Communication Lower Bounds for Cryptographic Broadcast Protocols

Erica Blum
REED COLLEGE

Elette Boyle
Reichman University
NTT Research

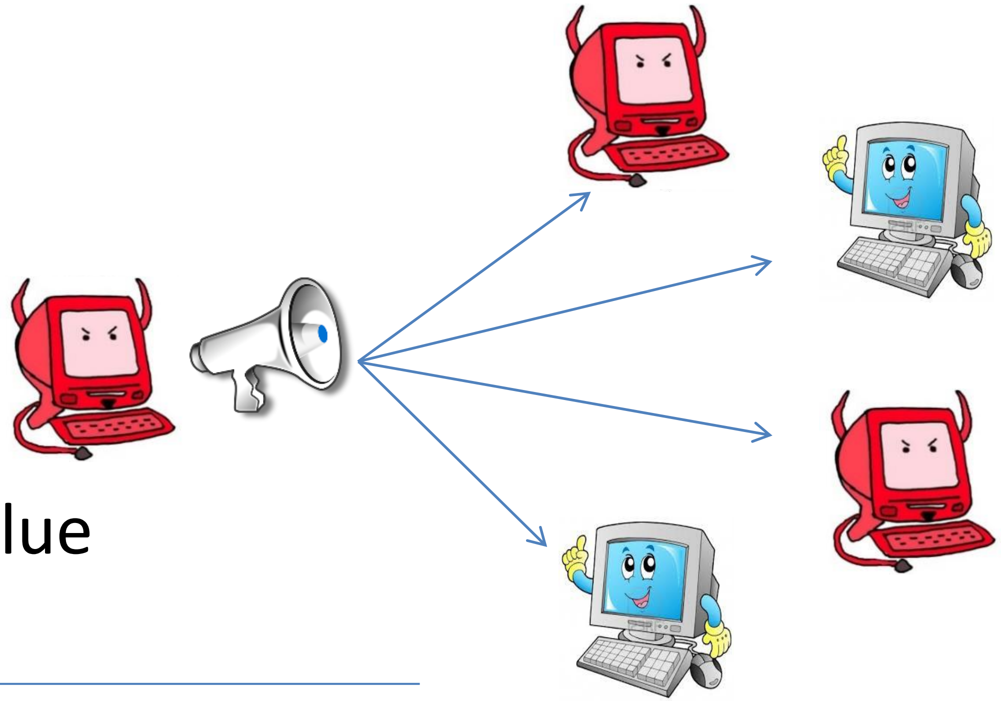
Ran Cohen
Reichman University

Chen-Da Liu-Zhang
HSLU Hochschule Luzern
web3 foundation

Broadcast Protocols

A **broadcast protocol** with sender S satisfies the following properties:

- Validity: if the sender is honest then all honest output its value
- Agreement: all honest output the same value

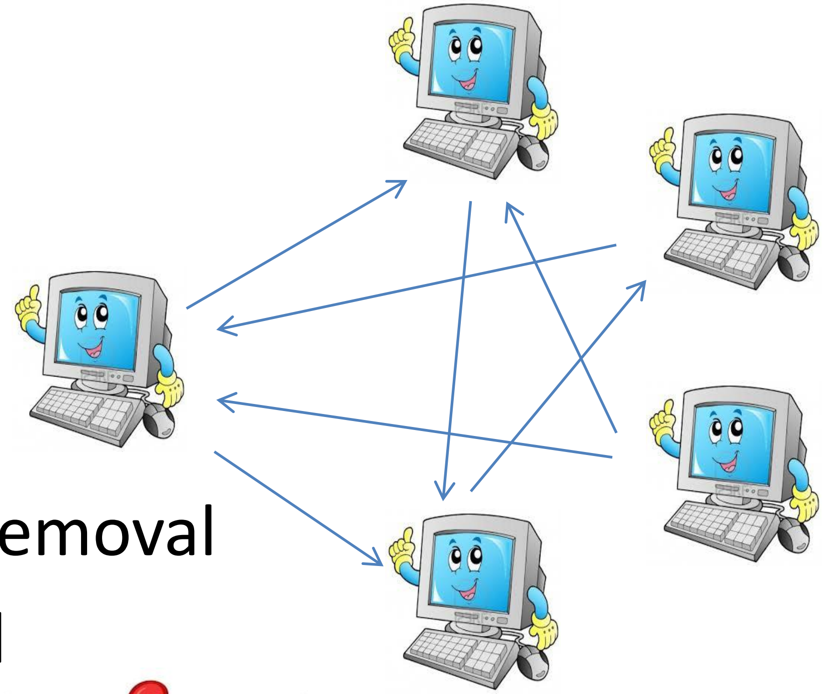


Byzantine agreement: a closely related multi-input version

- Validity: if all honest parties begin with input x, they all output x
- Agreement: as before

Setting

- Synchronous message passing
- Malicious (Byzantine) adversary
- Corruption timing:
  - **Static**: before the protocol begins
  - **Adaptive**: on-the-fly during the execution
    - **Strongly adaptive**: “after the fact” message removal
    - **Weakly adaptive**: no “after the fact” removal



static

weakly adaptive

strongly adaptive

Playground of feasibility & impossibility

Deterministic broadcast: simple protocols, prefect security

Feasibility		Resiliency		Rounds		Connectivity		Communication	
✗	✓	✗	✓	✗	✓	✗	✓	✗	✓
async	sync	$t \geq n/3$	$t < n/3$	$< t+1$	$\geq t+1$	$< 2t+1$	$\geq 2t+1$	$o(n^2)$	$\Omega(n^2)$

Not scalable

Let's lower our expectations

Clean & elegant results

Playground of feasibility & impossibility

Feasibility		Resiliency		Rounds		Connectivity		Communication	
async	sync	$t \geq n/3$	$t < n/3$	$< t+1$	$\geq t+1$	$< 2t+1$	$\geq 2t+1$	$o(n^2)$	$\Omega(n^2)$

Randomness & Cryptography

Security with high probability

Security wrt PPT adversaries

Playground of feasibility & impossibility

Feasibility	Resiliency	Rounds	Connectivity	Communication
async / sync	$t \geq n/3$ / $t < n/3$	$< t+1$ / $\geq t+1$	$< 2t+1$ / $\geq 2t+1$	$o(n^2)$ / $\Omega(n^2)$

[Ben-Or'83]
[Rabin'83]
async BA

[Dolev-Strong'83]
$t < n$ (pki + sig)

[Feldman-Micali'88,…]
exp $O(1)$ rounds

These bounds held for >20 years

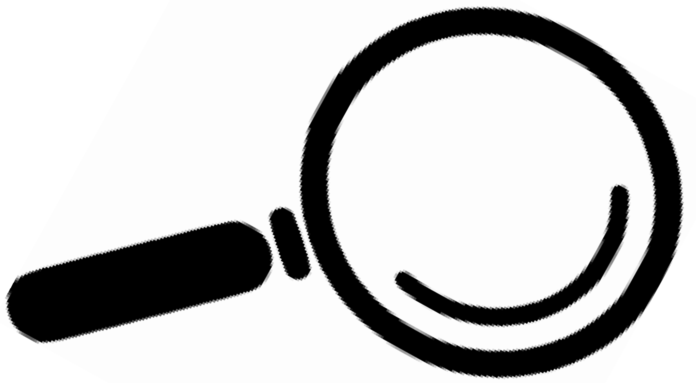
Playground of feasibility & impossibility

Feasibility		Resiliency		Rounds		Connectivity		Communication	
async	sync	$t \geq n/3$	$t < n/3$	$< t+1$	$\geq t+1$	$< 2t+1$	$\geq 2t+1$	$o(n^2)$	$\Omega(n^2)$

[Ben-Or'83]
[Rabin'83]
async BA

[Dolev-Strong'83]
$t < n$ (pki + sig)

[Feldman-Micali'88,...]
exp $O(1)$ rounds



Communication complexity: honest majority (partial)

Static

- [KS'09] BA with $o(n^2)$ communication and $o(n)$ connectivity
- [BGT'13] used cryptography for $\text{polylog}(n)$ locality

max degree in induced communication graph

- [B**C**G'21] balanced BA with $\tilde{O}(n)$ comm. ($\text{polylog}(n)$ bits per party)

Weakly Adaptive

- [Micali'17] & [ACDNPRS'19] unbalanced BA with $\tilde{O}(n)$ comm.

Strongly Adaptive

- **[ACDNPRS'19] t-secure BA $\Rightarrow \Omega(t^2)$ messages**

Communication complexity: dishonest majority (partial)

Strongly Adaptive

Corruption-unfair

- All communication-efficient broadcast based on [DS'83]
  $O(n^2)$ messages and $O(n^3)$ communication (pki + sig)

Weakly Adaptive

constant

- [CPS'20] for $t = (1 - \epsilon) \cdot n$ constructed broadcast
  with $\tilde{O}(n^2)$ communication (trusted pki + VRF)

Static

- [TLP'22] for $t = (1 - \epsilon) \cdot n$ constructed broadcast
  with $\tilde{O}(n^2)$ communication and $\mathrm{polylog}(n)$ locality (pki + sig)

Starting point

	Setup	Resiliency (t)	Total comm	Locality
Strongly adaptive				
Weakly adaptive				
Static				

Starting point

	Setup	Resiliency (t)	Total comm	Locality	
Strongly adaptive	pki	$t < n$	$O(n^3)$	n	[DS'83]
	any	$t = \Theta(n)$	$\Omega(n^2)$	$\Omega(n)$	[ACDNPRS19]
Weakly adaptive					
Static					

Starting point

	Setup	Resiliency (t)	Total comm	Locality	
Strongly adaptive	pki	$t < n$	$O(n^3)$	n	[DS'83]
	any	$t = \Theta(n)$	$\Omega(n^2)$	$\Omega(n)$	[ACDNPRS19]
Weakly adaptive	trusted pki	$(1-\epsilon) \cdot n$	$\tilde{O}(n^2)$	$O(n)$	[CPS'20]
Static					

Starting point

	Setup	Resiliency (t)	Total comm	Locality	
Strongly adaptive	pki	$t < n$	$O(n^3)$	n	[DS’83]
	any	$t = \Theta(n)$	$\Omega(n^2)$	$\Omega(n)$	[ACDNPRS19]
Weakly adaptive	trusted pki	$(1-\epsilon)\cdot n$	$\tilde{O}(n^2)$	$O(n)$	[CPS’20]
Static	any (deterministic)	$t = \Theta(n)$	$\Omega(n^2)$	$\Omega(n)$	[DR’85]
	pki	$(1-\epsilon)\cdot n$	$\tilde{O}(n^2)$	$\mathrm{polylog}(n)$	[TLP’22]

No lower bounds for randomized broadcast wrt static/weakly adaptive

Can we get $o(n^2)$ communication?

Yes! using randomness & cryptography

- [CPS'20] use a **polylog-size committee** to run DS ⇒ small signature-chains (but messages are propagated in an all-to-all network)
- [TLP'22] use a **polylog-degree expander** to propagate all-to-all messages
- Together we get:

Cor 1: Let $0 < \epsilon < 1$ be a constant and $t = (1 - \epsilon) \cdot n$
Assuming signatures + VRF and trusted-PKI setup
∃ statically t-secure broadcast with $\boldsymbol{\tilde{O}(n)}$ comm. and $\mathbf{polylog}(\boldsymbol{n})$ locality

Can we do better?

An analog for Cor 1 with **more static corruptions**?

Thm 2: Let $\varphi(n) \in o(1)$ and $t = \big(1 - \varphi(n)\big) \cdot n$

For any **statically** t-secure broadcast, the message complexity is

$$\Omega\left(n \cdot \frac{1}{\varphi(n)}\right)$$

Examples:

- $n - \frac{n}{\log^d n}$ corruptions (ie, $\varphi(n) = \frac{1}{\log^d n}$) require $\Omega\big(n \cdot \log^d n\big)$ messages
- $n - \sqrt{n}$ corruptions (ie, $\varphi(n) = \frac{1}{\sqrt{n}}$) require $\Omega(n \cdot \sqrt{n})$ messages
- $n - c$ corruptions (ie, $\varphi(n) = \frac{c}{n}$) require $\Omega(n^2)$ messages

Can we do better (#2)?

An analog for Cor 1 with a **constant fraction of adaptive corruptions**?

Recall that Cor 1 guarantees $\text{polylog}(n)$ locality

With adaptive corruptions the sender must talk to $t+1$ (o/w gets isolated)

What about non-sender parties?

Thm 3: Let $0 < k < n/2$ and $t = n/2 + k$
Let π be a **weakly adaptive** t-secure broadcast and let P^* be a **non-sender**
Then, there exists an adversary that can force P^* to talk to k parties

E.g., for $t = 0.51 \cdot n$, the (non-sender) locality is $\Theta(n)$

Protocol design: ensure that each party has a path with high communication

Main Results

	Setup	Resiliency (t)	Total comm	Locality (non-sender)	
Strongly adaptive	pki	$t < n$	$O(n^3)$	n	[DS'83]
	any	$t = \Theta(n)$	$\Omega(n^2)$	$\Omega(n)$	[ACDNPRS19]
Weakly adaptive	trusted pki	$(1-\epsilon) \cdot n$	$\tilde{O}(n^2)$	$O(n)$	[CPS'20]
	any	$\boldsymbol{t = n/2 + k}$		$\boldsymbol{> k}$	**Thm 3**
Static	any (deterministic)	$t = \Theta(n)$	$\Omega(n^2)$	$\Omega(n)$	[DR'85]
	pki	$(1-\epsilon) \cdot n$	$\tilde{O}(n^2)$	$\mathrm{polylog}(n)$	[TLP'22]
	trusted pki	$\boldsymbol{(1-\epsilon) \cdot n}$	$\boldsymbol{\tilde{O}(n)}$	$\boldsymbol{\mathrm{polylog}(n)}$	**Cor 1**
	any	$\boldsymbol{(1-\varphi(n)) \cdot n}$	$\boldsymbol{\Omega(n/\varphi(n))}$		**Thm 2**

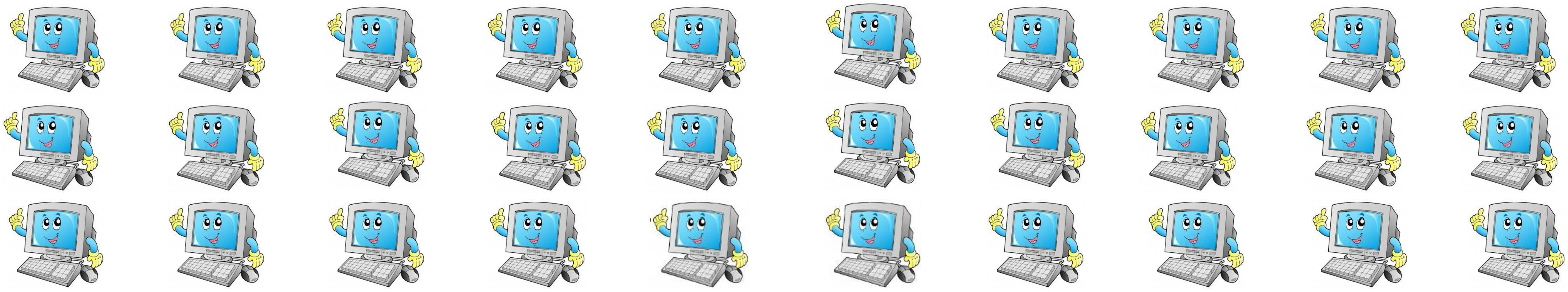
High-Level Overview

High-level idea for Thm 2

Thm 2: Let $\varphi(n) \in o(1)$ and $t = \big(1 - \varphi(n)\big) \cdot n$

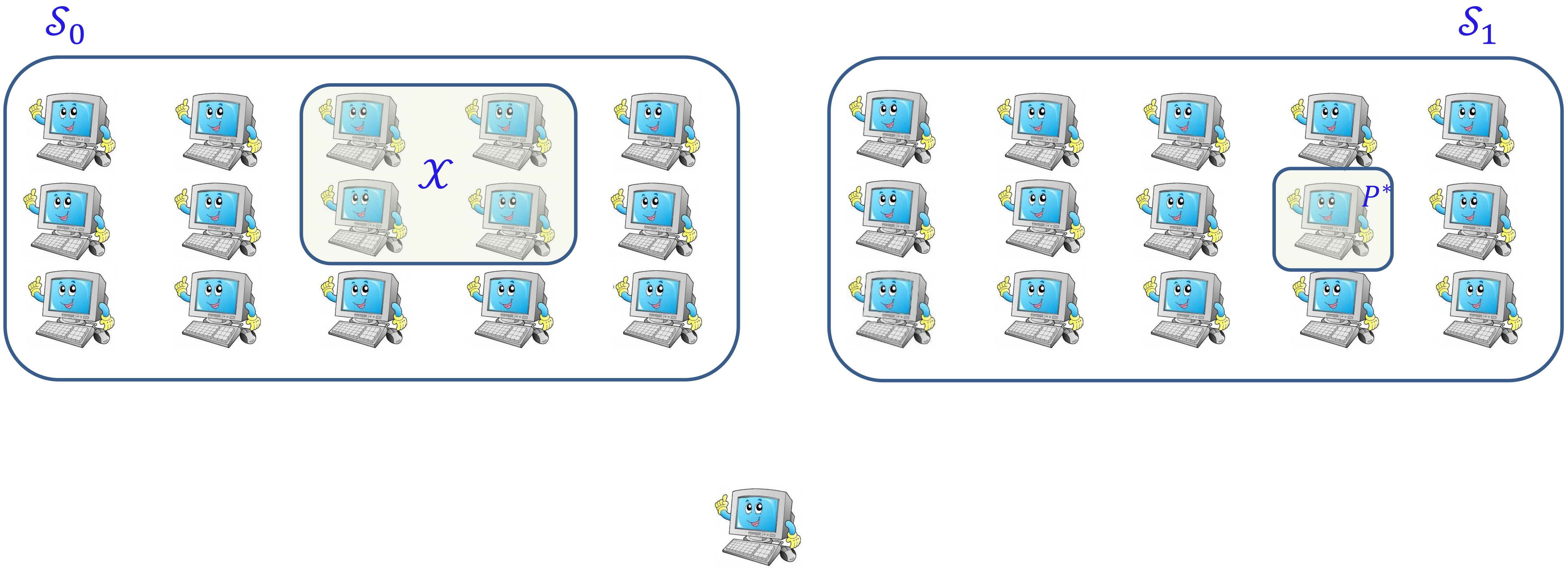
For any **statically** t-secure broadcast, the message complexity is

$$\Omega\left(n \cdot \frac{1}{\varphi(n)}\right)$$



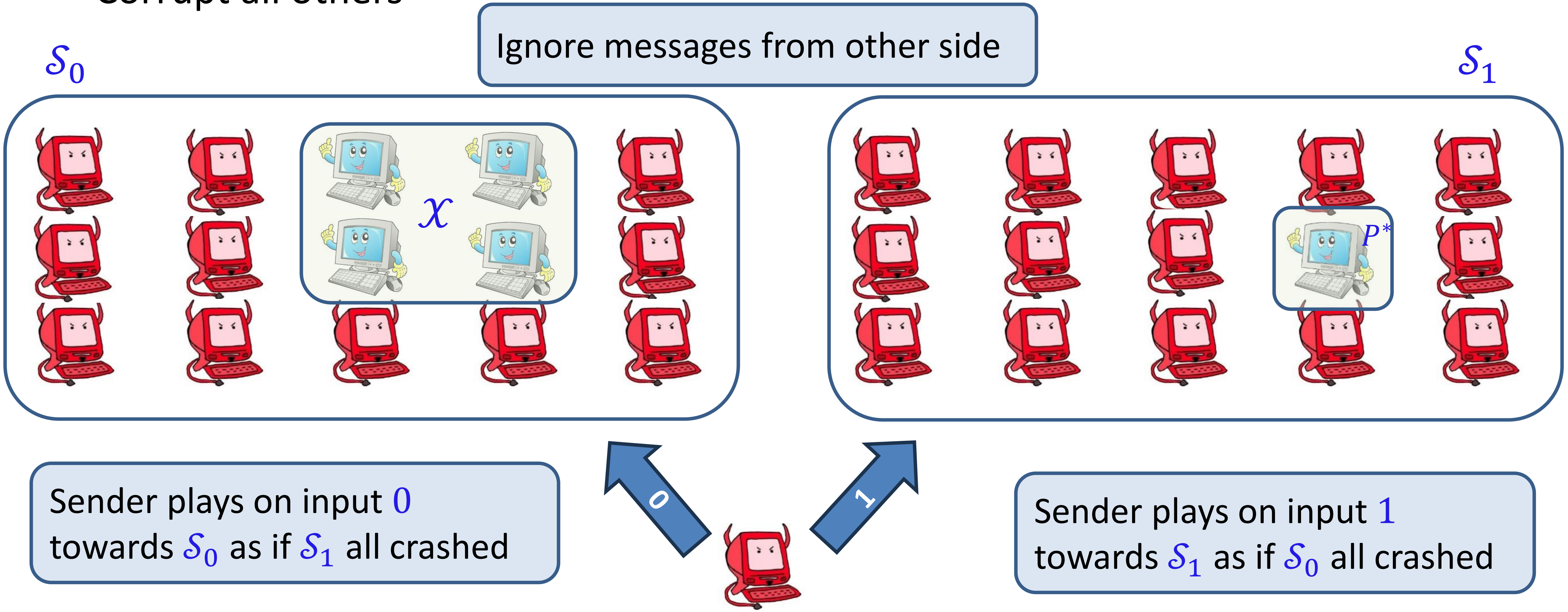
High-level idea for Thm 2

- Split all receivers to two subsets $\mathcal{S}_0$ and $\mathcal{S}_1$
- Choose set $\mathcal{X} \subseteq \mathcal{S}_0$ of size $\varphi(n) \cdot n - 1$ and a party $P^* \in \mathcal{S}_1$



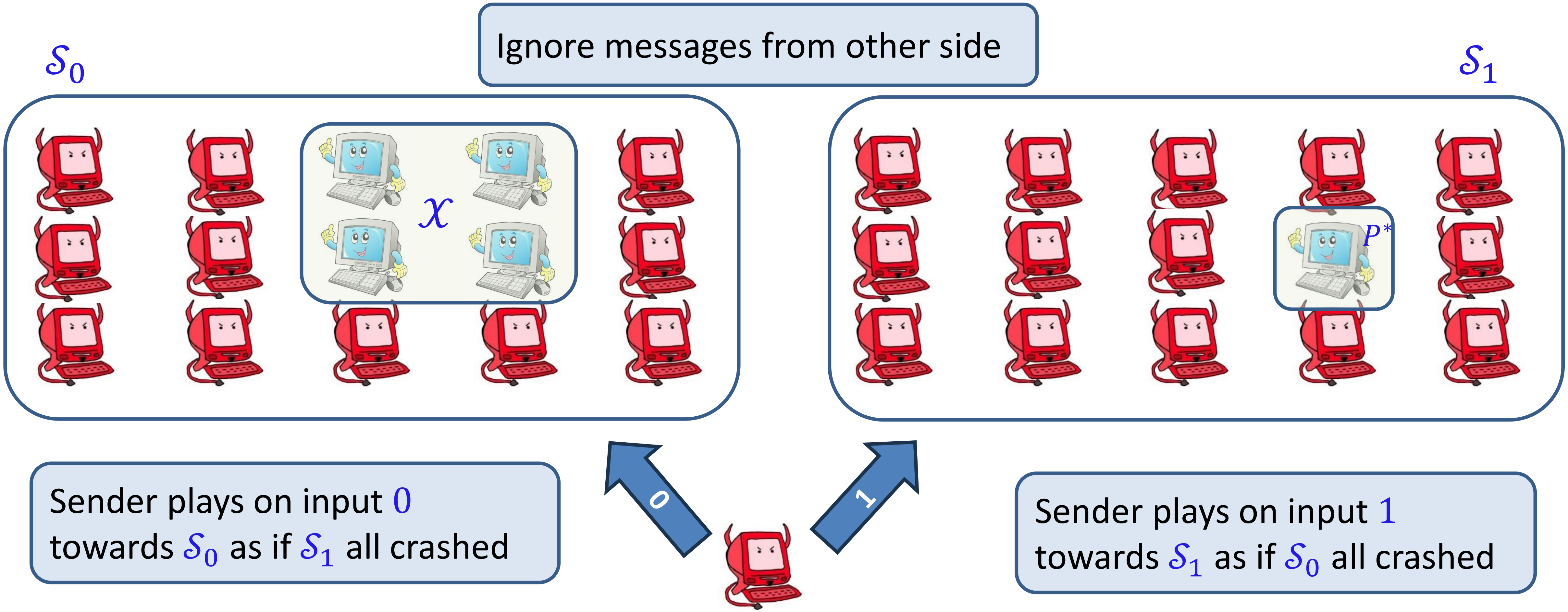
High-level idea for Thm 2

- Split all receivers to two subsets $\mathcal{S}_0$ and $\mathcal{S}_1$
- Choose set $\mathcal{X} \subseteq \mathcal{S}_0$ of size $\varphi(n) \cdot n - 1$ and a party $P^* \in \mathcal{S}_1$
- Corrupt all others



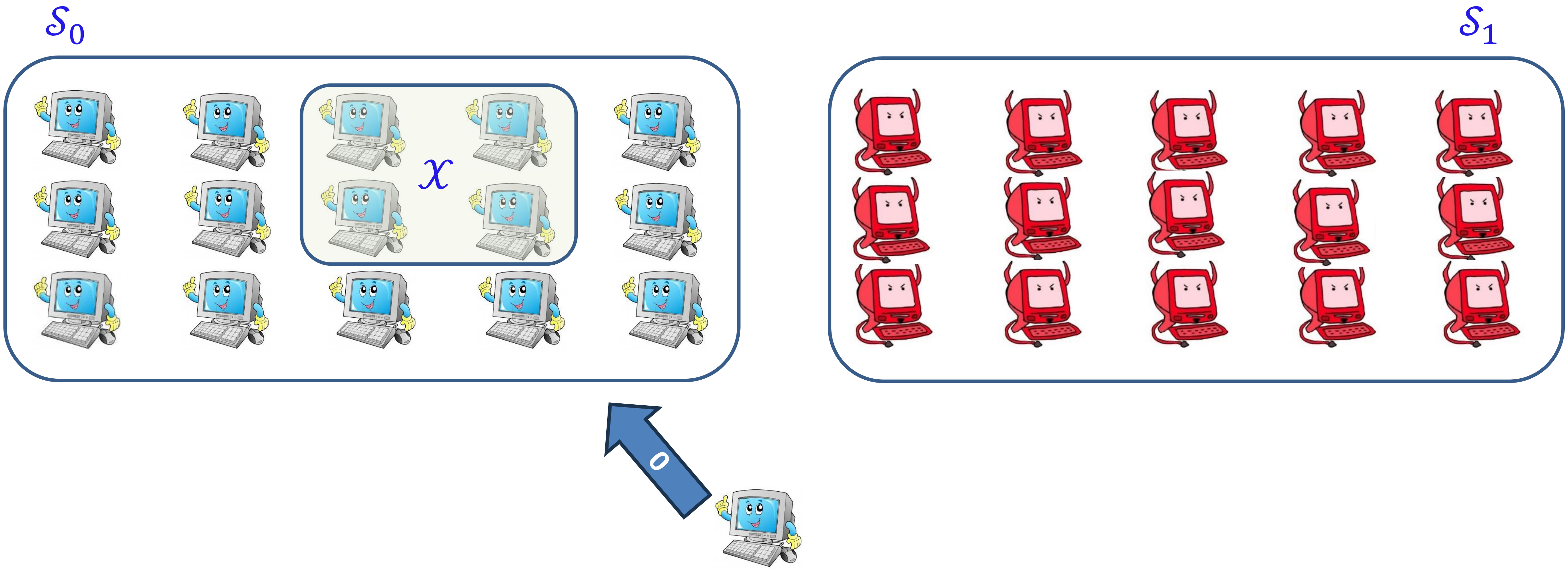
High-level idea for Thm 2

Lemma 1: if P^* and $\mathcal{X}$ do not communicate $\Rightarrow$ $\mathcal{X}$ outputs 0 and P^* outputs 1



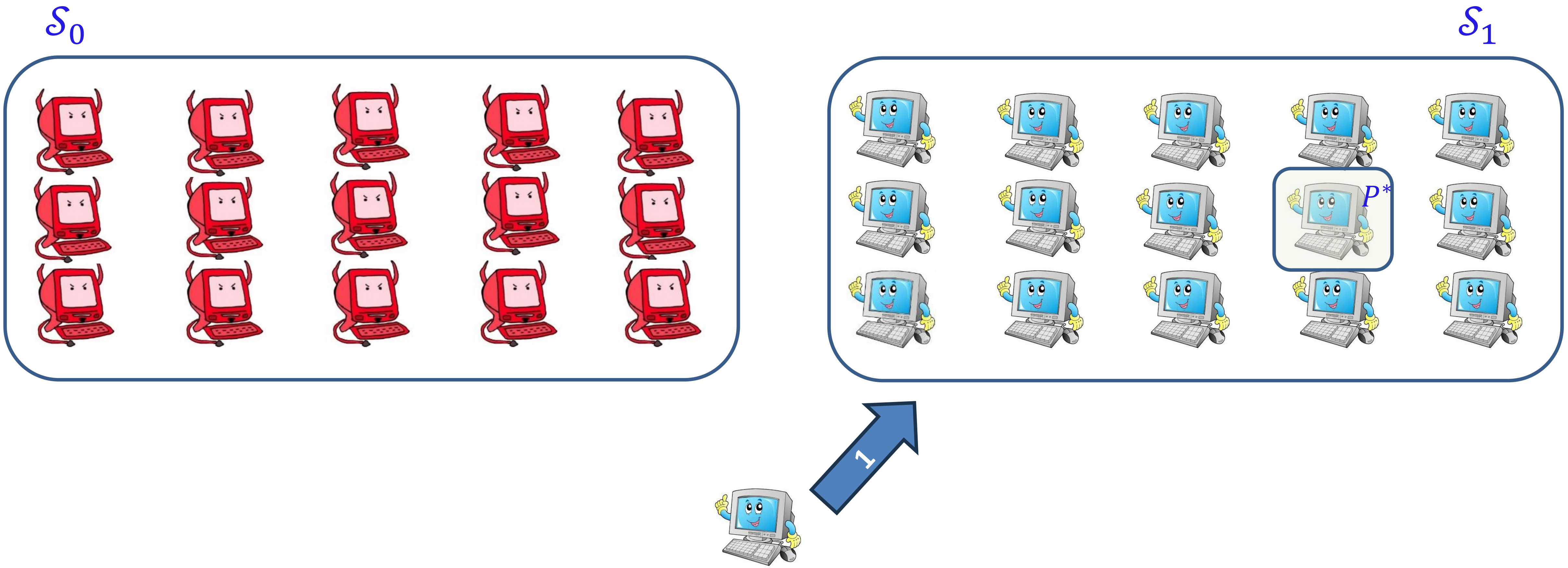
High-level idea for Thm 2

Lemma 1: if P^* and $\mathcal{X}$ do not communicate $\Rightarrow$ $\mathcal{X}$ outputs 0 and P^* outputs 1



High-level idea for Thm 2

Lemma 1: if P^* and $\mathcal{X}$ do not communicate $\Rightarrow$ $\mathcal{X}$ outputs 0 and P^* outputs 1

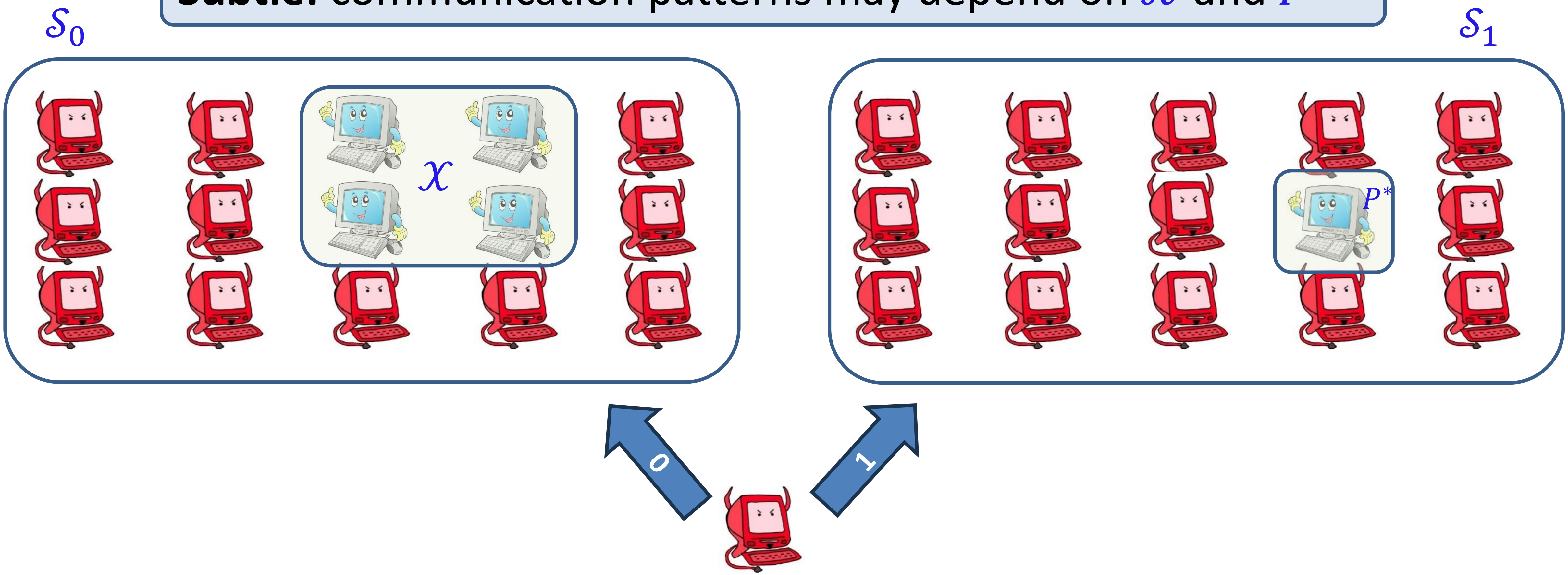


High-level idea for Thm 2

Lemma 1: if P^* and $\mathcal{X}$ do not communicate $\Rightarrow$ $\mathcal{X}$ outputs 0 and P^* outputs 1

Lemma 2: P^* and $\mathcal{X}$ do not communicate with noticeable probability

Subtle: communication patterns may depend on $\mathcal{X}$ and P^*



High-Level Overview

High-level idea for Thm 3

Thm 3: Let $0 < k < n/2$ and $t = n/2 + k$
Let π be a **weakly adaptive** t-secure broadcast and let P^* be a **non-sender**
Then, there exists an adversary that can force P^* to talk to k parties

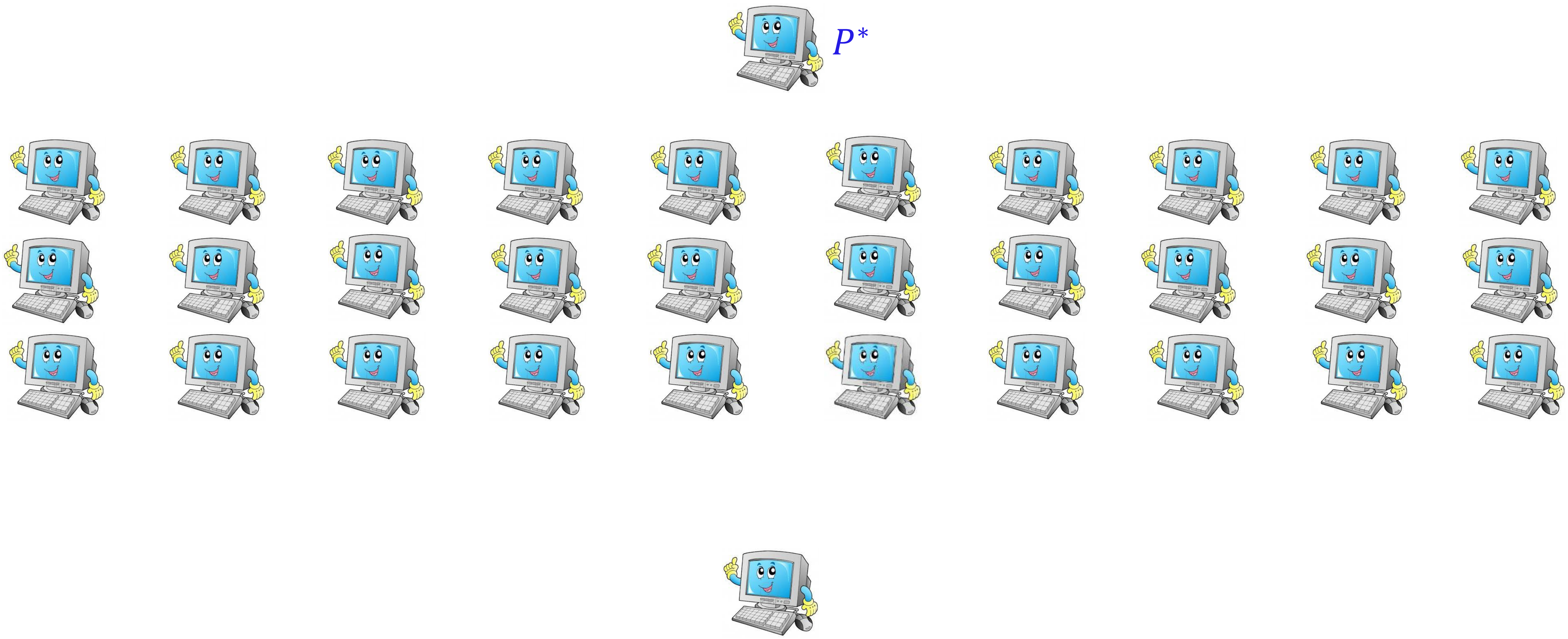
Challenge 1:
A linear number of honest parties so hard to isolate an honest receiver

Challenge 2:
Adv is weakly adaptive so every message sent by an honest party is delivered

Previous strategy doesn’t seem to work:
Cannot play two honest-looking executions toward two honest parties

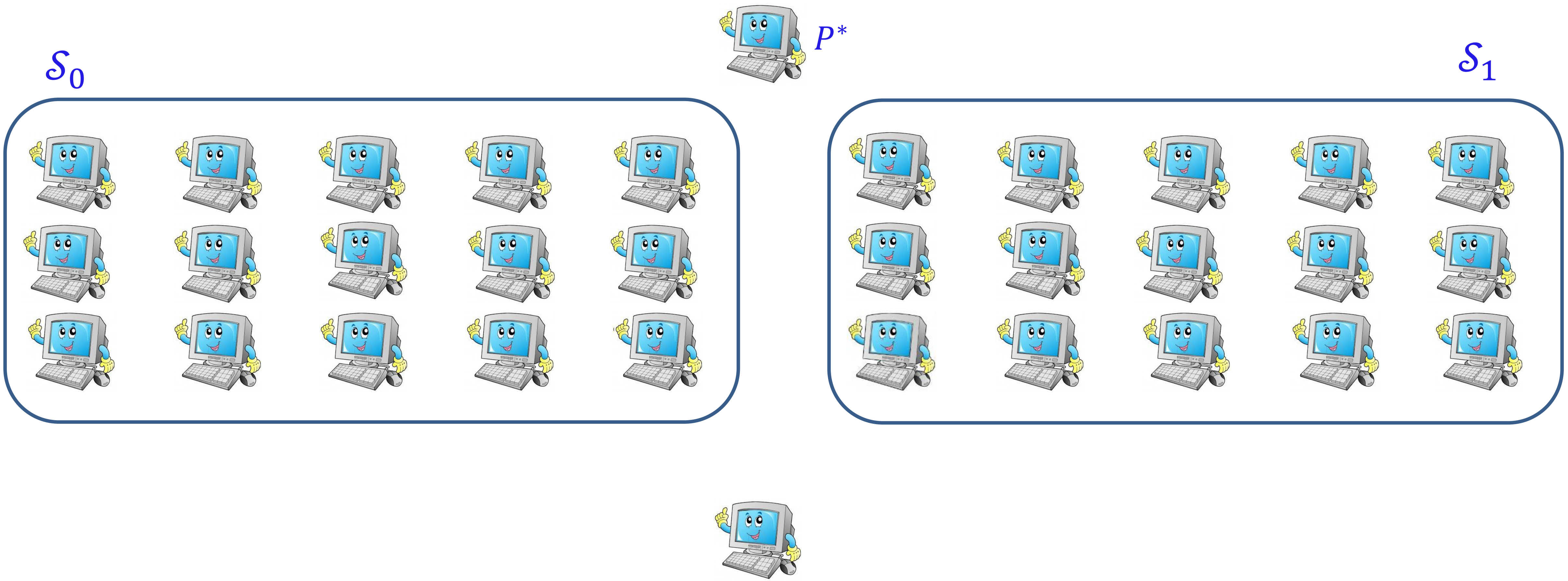
High-level idea for Thm 3

Thm 3: Let $0 < k < n/2$ and $t = n/2 + k$
Let π be a **weakly adaptive** t-secure broadcast and let P^* be a **non-sender**
Then, there exists an adversary that can force P^* to talk to k parties



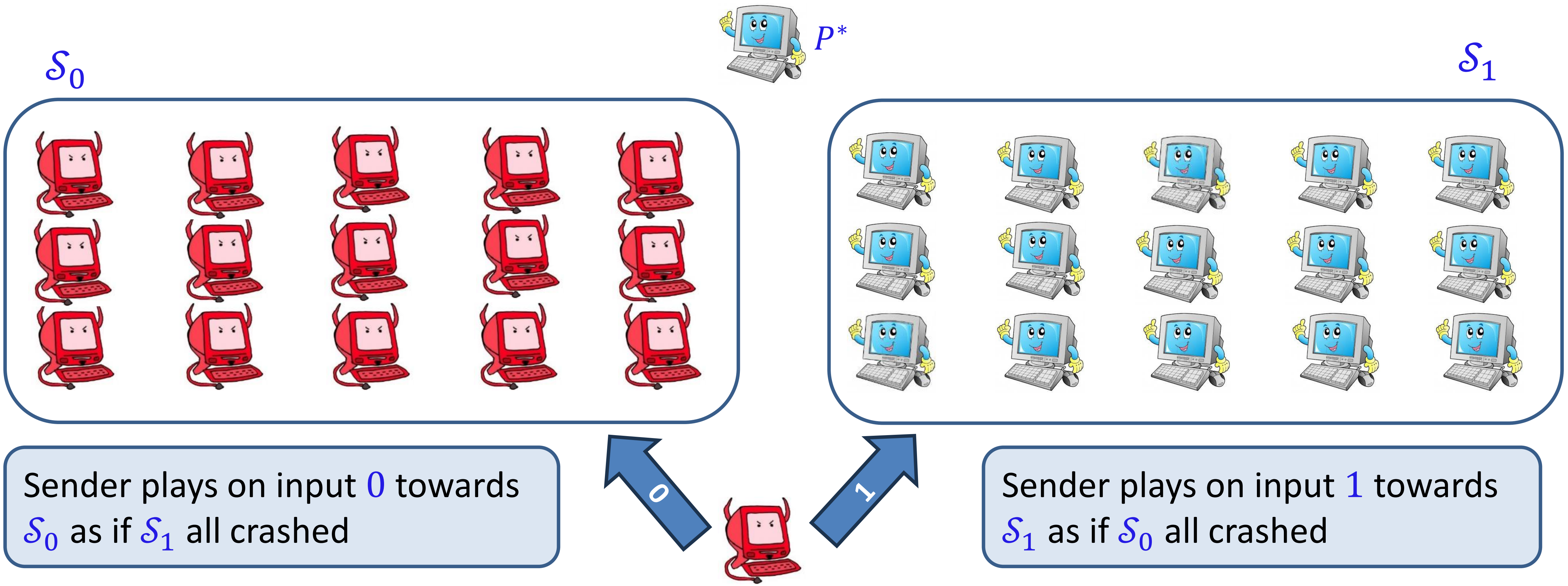
High-level idea for Thm 3

- Split all receivers but P^* to two subsets $\mathcal{S}_0$ and $\mathcal{S}_1$



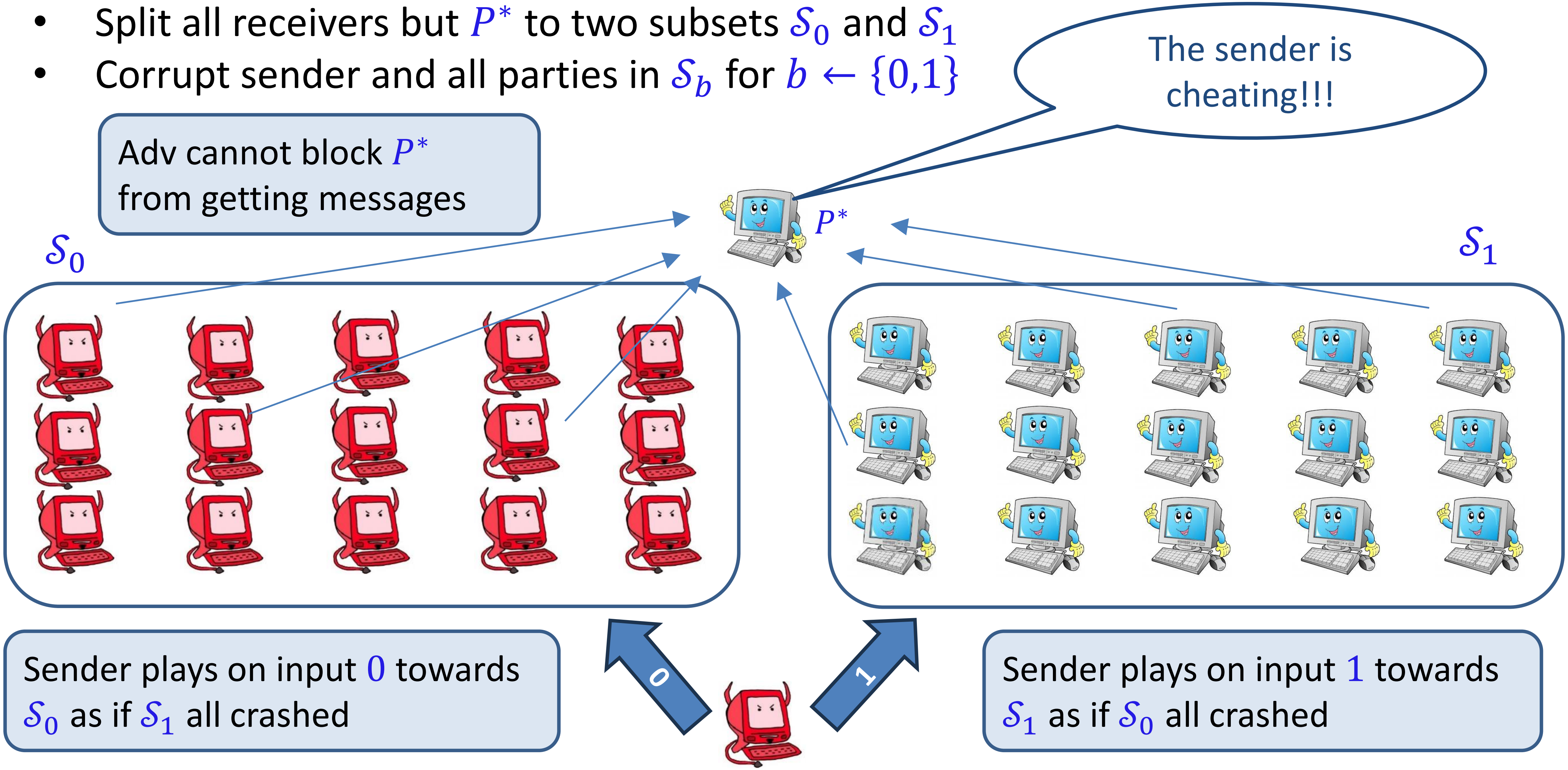
High-level idea for Thm 3

- Split all receivers but P^* to two subsets $\mathcal{S}_0$ and $\mathcal{S}_1$
- Corrupt sender and all parties in $\mathcal{S}_b$ for $b \leftarrow \{0,1\}$



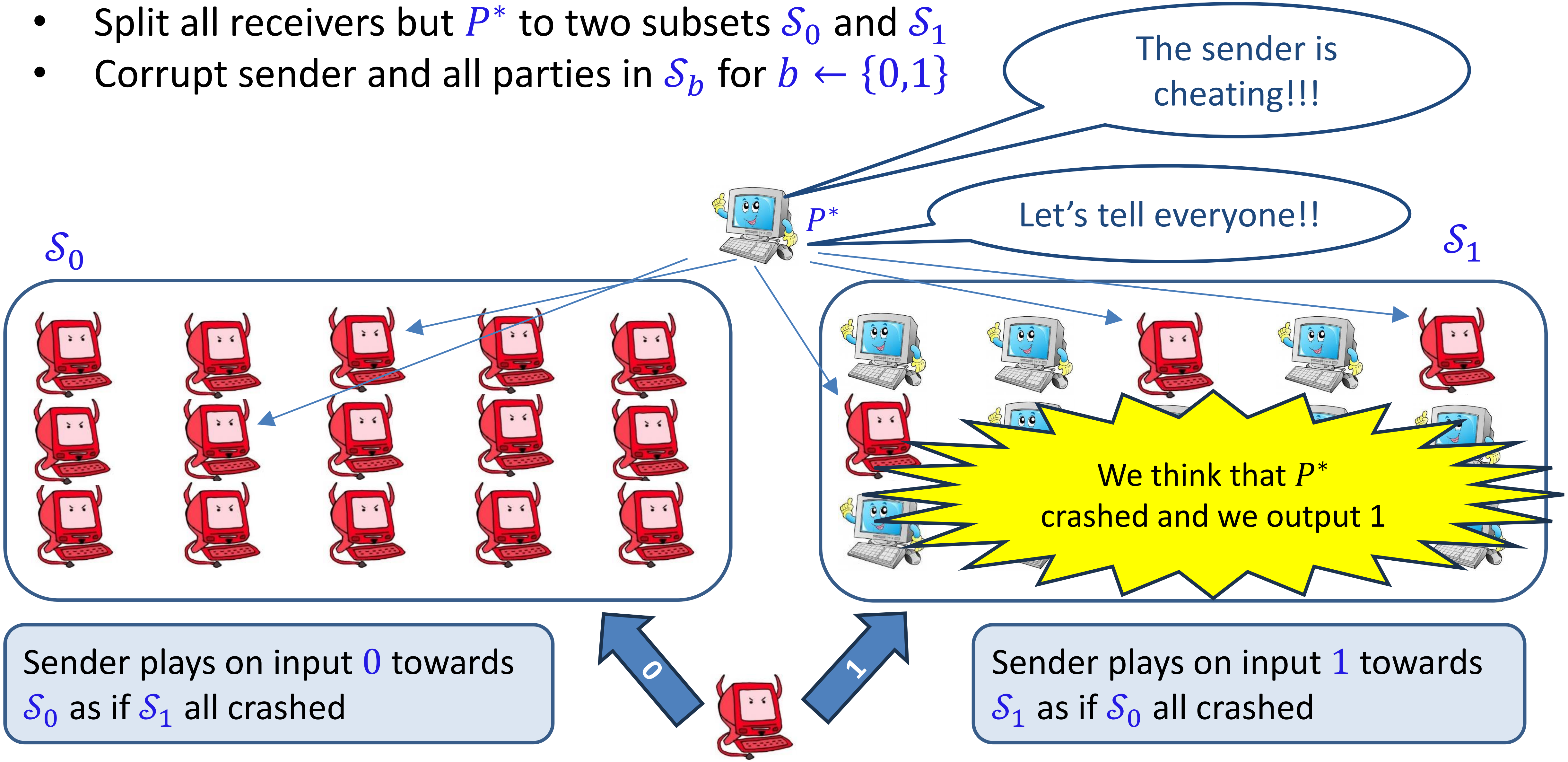
High-level idea for Thm 3

- Split all receivers but P^* to two subsets $\mathcal{S}_0$ and $\mathcal{S}_1$
- Corrupt sender and all parties in $\mathcal{S}_b$ for $b \leftarrow \{0,1\}$



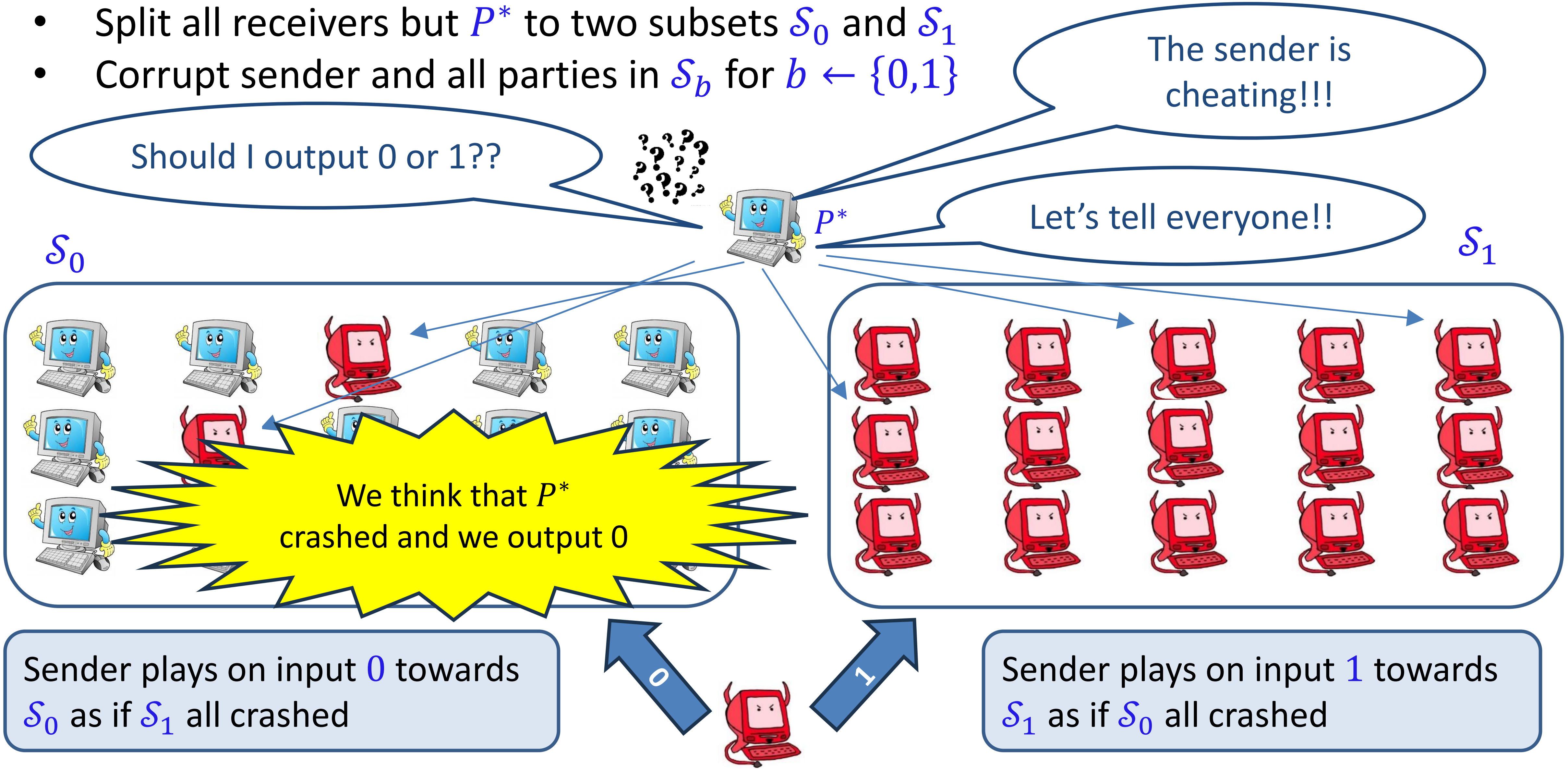
High-level idea for Thm 3

- Split all receivers but P^* to two subsets $\mathcal{S}_0$ and $\mathcal{S}_1$
- Corrupt sender and all parties in $\mathcal{S}_b$ for $b \leftarrow \{0,1\}$



High-level idea for Thm 3

- Split all receivers but P^* to two subsets $\mathcal{S}_0$ and $\mathcal{S}_1$
- Corrupt sender and all parties in $\mathcal{S}_b$ for $b \leftarrow \{0,1\}$



Main Results

	Setup	Resiliency (t)	Total comm	Locality (non-sender)	
Strongly adaptive	pki	$t < n$	$O(n^3)$	n	[DS'83]
	any	$t = \Theta(n)$	$\Omega(n^2)$	$\Omega(n)$	[ACDNPRS19]
Weakly adaptive	trusted pki	$(1-\epsilon) \cdot n$	$\tilde{O}(n^2)$	$O(n)$	[CPS'20]
	any	$\boldsymbol{t = n/2 + k}$		$\boldsymbol{> k}$	**Thm 3**
Static	any (deterministic)	$t = \Theta(n)$	$\Omega(n^2)$	$\Omega(n)$	[DR'85]
	pki	$(1-\epsilon) \cdot n$	$\tilde{O}(n^2)$	$\mathrm{polylog}(n)$	[TLP'22]
	trusted pki	$\boldsymbol{(1-\epsilon) \cdot n}$	$\boldsymbol{\tilde{O}(n)}$	$\boldsymbol{\mathrm{polylog}(n)}$	**Cor 1**
	any	$\boldsymbol{(1-\varphi(n)) \cdot n}$	$\boldsymbol{\Omega(n/\varphi(n))}$		**Thm 2**

Open Questions

Static corruptions: match the LB

- For $\varphi(n) = \frac{1}{\log^d n}$ we need $\Omega\left(n \cdot \log^d n\right)$ messages; DS requires $O(n^2)$
- For $\varphi(n) = \frac{1}{\sqrt{n}}$ we need $\Omega(n \cdot \sqrt{n}\,)$ messages; DS requires $O(n^2)$

Static corruptions: sub-quadratic broadcast from weaker assumptions (currently need trusted pki + VRF)

Weakly adaptive: is there sub-quadratic broadcast?

Understand the limitations of cryptography in distributed systems

Thank You