Communication Lower Bounds for Cryptographic Broadcast Protocols

Erica Blum: University of Maryland

Elette Boyle: Reichman University & NTT Research

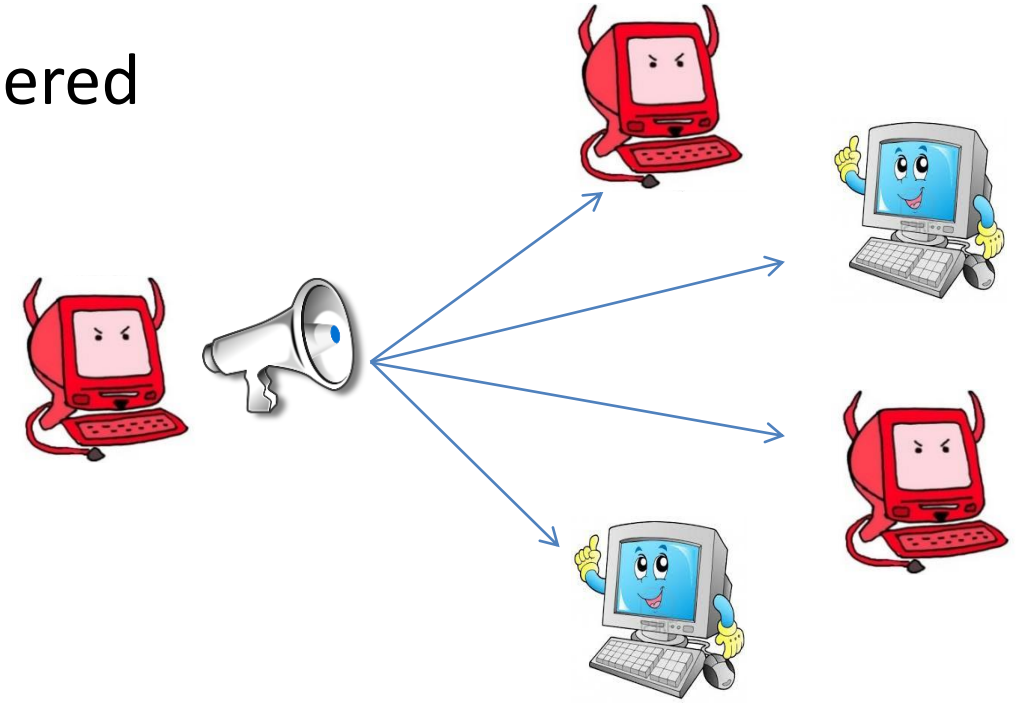
Ran Cohen: Reichman University

Chen-Da Liu-Zhang: HSLU & Web3 Foundation

Broadcast Protocols

A broadcast protocol with sender S is considered secure if it satisfies the following properties:

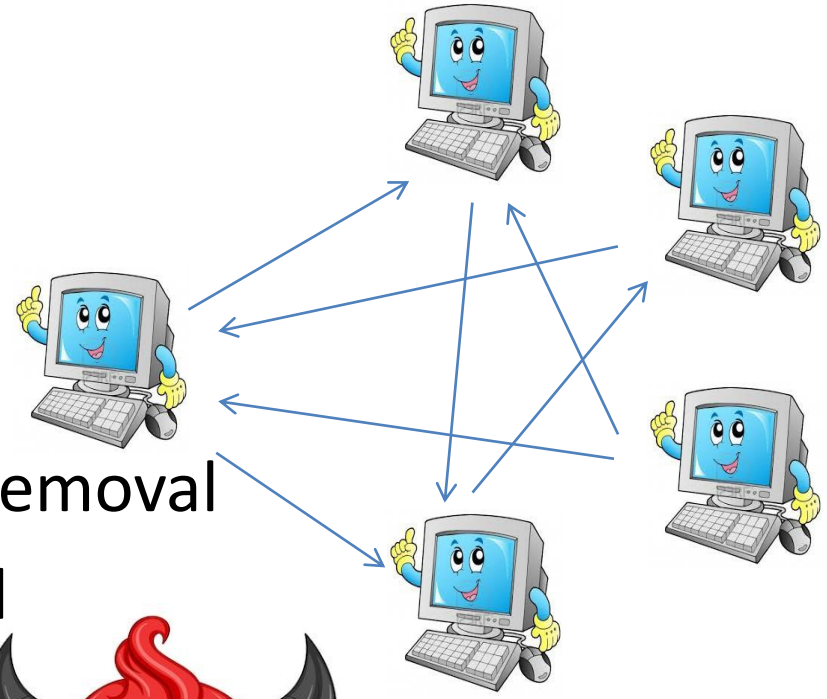
- Validity: if the sender is honest and has input x, then $y = x$
- Agreement: every honest party outputs the same value y



Byzantine agreement: a closely related multi-input version

Setting

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



static

weakly adaptive

strongly adaptive

Playground of feasibility & impossibility

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

Deterministic broadcast protocols

Not scalable

Let's lower our expectations

Clean & elegant results

Playground of feasibility & impossibility

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

Randomness & Cryptography

Security with high probability

Security wrt PPT adversaries

Playground of feasibility & impossibility

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

✓ [Ben-Or'83] [Rabin'83] async BA

✓ [DS'83] PKI + Sig $t < n$

✓ [many] exp constant for $t = \Theta(n)$

These bounds held for >20 years

Playground of feasibility & impossibility

Feasibility	Resiliency	Rounds	Connectivity	Communication
✗ async	✓ sync	✗ $t \geq n/3$	✓ $t < n/3$	✗ $< t+1$	✓ $\geq t+1$	✗ $< 2t+1$	✓ $\geq 2t+1$	✗ $o(n^2)$	✓ $\Theta(n^2)$
✓ [Ben-Or'83] [Rabin'83] async BA	✓ [DS'83] PKI + Sig $t < n$	✓ [many] exp constant for $t = \Theta(n)$		

Communication complexity (partial)

Honest majority

- [KS'09] statically secure BA with $o(n^2)$ communication and $o(n)$ connectivity
- [BGT'13] used cryptography for $\mathrm{polylog}(n)$ locality (max degree in induced communication graph)
- [BCG'21] balanced BA with $\tilde{O}(n)$ comm. ($\mathrm{polylog}(n)$ bits per party)
- [Micali'17] & [ACDNPRS'19] unbalanced BA with $\tilde{O}(n)$ comm. against weakly adaptive
- **[ACDNPRS'19] security wrt t strongly-adaptive $\Rightarrow \Omega(t^2)$ messages**

Communication complexity (partial)

Dishonest majority

- All communication-efficient broadcast based on [DS'83] $O(n^2)$ messages and $O(n^3)$ communication (bare pki + sig)
- [CPS'20] for $t = \Theta(n)$ constructed broadcast with $\tilde{O}(n^2)$ communication against weakly adaptive (trusted pki + cryptography)
- [TLP'22] for $t = \Theta(n)$ constructed broadcast with $\tilde{O}(n^2)$ communication and $\tilde{O}(1)$ locality against static adaptive (bare pki + sig)

Starting point

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

Starting point

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

Starting point

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

Starting point

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

No lower bounds for randomized broadcast for static/weakly adaptive

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

Yes! Under strong assumptions

- [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:

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

Can we do better?

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

Thm 2: Let $\epsilon(n) \in o(1)$ and $t = \left(1 - \epsilon(n)\right) \cdot n$
For any (statically) t-secure broadcast, the message complexity is

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

Examples:

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

Can we do better (#2)?

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

Recall that Thm 1 guarantees $\tilde{O}(1)$ 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 P_{i^*} be a non-sender, and let π be a weakly adaptive t-secure broadcast protocol
Then, there exists an adversary that can force P_{i^*} 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

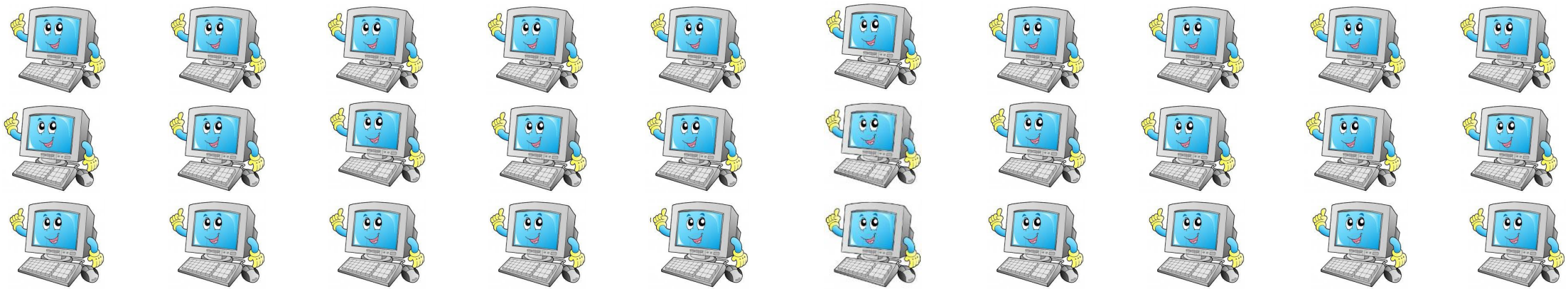
	Setup	Resiliency (t)	Total comm	Locality (non-sender)	
Strongly adaptive	bare pki	$t < n$	$O(n^3)$	n	[DS'83]
	any	$\Theta(n)$	$\Omega(n^2)$	$\Omega(n)$	[ACDNPRS19]
Weakly adaptive	trusted pki	$\Theta(n)$	$\tilde{O}(n^2)$	$O(n)$	[CPS'20]
	any	$\boldsymbol{n/2 + k}$		$> \boldsymbol{k}$	**Thm 3**
Static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

High-level idea for Thm 2

Thm 2: Let $\epsilon(n) \in o(1)$ and $t = \left(1 - \epsilon(n)\right) \cdot n$

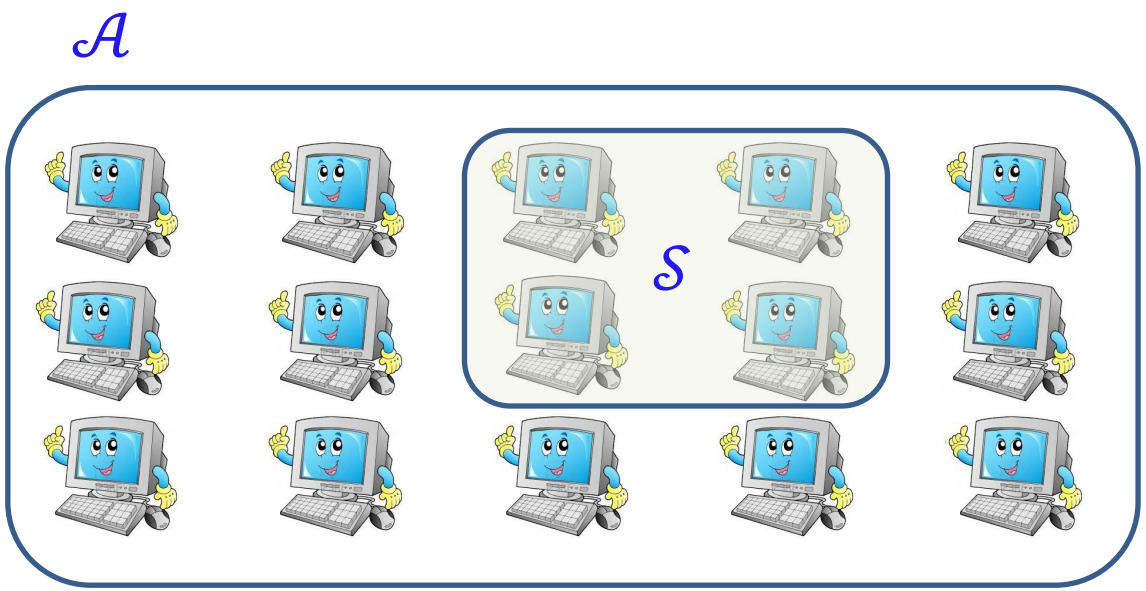
For any (statically) t-secure broadcast, the message complexity is

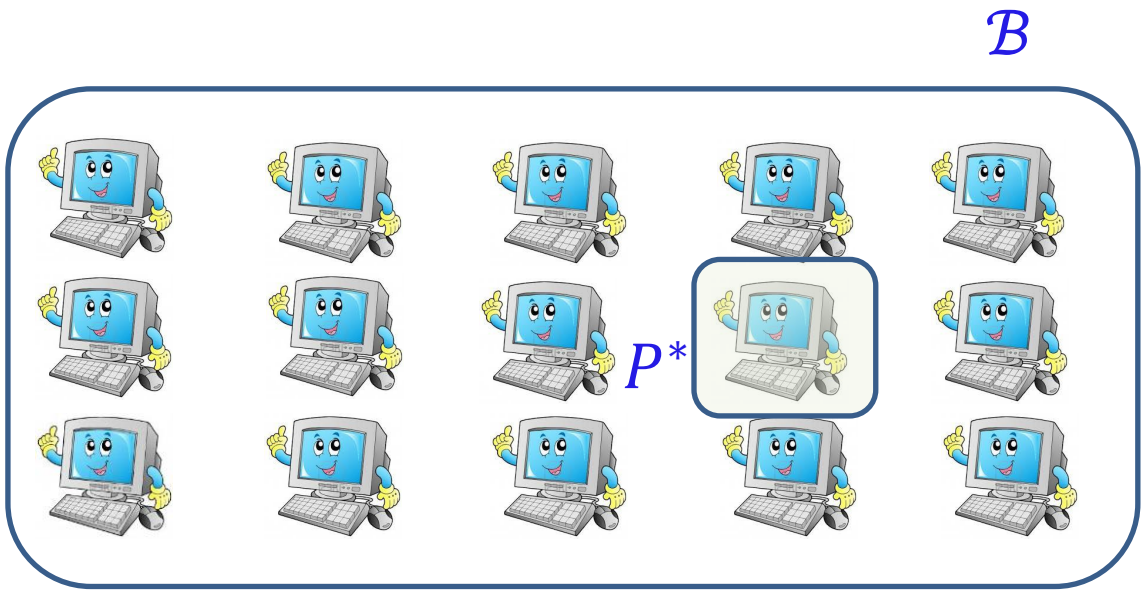
$$\Omega\left(n \cdot \frac{1}{\epsilon(n)}\right)$$



High-level idea for Thm 2

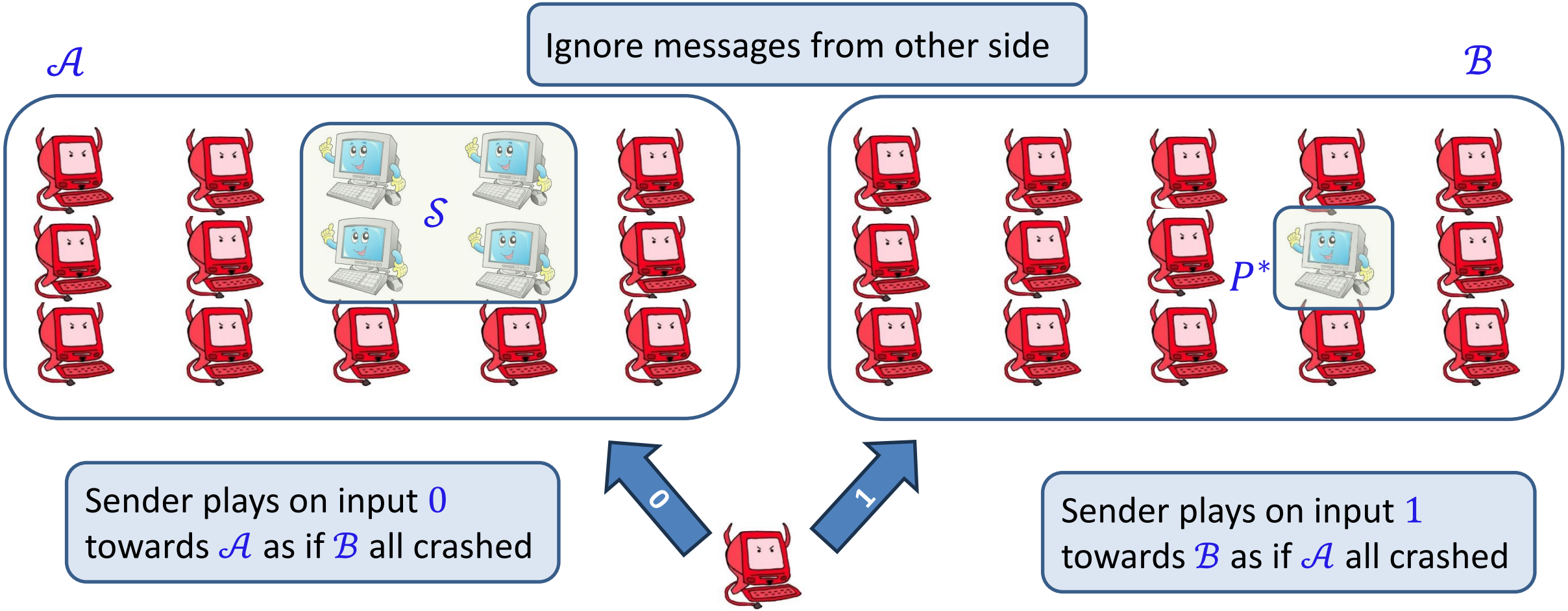
- Split all receivers to two subsets $\mathcal{A}$ and $\mathcal{B}$
- Choose set $\mathcal{S} \subseteq \mathcal{A}$ of size $\epsilon(n) \cdot n - 1$ and a party $P^* \in \mathcal{B}$ and corrupt all others





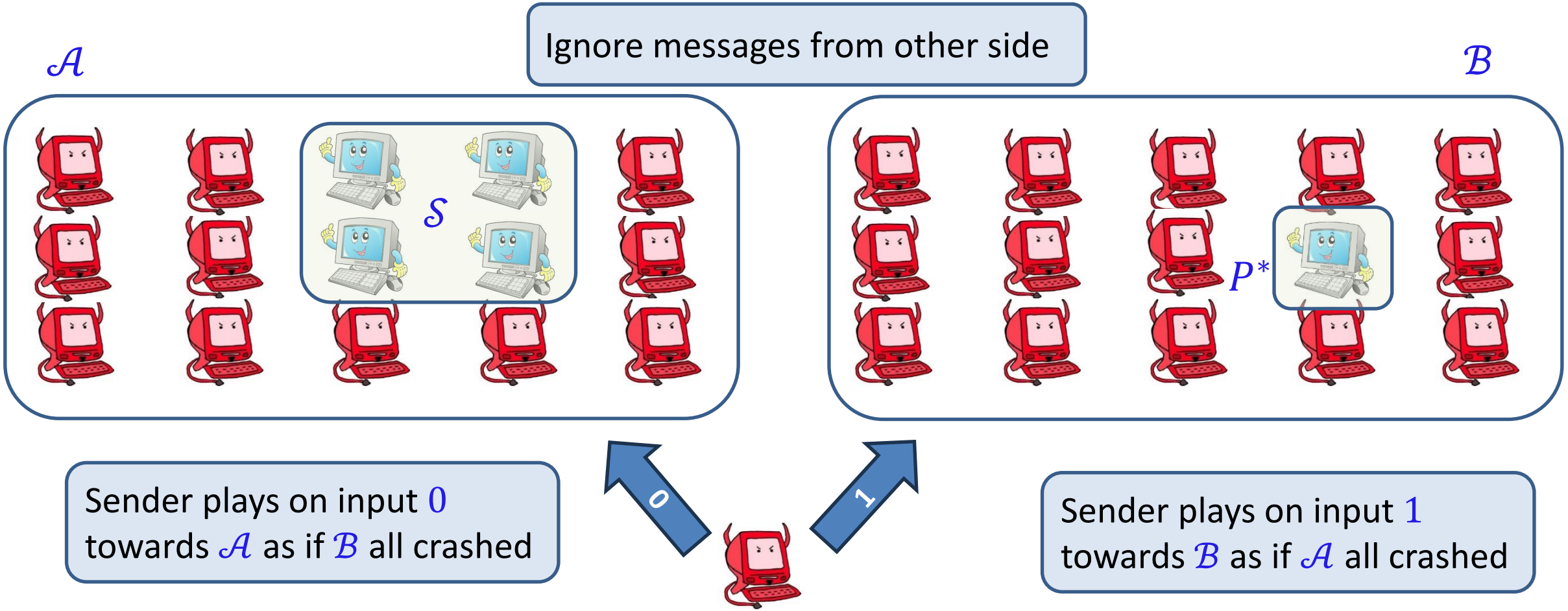
High-level idea for Thm 2

- Split all receivers to two subsets $\mathcal{A}$ and $\mathcal{B}$
- Choose set $\mathcal{S} \subseteq \mathcal{A}$ of size $\epsilon(n) \cdot n - 1$ and a party $P^* \in \mathcal{B}$ and corrupt all others



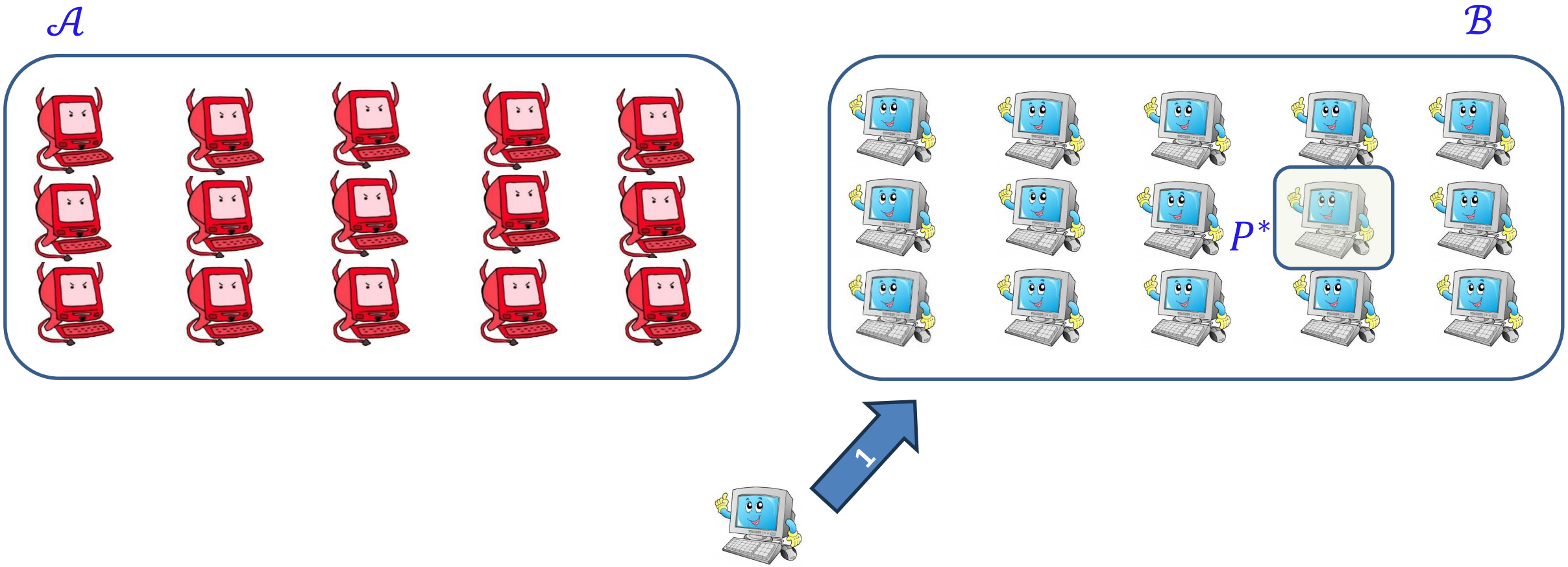
High-level idea for Thm 2

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



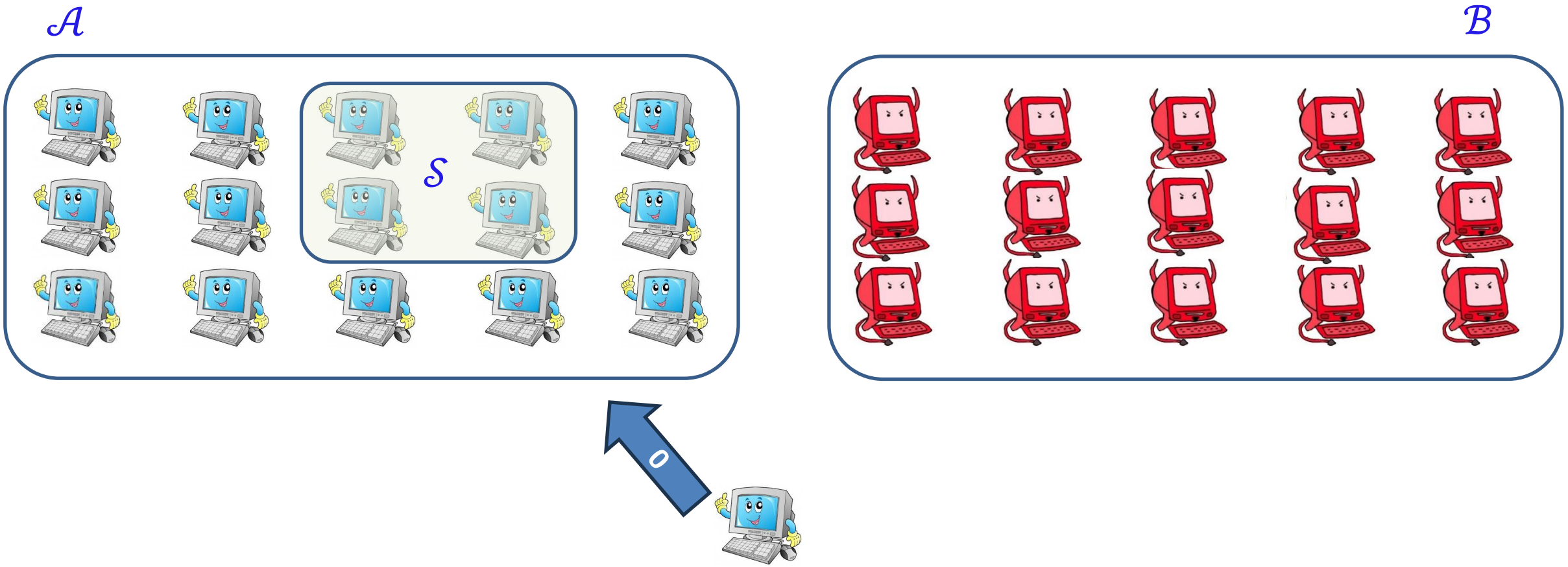
High-level idea for Thm 2

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



High-level idea for Thm 2

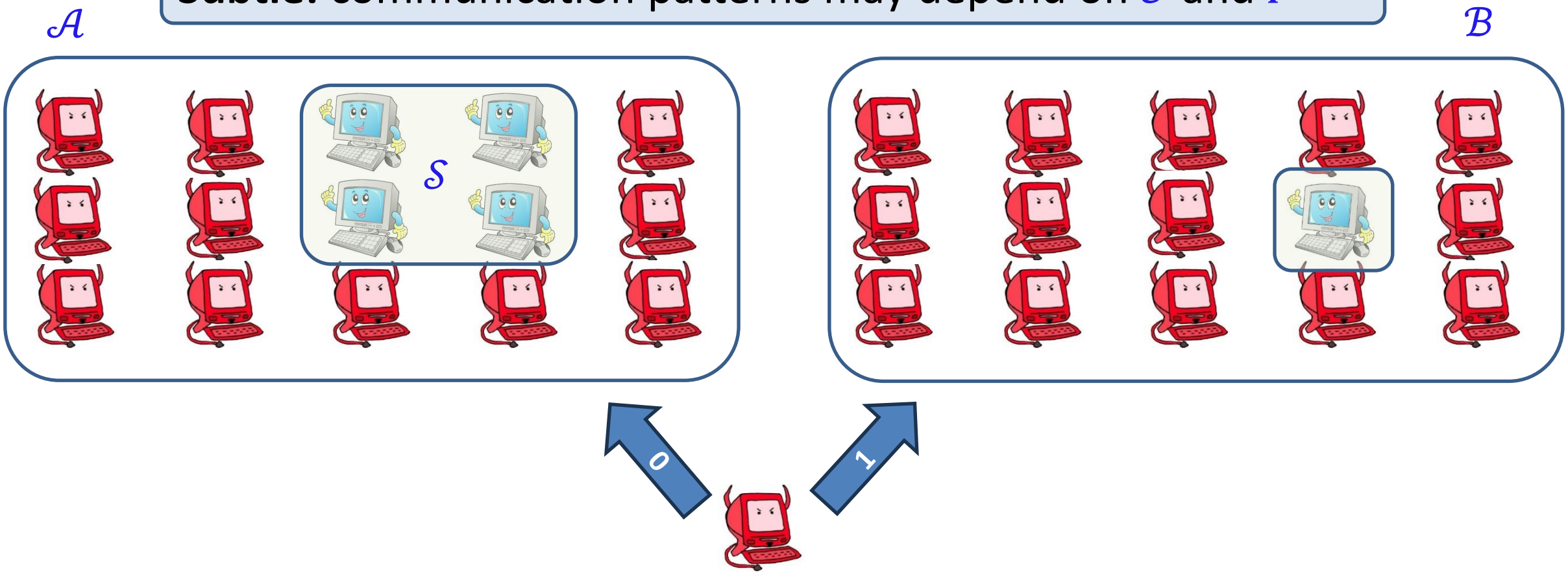
- **Lemma 1:** if P^* and $\mathcal{S}$ do not communicate $\Rightarrow$ $\mathcal{S}$ outputs 0 and P^* outputs 1



High-level idea for Thm 2

- **Lemma 1:** if P^* and $\mathcal{S}$ do not communicate $\Rightarrow$ $\mathcal{S}$ outputs 0 and P^* outputs 1
- **Lemma 2:** P^* and $\mathcal{S}$ do not communicate with noticeable probability

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



Open Questions

Static: match the LB (e.g., for $\epsilon(n) = \log^{-d} n$ and $\epsilon(n) = \sqrt{n}$)

Static: sub-quadratic broadcast from weaker assumptions

Weakly adaptive: is there sub-quadratic broadcast?

Understand the limitations of cryptography in distributed systems

Thank You