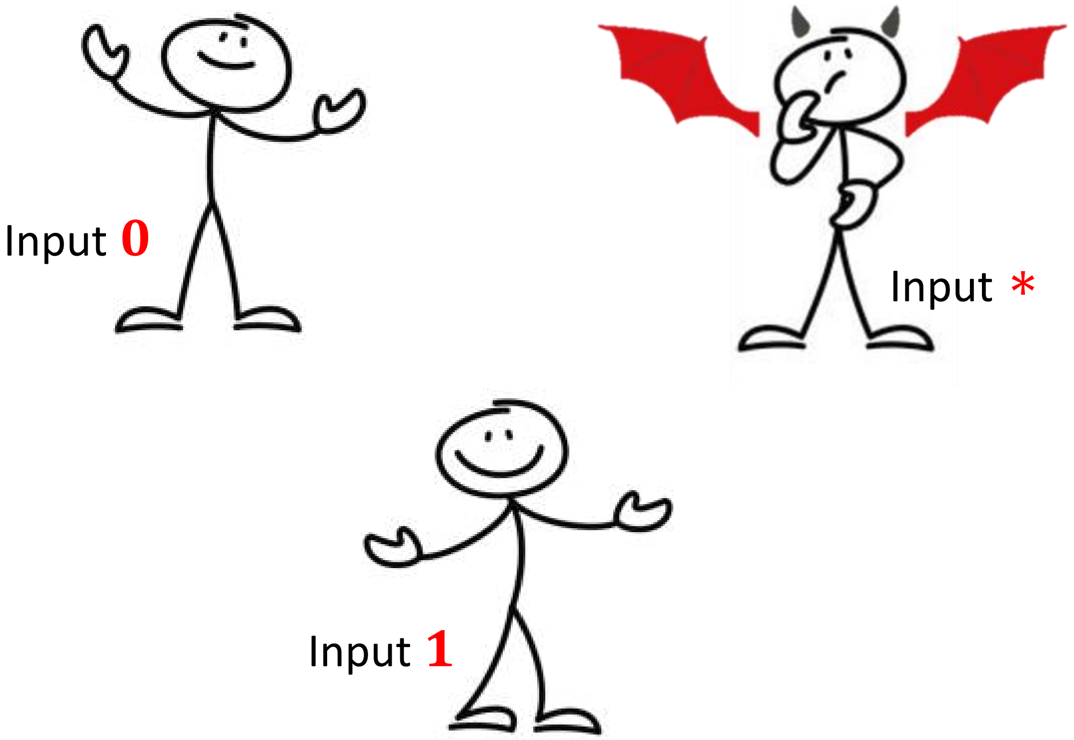
- On the positive (protocols) side

Additional Contribution (See Full Version of the Paper)

Locally consistent security $\Longrightarrow$ Malicious security

Our Attack
1st Round Halting

Lower bound for 1st Round Halting

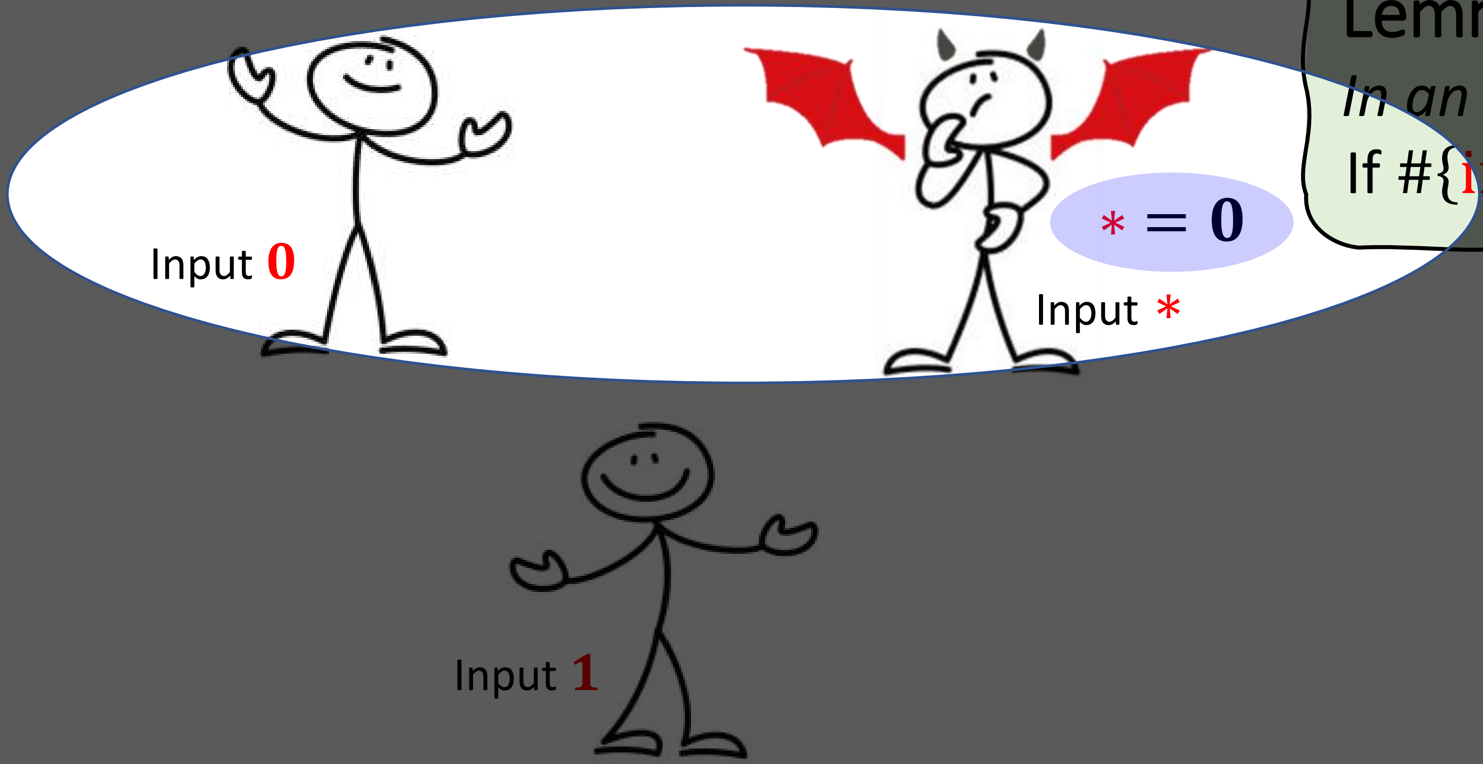


Lemma (Folklore)

In an honest *execution*:

If $\#\{\text{inputs} = z\} \geq 2n/3$ then $\text{output} = z$

Lower bound for 1st Round Halting

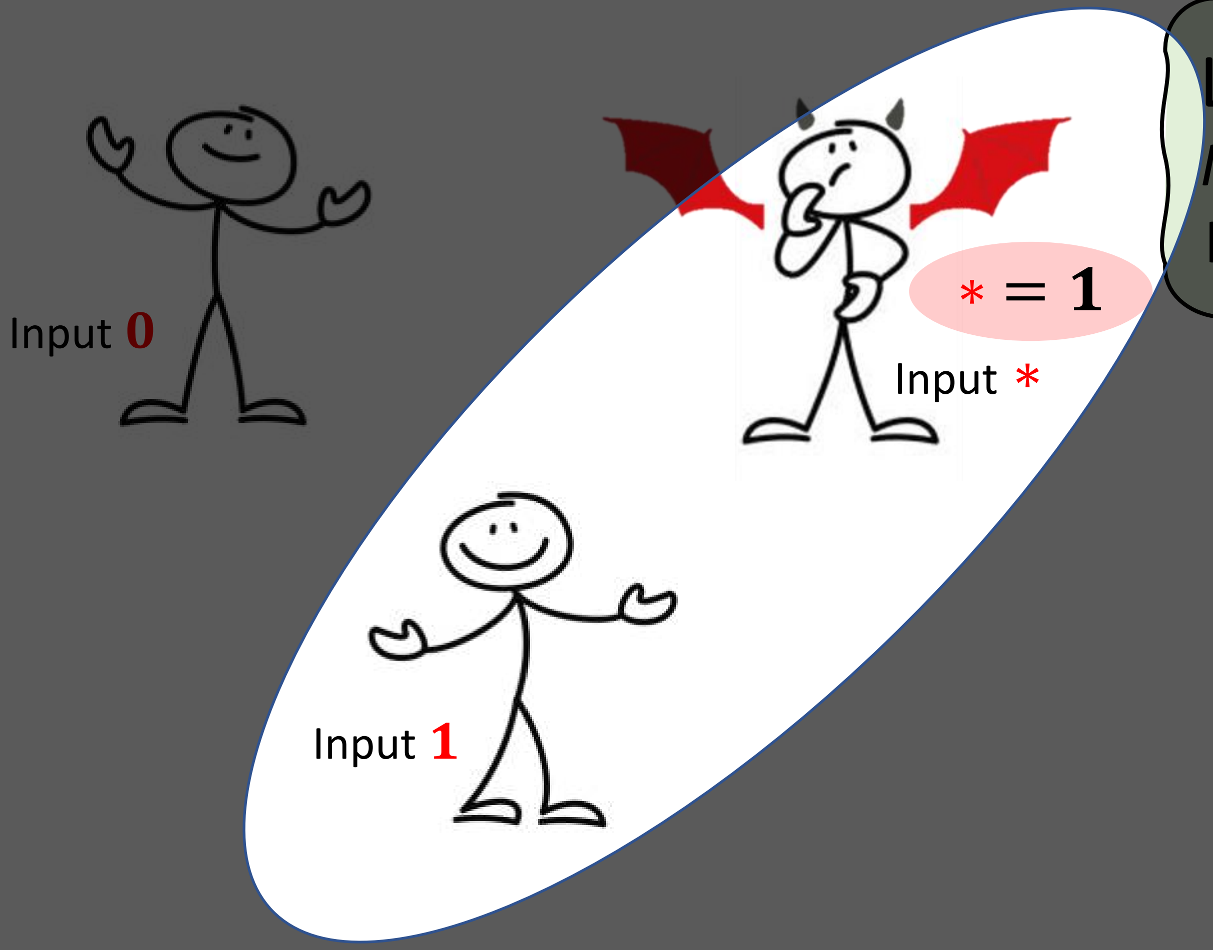


Lemma (Folklore)

In an honest *execution*:

If $\#\{\text{inputs} = z\} \geq 2n/3$ then $\text{output} = z$

Lower bound for 1^{st} Round Halting

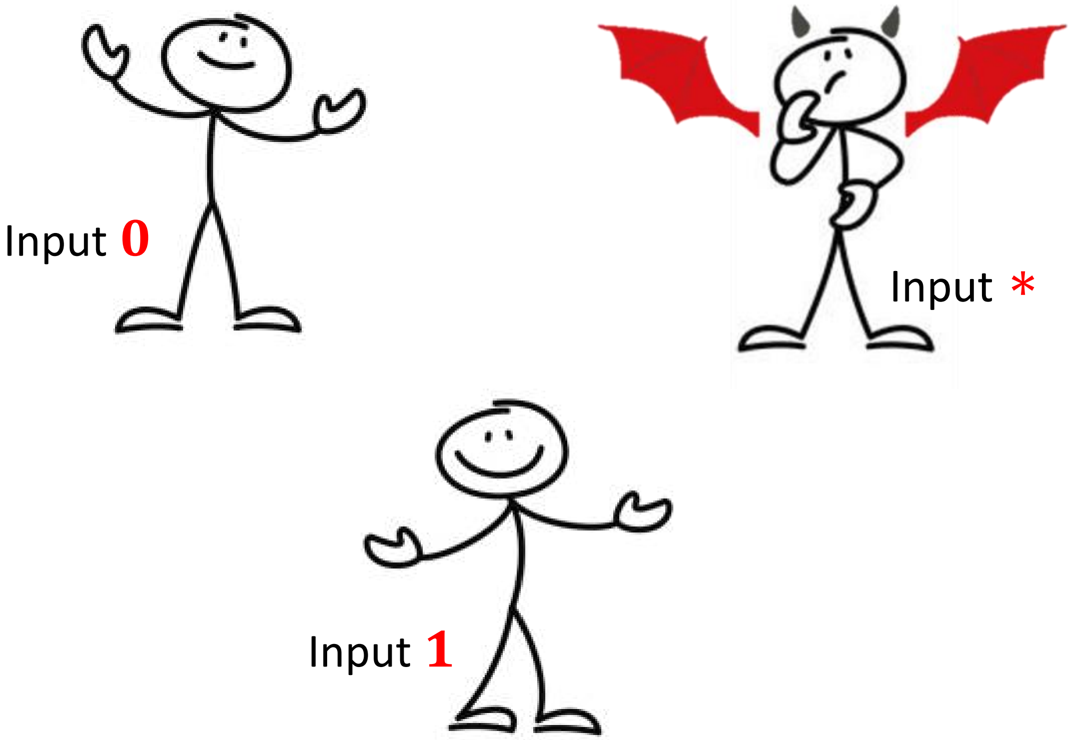


Lemma (Folklore)

In an honest *execution*:

If $\#\{\text{inputs} = z\} \geq 2n/3$ then $\text{output} = z$

Lower bound for 1st Round Halting



Lemma (Folklore)

In an honest *execution*:

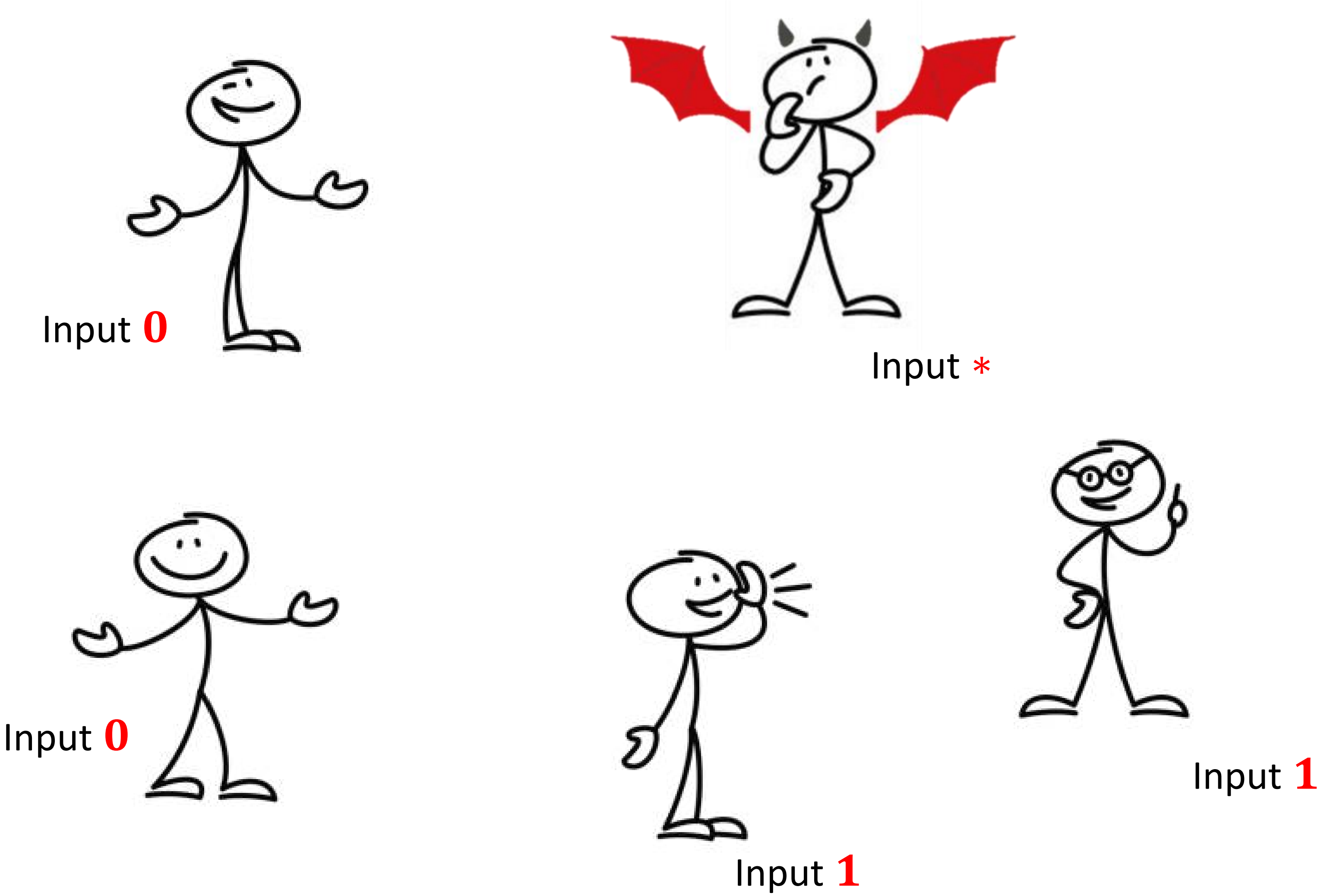
If $\#\{\text{inputs} = z\} \geq 2n/3$ then $\text{output} = z$

Theorem

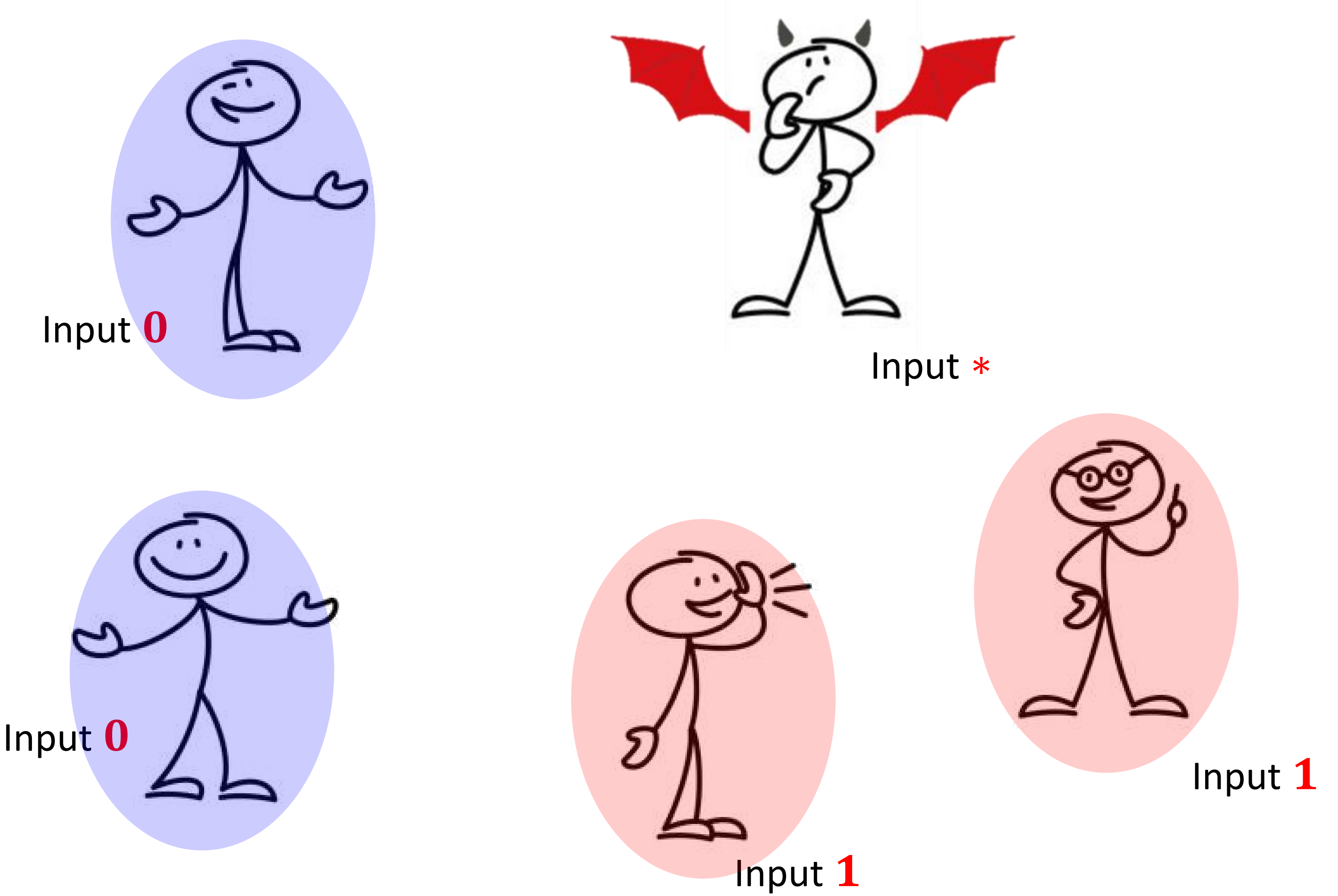
BA resilient against $n/3$ corruptions never halts at the 1st round.

Our Attack
2nd Round Halting

Lower bound for 2nd Round Halting



Lower bound for 2nd Round Halting



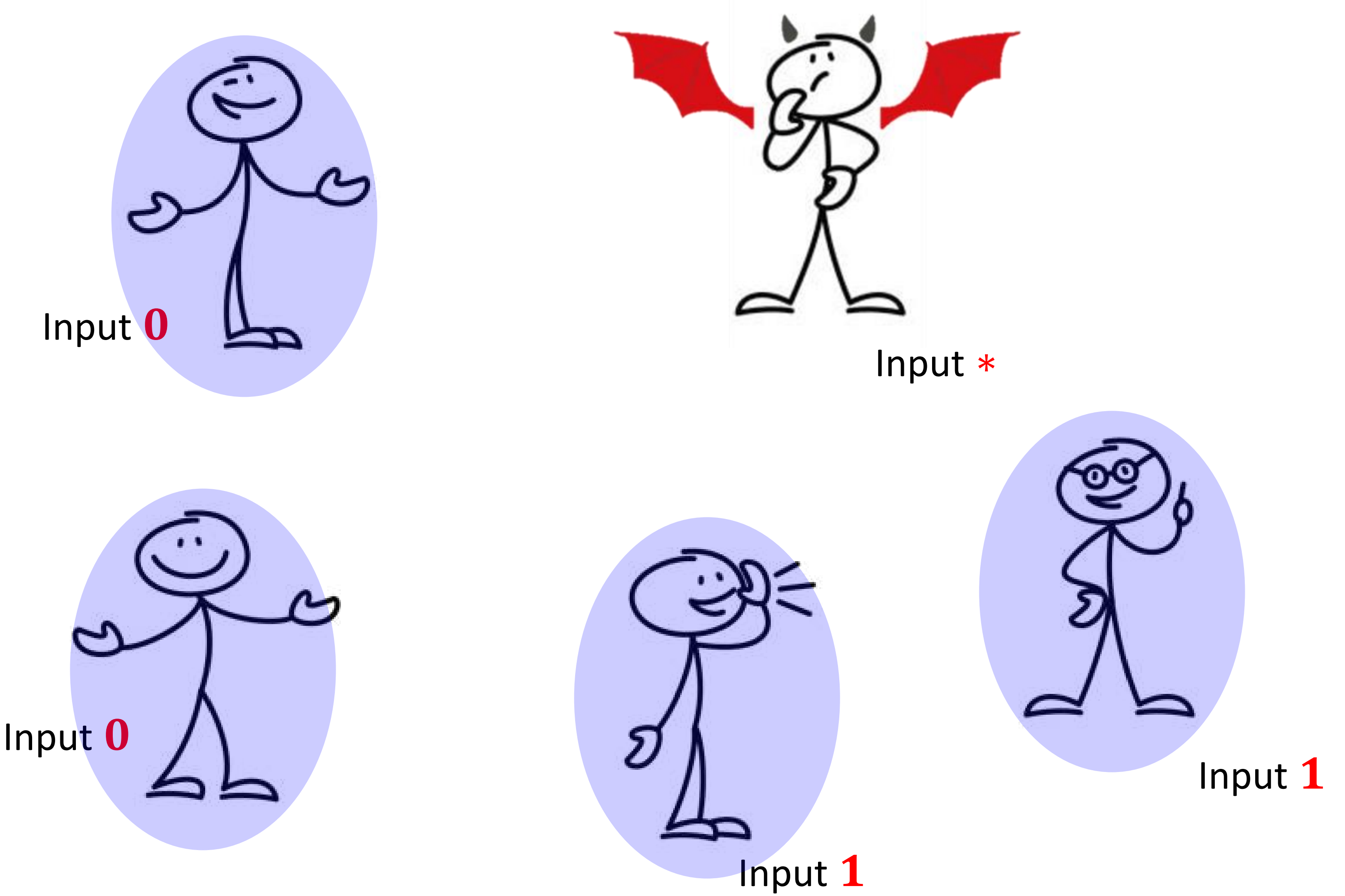
$* = 0$

$* = 1$

Parties can use the second round to ***spot liars!***

Lower bound for 2nd Round Halting

(Assume parties always halt at 2nd round)



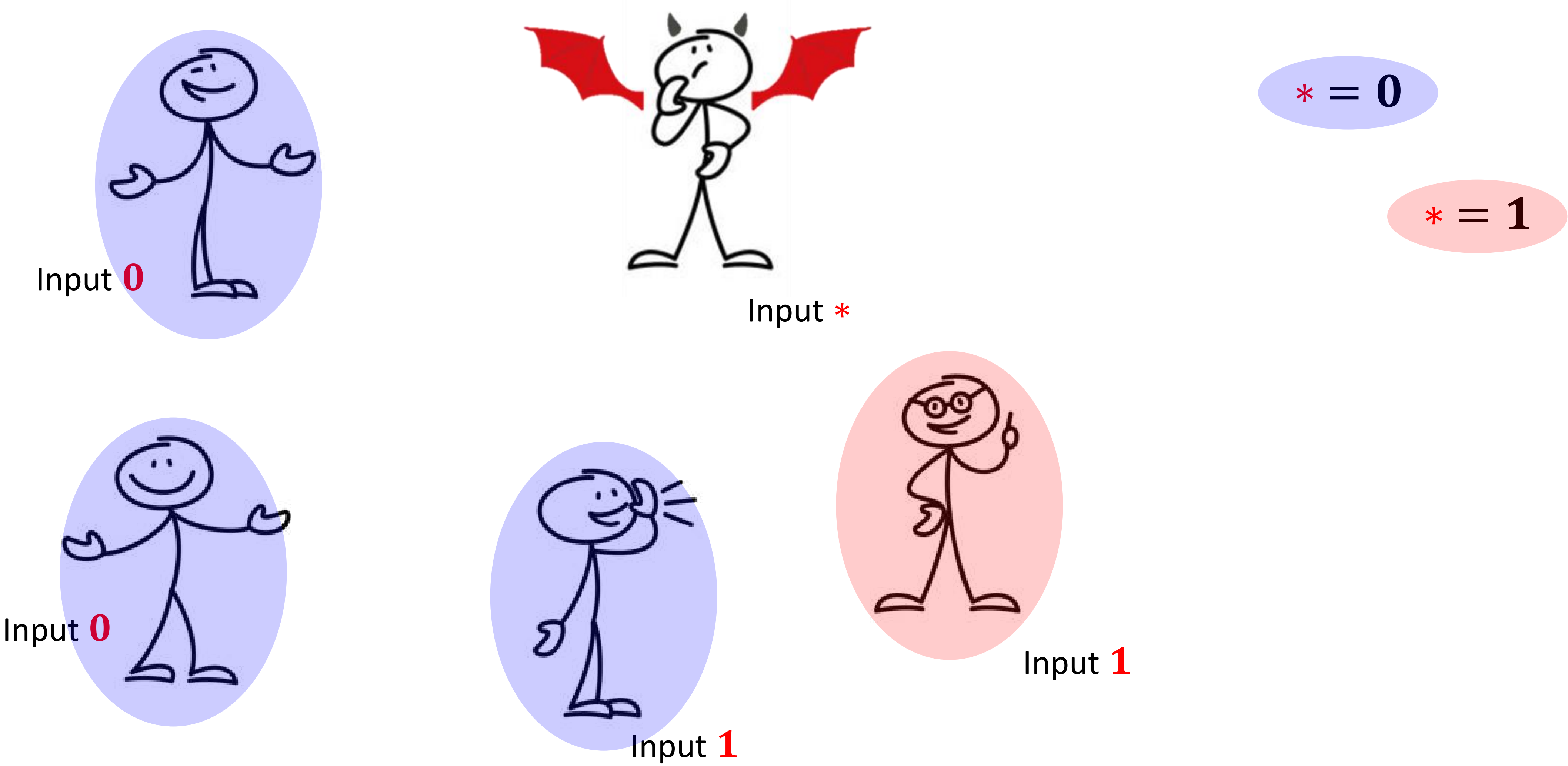
$* = 0$

$* = 1$

Honest execution with 2/3 inputs = 0

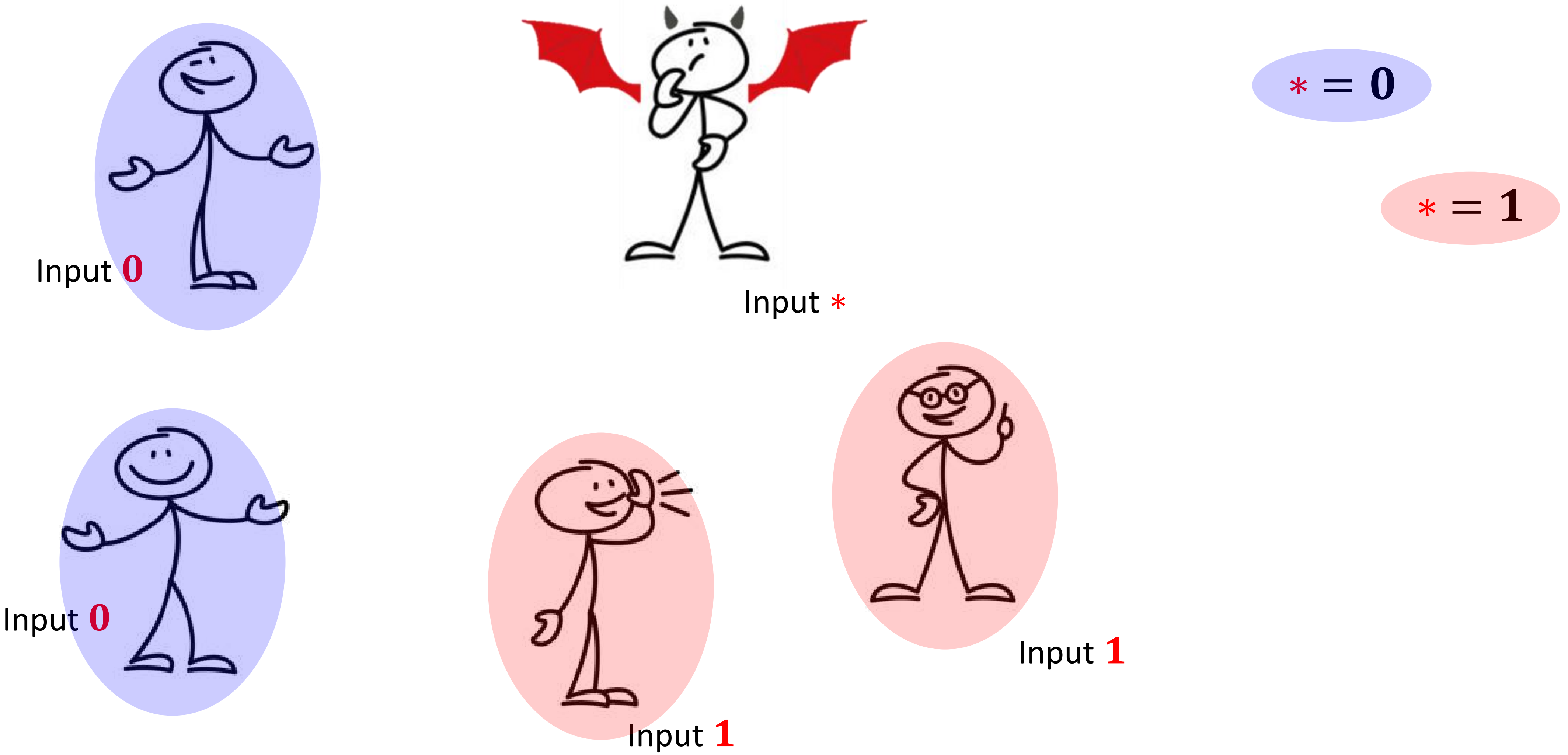
Lower bound for 2^{nd} Round Halting

(Assume parties always halt at 2^{nd} round)



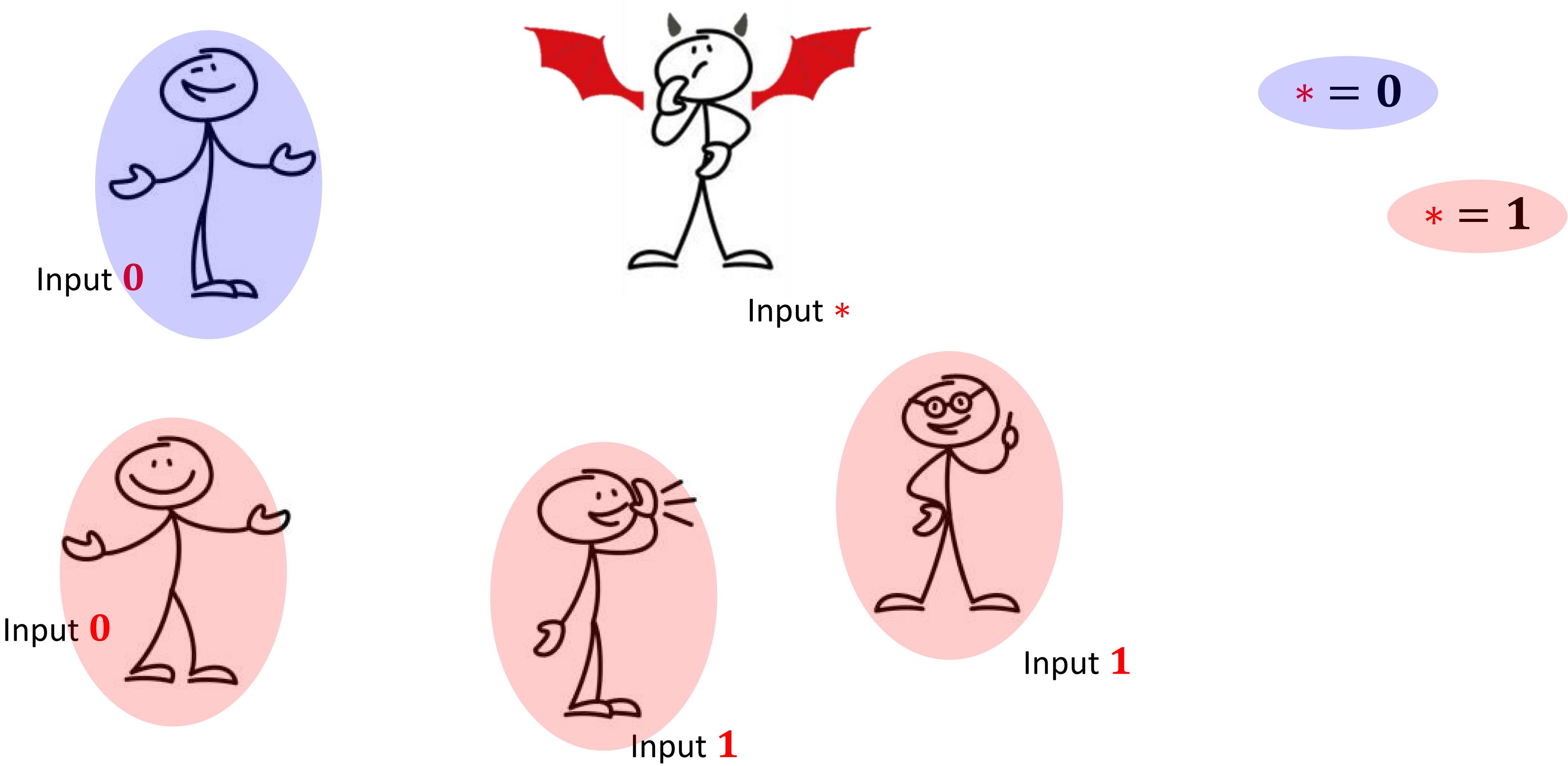
Lower bound for 2^{nd} Round Halting

(Assume parties always halt at 2^{nd} round)



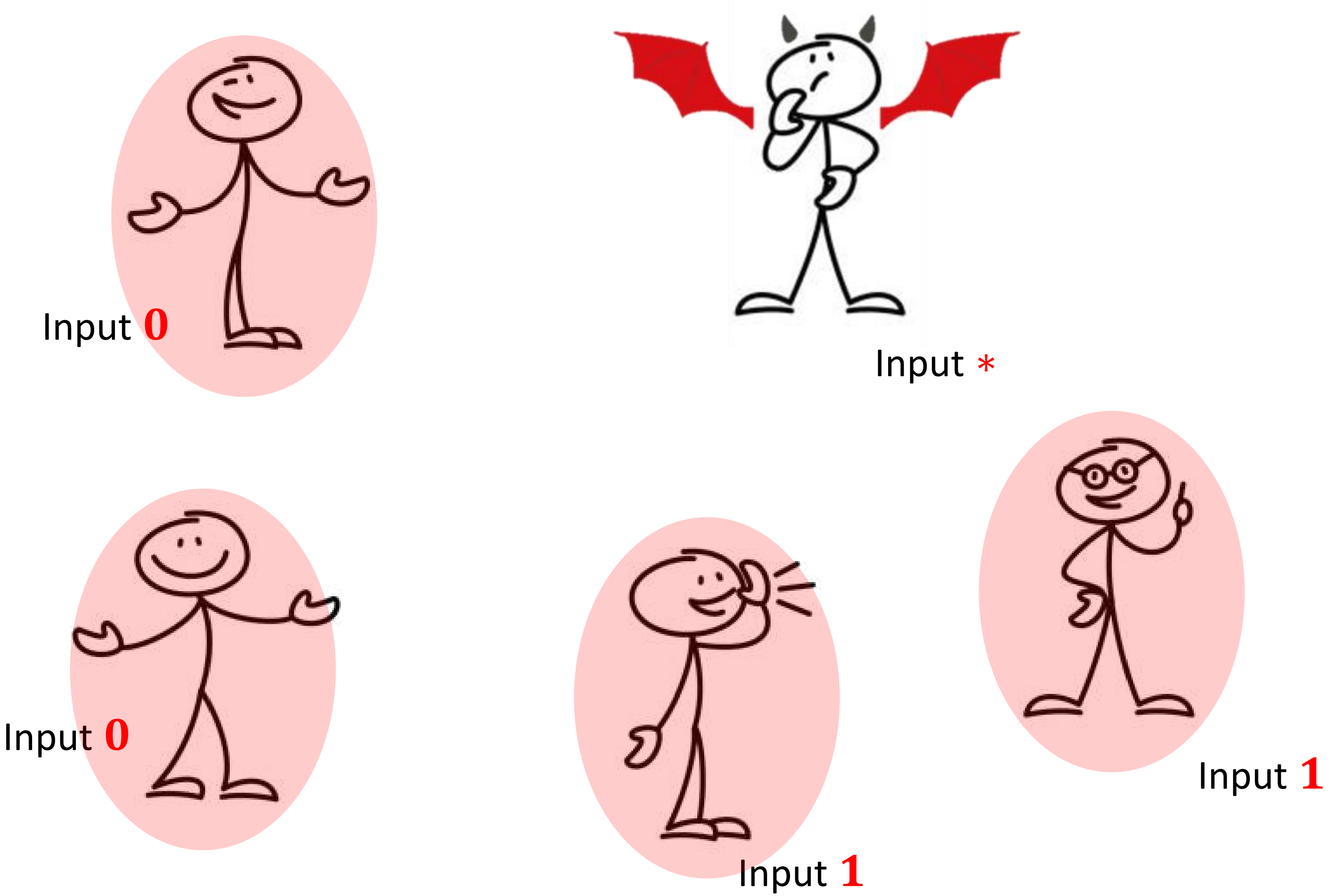
Lower bound for 2nd Round Halting

(Assume parties always halt at 2nd round)



Lower bound for 2^{nd} Round Halting

(Assume parties always halt at 2^{nd} round)



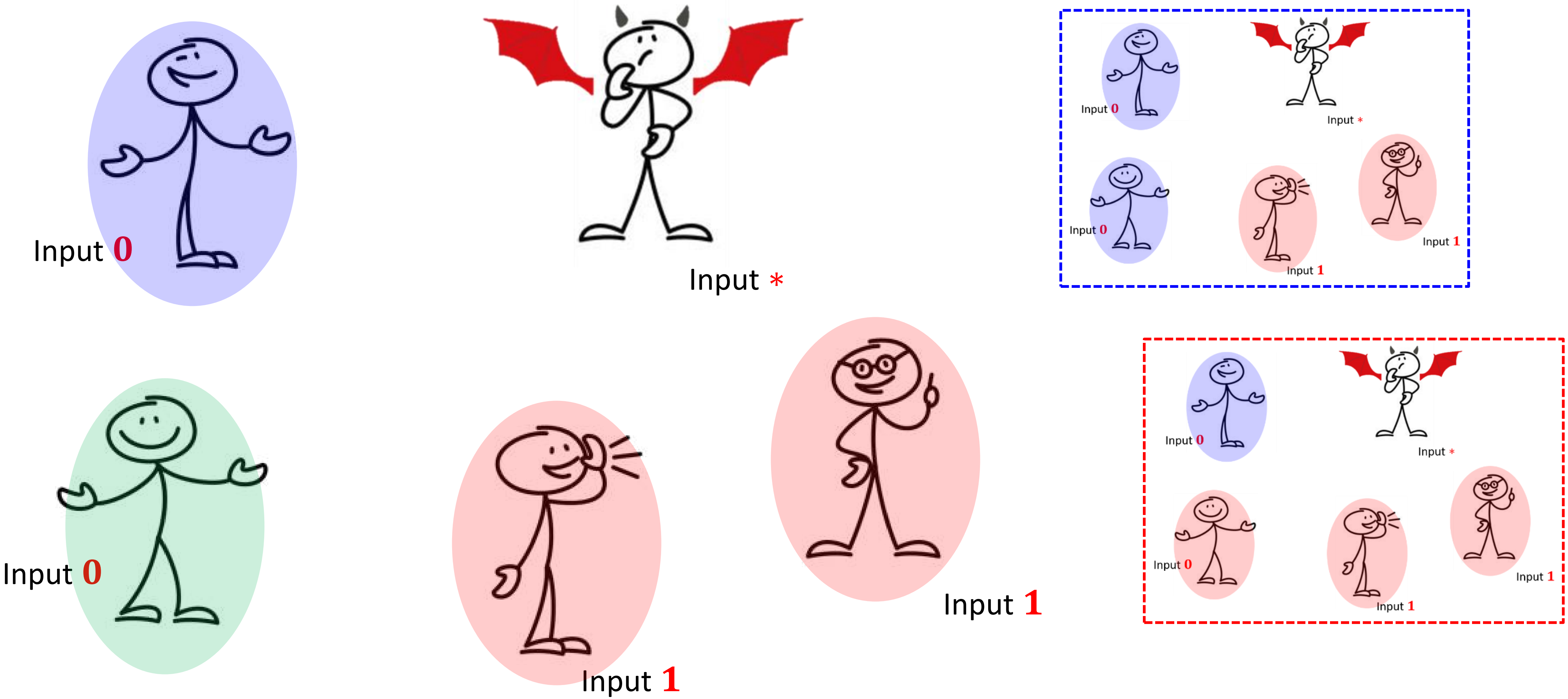
$* = 0$

$* = 1$

Honest execution with 2/3 inputs = 1

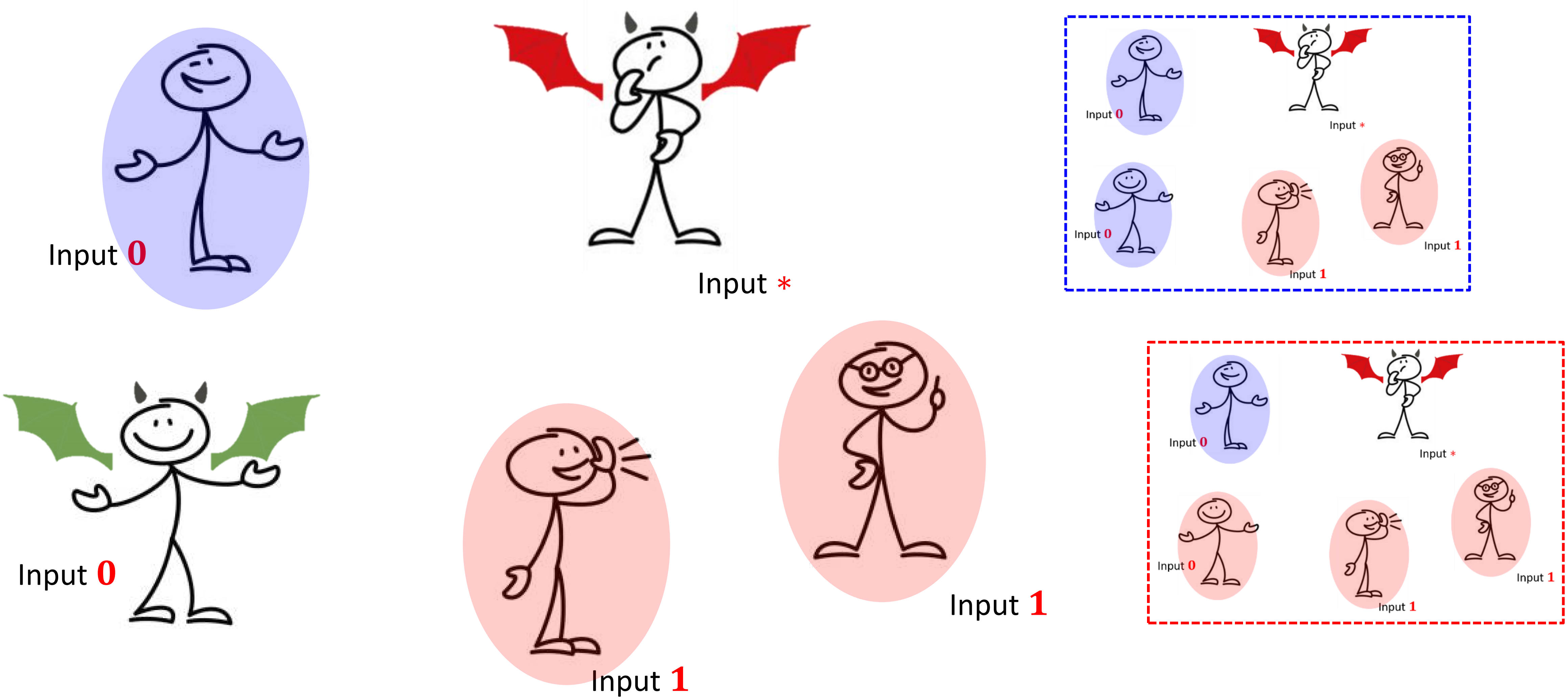
Lower bound for 2nd Round Halting

(Assume parties always halt at 2nd round)

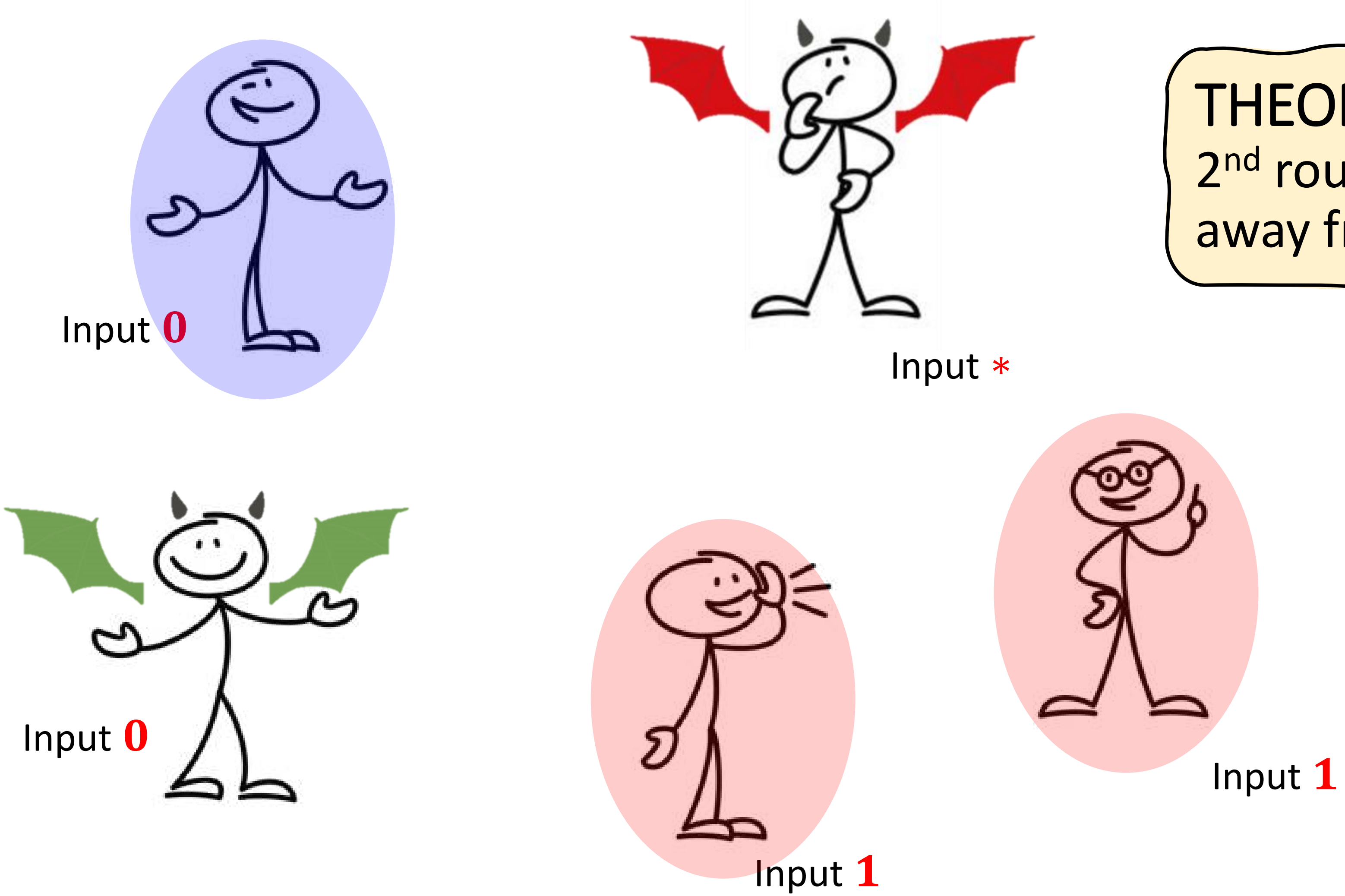


Lower bound for 2^{nd} Round Halting

(Assume parties always halt at 2^{nd} round)



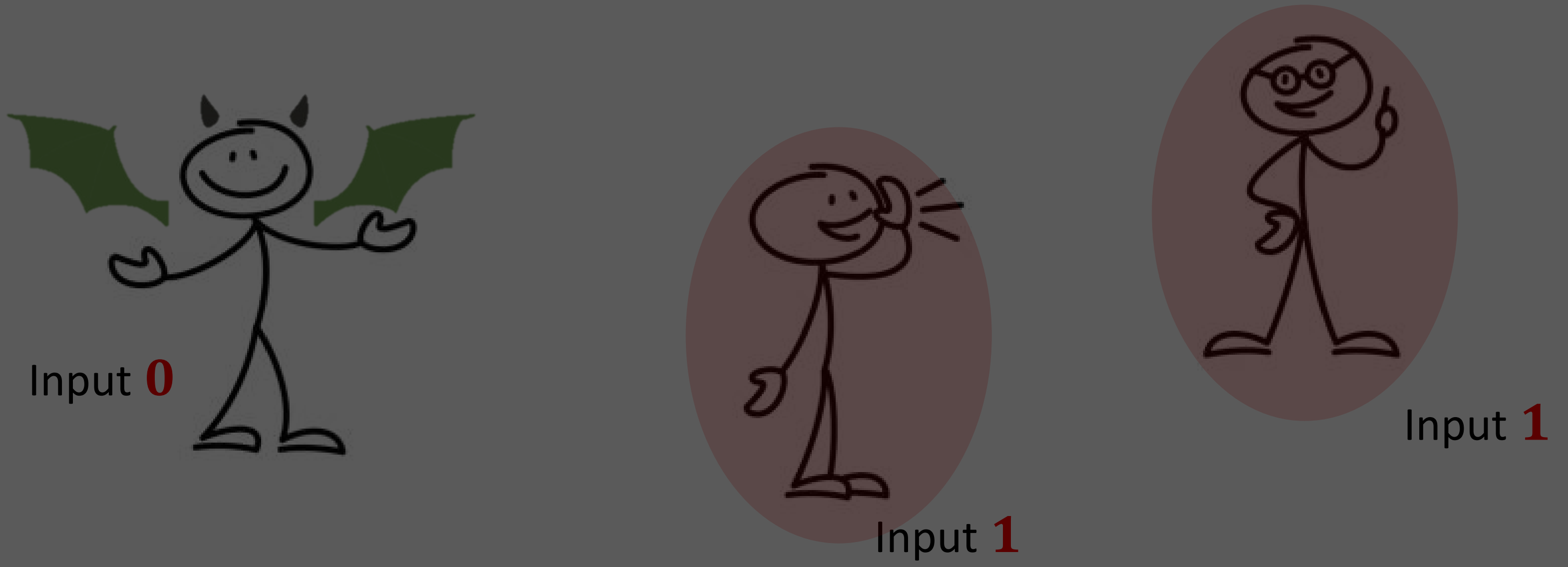
Lower bound for 2^{nd} Round Halting



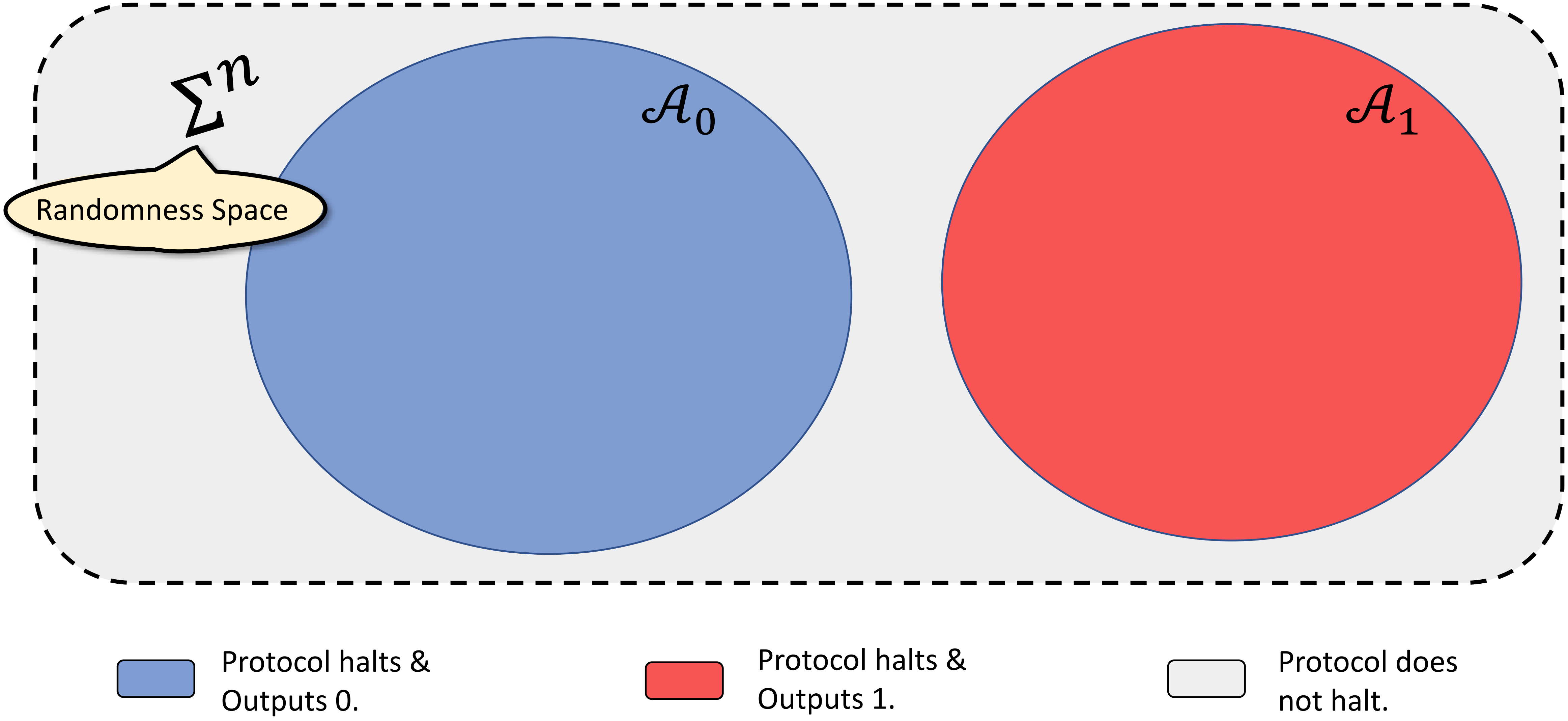
THEOREM
2^{nd} round halting is bounded away from 1.

Lower bound for 2^{nd} Round Halting

THEOREM
2^{nd} round halting is bounded away from 1.

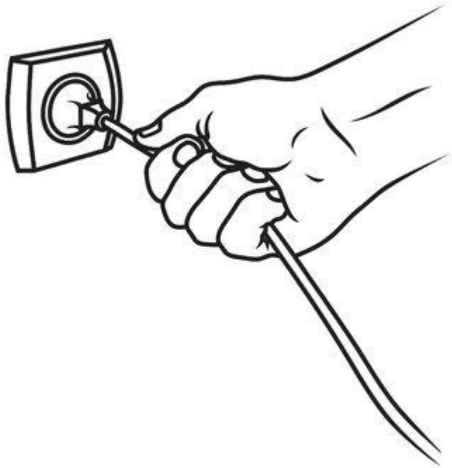


Limits of Attack



Our Attack
2nd Round Halting
with Abort

Attack with Aborting Parties

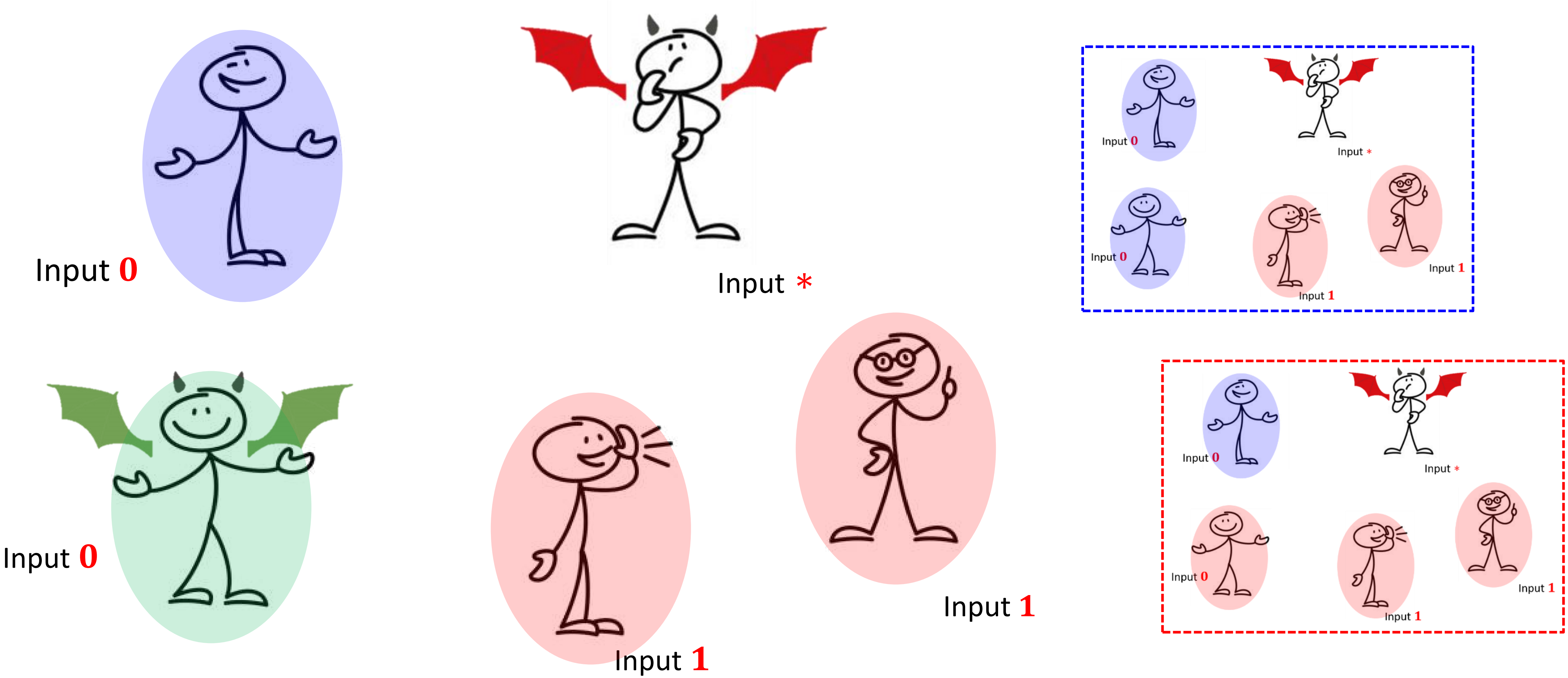


We add another dimension to our attack by instructing (certain) corrupted parties to **abort prematurely**

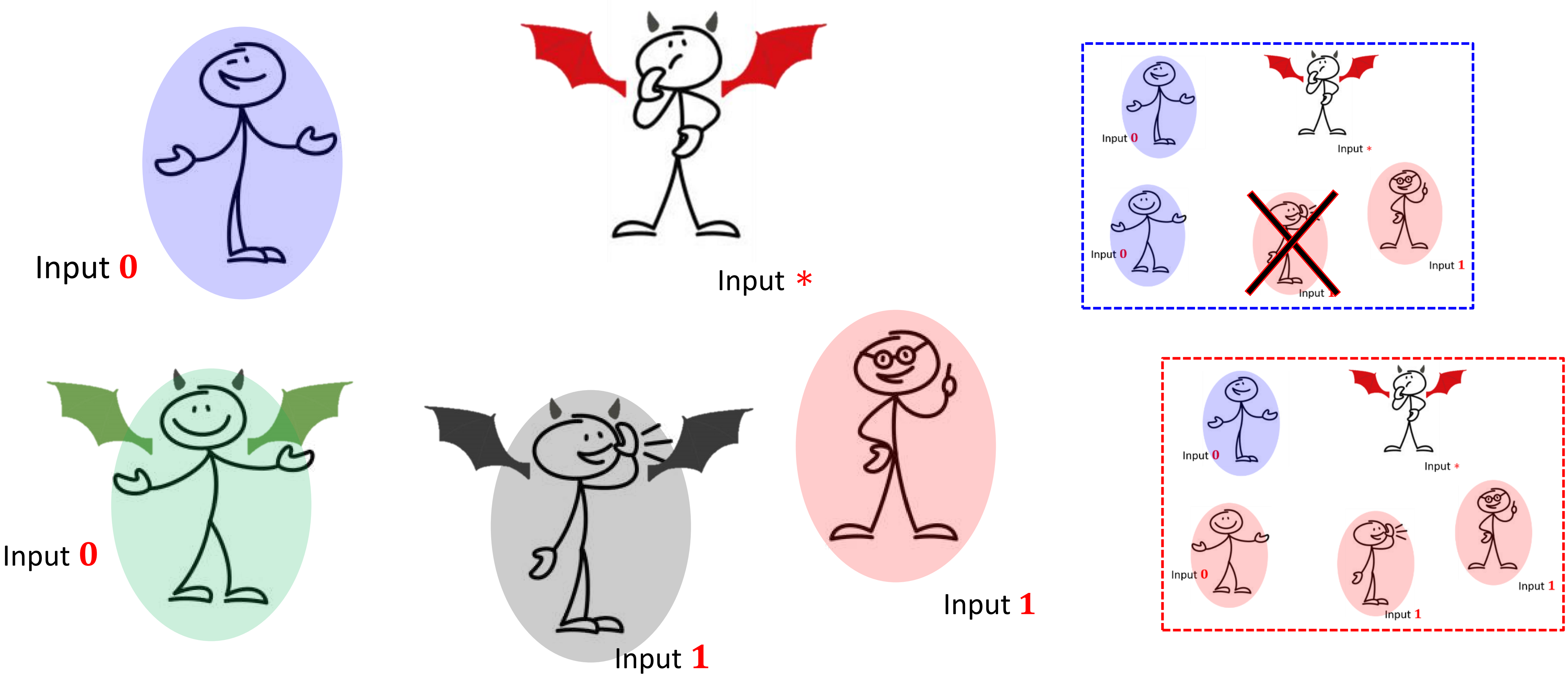
ATTACK w/ Aborting Parties

- Follow previous attack.
- At round **2**:
  Choose a random set $\mathcal{S}$ and **abort** it for a **subset** of honest parties.

Attack with Aborting Parties



Attack with Aborting Parties



Theorem Statement

Theorem Statement

Conjecture 1.5. *For any $\sigma, \lambda > 0$ there exists $\delta > 0$ such that the following holds for large enough $n \in \mathbb{N}$: let Σ be a finite alphabet, and let $\mathcal{A}_0, \mathcal{A}_1 \subseteq \{\Sigma \cup \perp\}^n$ be two sets such that for both $b \in \{0,1\}$:*

$$\Pr_{\mathcal{S} \leftarrow \mathrm{D}_{n,\sigma}} \left[\Pr_{\boldsymbol{r} \leftarrow \Sigma^n} [\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r}) \in \mathcal{A}_b] \geq \lambda \right] \geq 1 - \delta.$$

Then,

$$\Pr_{\substack{\mathcal{S} \leftarrow \mathrm{D}_{n,\sigma} \\ \boldsymbol{r} \leftarrow \Sigma^n}} [\forall b \in \{0,1\} \colon \{\boldsymbol{r}, \perp_{\mathcal{S}}(\boldsymbol{r})\} \cap \mathcal{A}_b \neq \emptyset] \geq \delta.$$

We know how to handle limited (and unrealistic) cases without the conjecture.

THEOREM

Conj. 1.5. $\Longrightarrow$ *BA protocols* halt after two rounds with probability 0.

Public Randomness (PR) Protocols

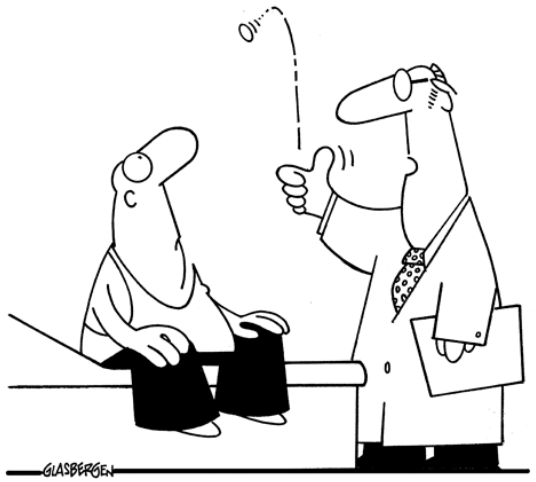
Analogues of (inputless) public coin protocols

Randomness is sent in the clear

Public Randomness Protocols:

The ℓ-th round message from P_i to P_k is a pair $(m_{i,k}^{(\ell)}, r_i^{(\ell)})$ s.t.
$m_{i,k}^{(\ell)}$ is a deterministic function of P_i's view.

- Such protocols are typically
  - ✓ Conceptually Simple(r)
  - ✓ Highly Efficient (inputless regime).
- All known BA protocols can be cast as PR protocols.



Summary

For every BA resilient against $t = n/3$ corruptions

Halting Probability in round 1	Halting Probability in round 2
$o(1) \approx 0$	$1 - \Theta(1) \ll 1$

Under plausible combinatorial assumption:

Halting Probability in round 2
$o(1) \approx 0$

FIN