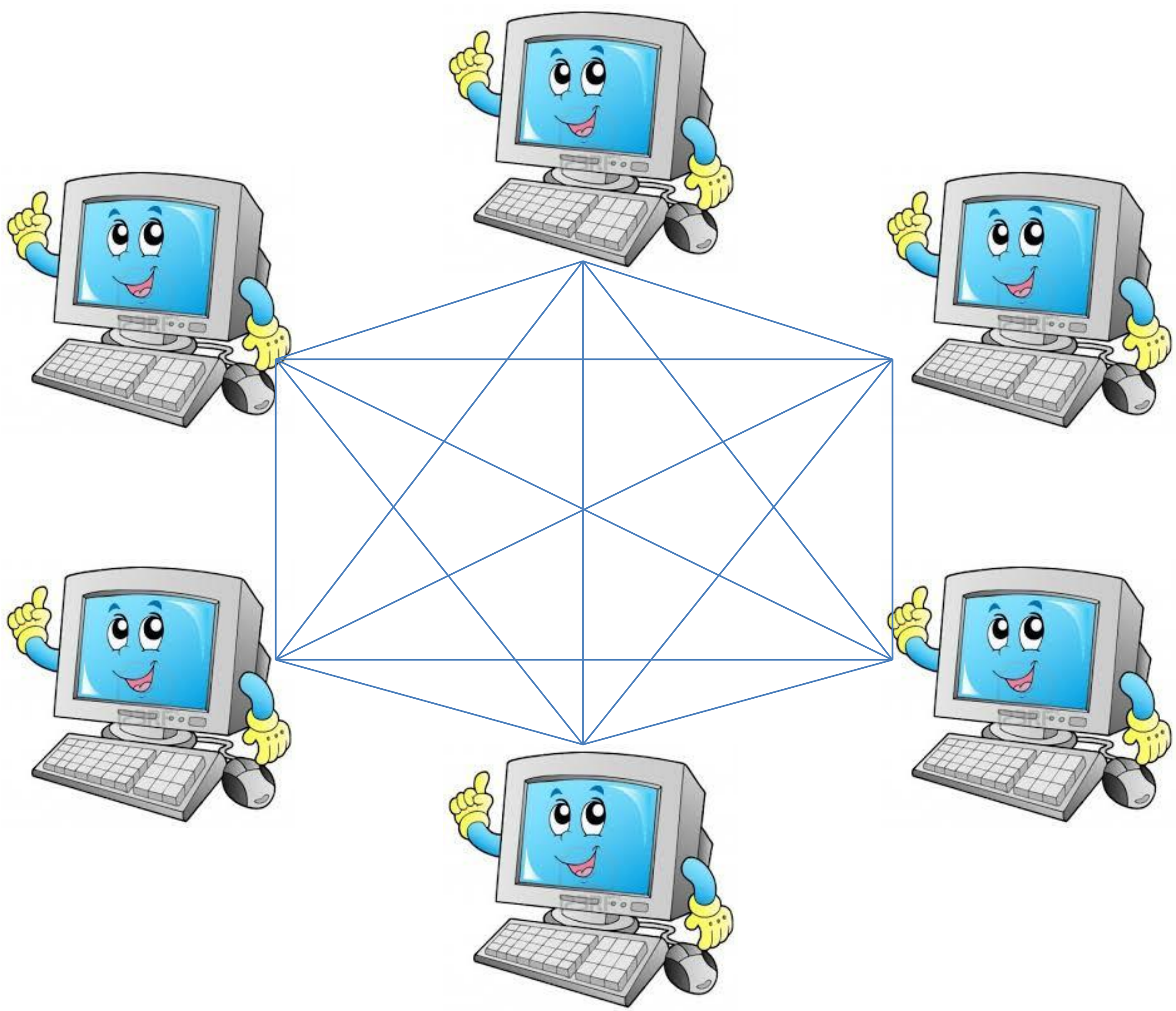
# Characterization of Secure Multiparty Computation Without Broadcast

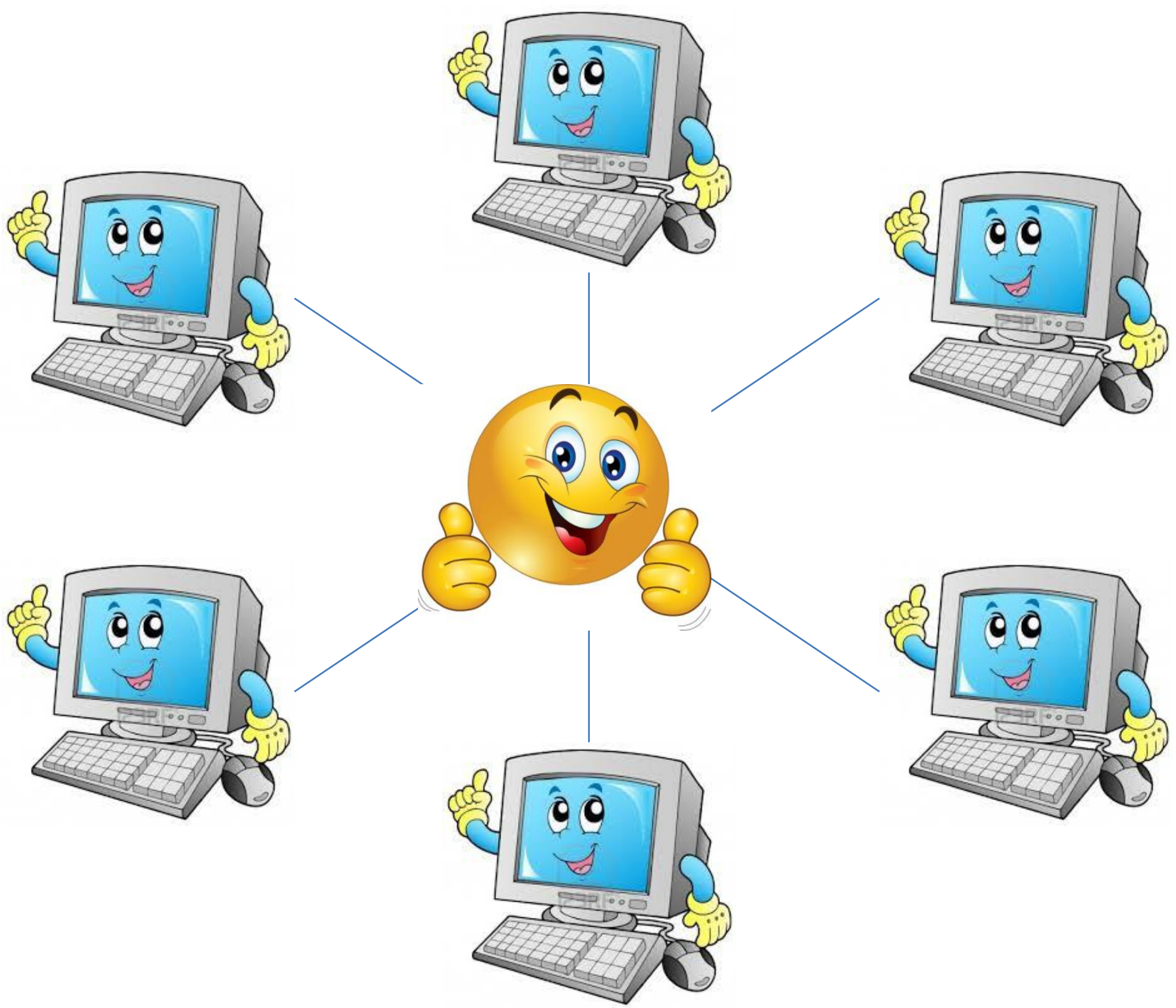
[TCC'16]


Ran Cohen (Bar-Ilan University)
Iftach Haitner (Tel-Aviv University)
Eran Omri (Ariel University)
Lior Rotem (Hebrew University)

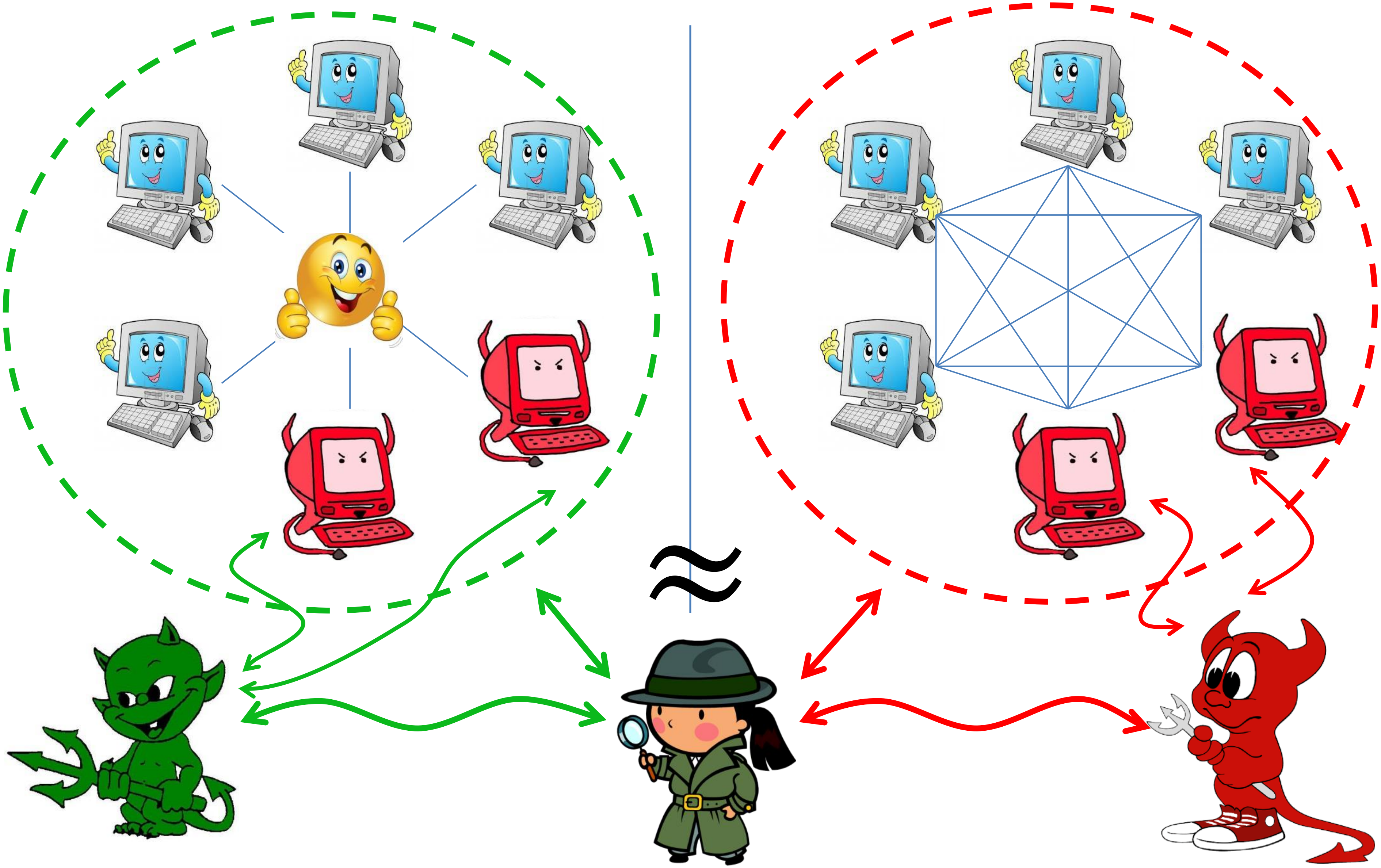
# Secure multiparty computation



# Ideal world

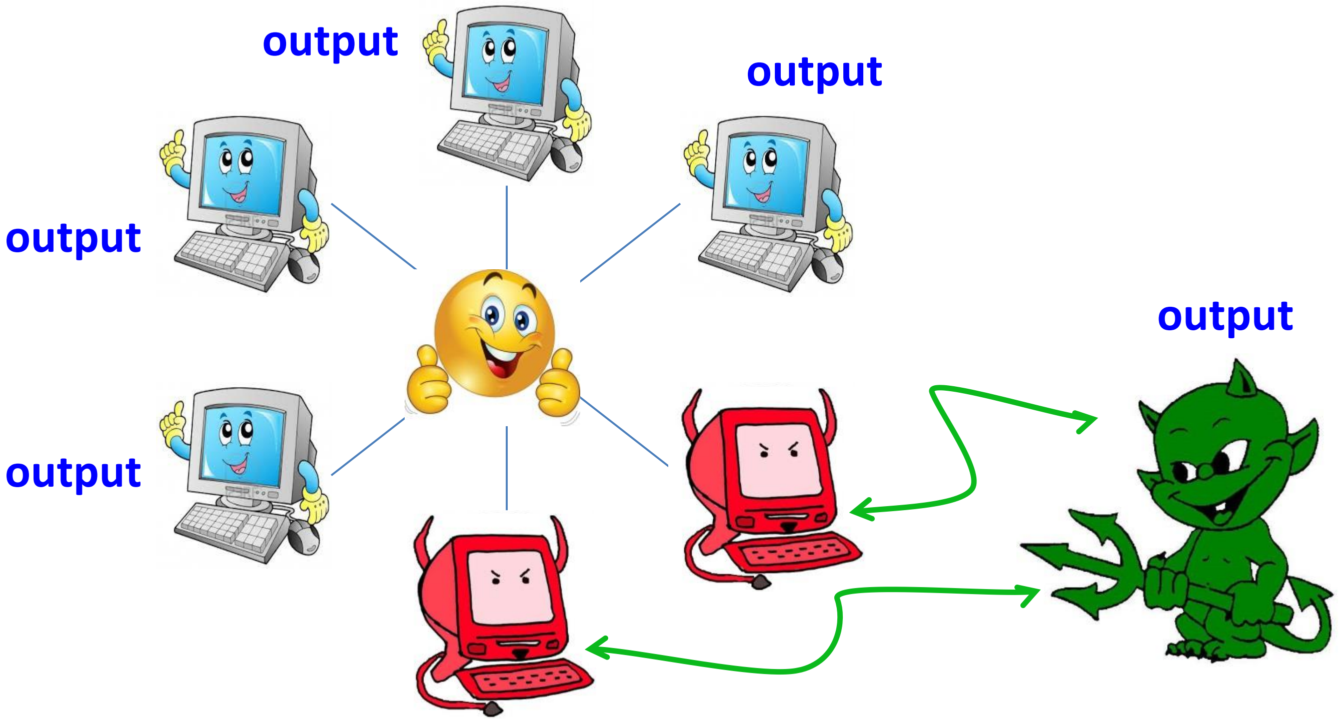


# Simulation-based security



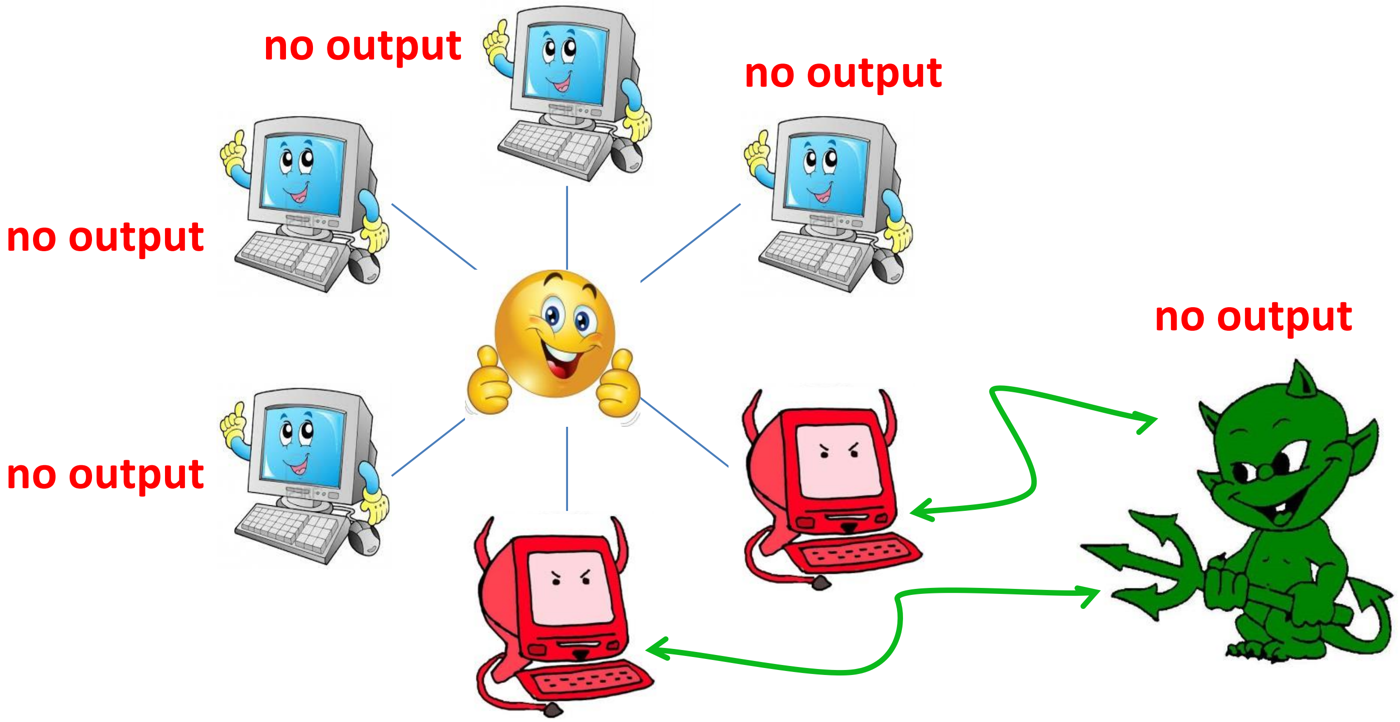
# Notions of security

- Full security: **no abort**



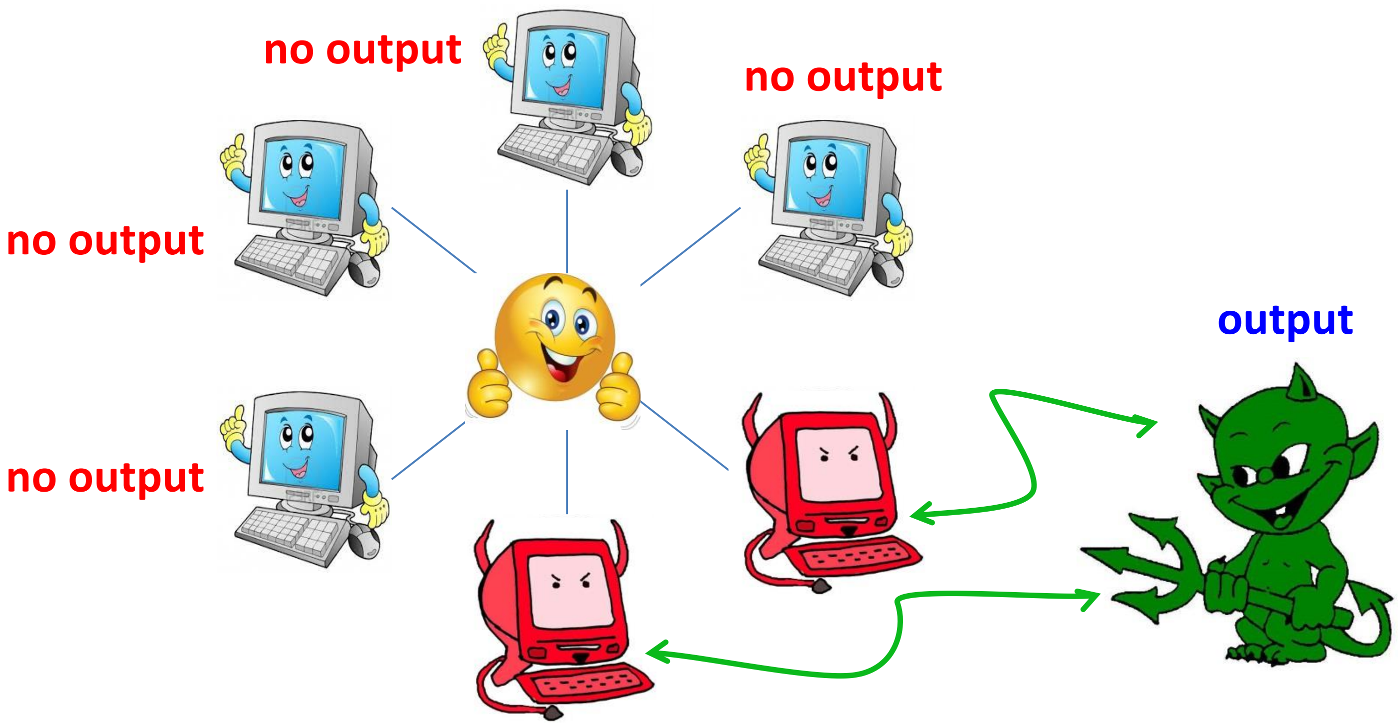
# Notions of security

- Full security: **no abort**
- Fairness: **abort before** obtaining output



# Notions of security

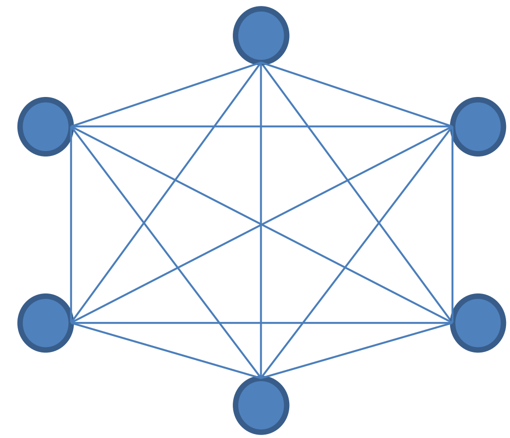
- Full security: **no abort**
- Fairness: **abort before** obtaining output
- Security with abort: **abort after** obtaining output



# Communication Model

# Communication model

- Point-to-point (P2P) model
  - Secure channels
  - Authenticated channels



- Broadcast model
  - Additional broadcast channel

# Settings

$n$ – # of parties
$t$ – (bound on) # of corrupted parties

$n \geq 3, t \geq n/3$

Full security in the P2P model (without setup)

Static malicious adversaries

Stand-alone security

1) Honest majority:
   - All-powerful adversaries (statistical security)
   - Secure channels
2) No honest majority:
   - Efficient adversaries (computational security)
   - Authenticated channels

# Known results (w/o setup)

**Broadcast**

$t < n/2$

- $\forall f$ full security [RB'89, CDDHR'99]

$t \geq n/2$

- $\exists f$ without fairness [Cleve'86]

$t < n$ $(*)$

- $\forall f$ security with abort [GMW'87]
- $\exists f$ with full security [GK'09]
- Full security $\Leftrightarrow$ fairness [CL'14]

$(*)$ assuming OT

**Point-to-Point**

$t < n/3$

- $\forall f$ full security [BGW'88, CCD'88]

$t \geq n/3$

- $\exists f$ without full security [PSL'80,CL'14]

$t < n/2$

- $\forall f$ fairness [FGMR'02]

$t < n$ $(*)$

- $\forall f$ security with abort [FGHHS'02]
- $\exists f$ with full security [FGHHS'02 ,CL'14]

# Question #1

In the P2P model, for $n \geq 3$, $t \geq n/3$, and **w/o** setup, which functions can be computed with full security?

| | $t < n/2$ | $t < n$ |
|---|---|---|
| Byzantine agreement | ✗ | ✗ |
| Three-party majority | ✗ | ✗ |
| Weak Byzantine agreement | ✓ | ✓ |
| Boolean OR | ✓ | ✓ |
| Boolean XOR | ? | ✗ |
| $\max(x_1, \ldots, x_n)$ over $\mathbb{Z}$ | ? | ? |

- Open even for $n = 3$ and $t = 1$

# Our result #1 - full security

**Def:** $f$ is **$k$-dominated**, if $\exists$ efficiently computable $y^*$, s.t. **every** $k$ inputs can **determine** the output $y^*$

**Example:** Boolean OR is $1$-dominated (with $y^* = 1$)

$f(x_1, \ldots, x_n) = (y, \ldots, y)$

**Theorem 1:** Let $n \geq 3$ and $f$ symmetric $n$-party functionality

1) Honest majority ($n/3 \leq t < n/2$ ):

$f$ has $t$-full-security (in P2P model) $\Leftrightarrow$ $f$ is $(n-2t)$-dominated

2) No honest majority ($n/2 \leq t < n$):

$f$ has $t$-full-security (in P2P model) $\Rightarrow$
1) $f$ is $1$-dominated
2) $f$ has $t$-full-security (with broadcast)

1) $f$ is $1$-dominated; 2) $f$ has $t$-full-security (with broadcast) $\xRightarrow{\text{OWF}}$ $f$ has $t$-full-security (in P2P model)

# Consequences (1)

| | $t < n/2$ | $t < n$ |
|---|---|---|
| Byzantine agreement | ✗ | ✗ |
| Three-party majority | ✗ | ✗ |
| Weak Byzantine agreement | ✓ | ✓ |
| Boolean OR | ✓ | ✓ |
| Boolean XOR | ✗ | ✗ |
| $\max(x_1, \ldots, x_n)$ over $\mathbb{Z}$ | ✗ | ✗ |

# Consequences (2)

Consider the $2$-dominated function

$$f(x_1, \ldots, x_6) = 1 \Leftrightarrow \exists \text{ at least two non-zero inputs}$$

- Honest majority ($t = 2$)
  $f$ has full security ($n - 2t = 6 - 4 = 2$)

- No honest majority ($t \geq 3$)
  $f$ does not have full security (not $1$-dominated)

# Our result #2 - coin flipping (CF)

Theorem 1 $\Rightarrow$ **No** fully secure CF with $t \geq n/3$

**Def:** **$\alpha$-bias coin flipping.** All honest parties agree on **common** bit that is $\boldsymbol{\alpha}$**-close** to uniform

**Broadcast model:** [Cleve'86]

$\exists 1/p$-bias CF secure $\forall t < n$, for every poly $p$

**Theorem 2:** Let $n \geq 3$ and $t \geq n/3$

**No** $\alpha$-bias CF in P2P model, for <u>any</u> $\alpha < 1/2$

**Corollary:**

Non-trivial $3$-party CF requires broadcast

# Main Lemma (lower bound)

**Def**: $\pi$ is ***t*-consistent**, if **all** honest parties output **same** value, facing $\leq t$ corrupted parties

**Lemma**: Let $t \geq n/3$ and $s = \begin{cases} n - 2t & ; t < n/2 \\ 1 & ; t \geq n/2 \end{cases}$

Let $\pi$ be $t$-consistent in the P2P model

Then $\exists$ PPT $\mathcal{A}$ that by controlling (any) subset $I$ of $s$ parties, can:

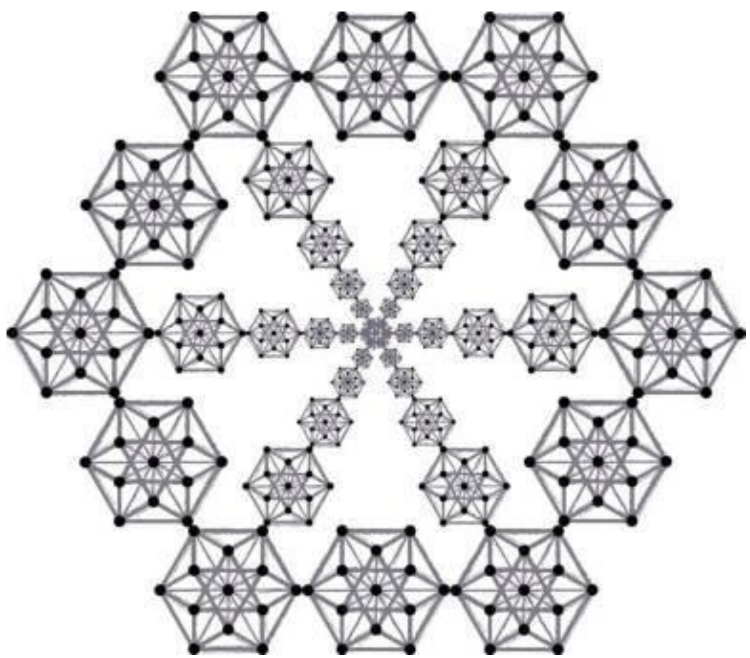
1) **Announce** a value $y_I^*$
2) **Force all** honest parties to output $y_I^*$

* Holds also for **expected** poly-time protocols

# The Attack

## Variant of [Fischer-Lynch-Merritt ’85]

## “Hexagon argument”



# Main Lemma ($n = 3, t = 1$)

**Lemma**: Let $\pi$ be $1$-consistent $3$-party protocol in the P2P model

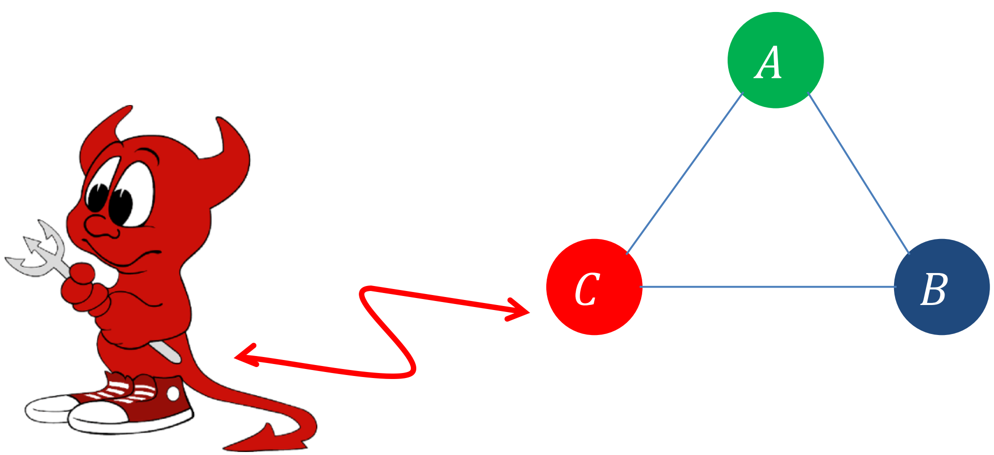
Then $\exists$ PPT $\mathcal{A}$ that by controlling **any party** $P_i$ can:

1) **Announce** value $y_i^*$
2) **Force all** honest parties to output $y_i^*$

# Proof

Let $\pi = (A, B, C)$ be a $3$-party, $q$-round, $1$-consistent protocol in the P2P model

Assume (for simplicity) that parties are **input-less**, and use $\kappa$ random coins

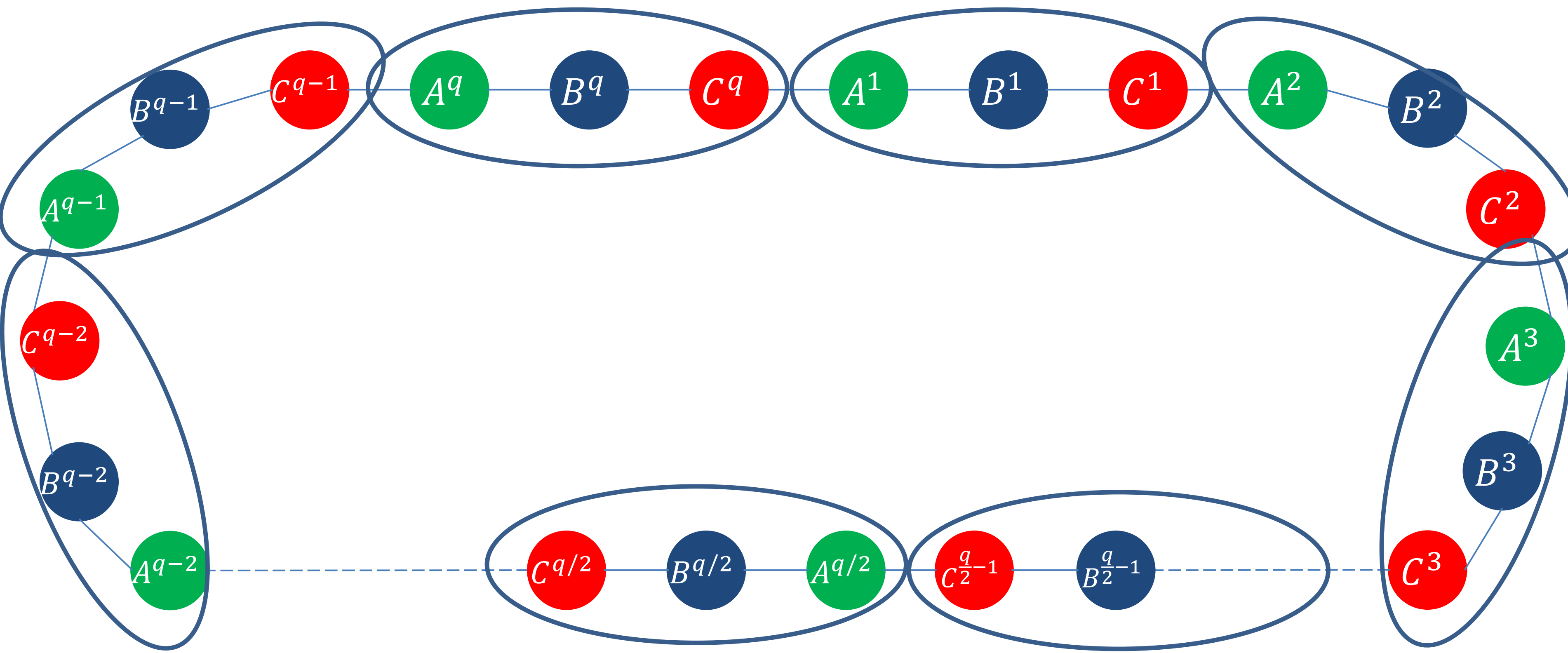


# The ring system $S$

$S = (A^1, B^1, C^1, \dots, A^q, B^q, C^q)$ – $q$ copies of $\pi$

$S(\boldsymbol{r})$ denotes the execution of $S$ on

$$\boldsymbol{r} = \left(r_A^1, r_B^1, r_C^1, \dots, r_A^q, r_B^q, r_C^q\right) \in (\{0,1\}^\kappa)^{3q}$$

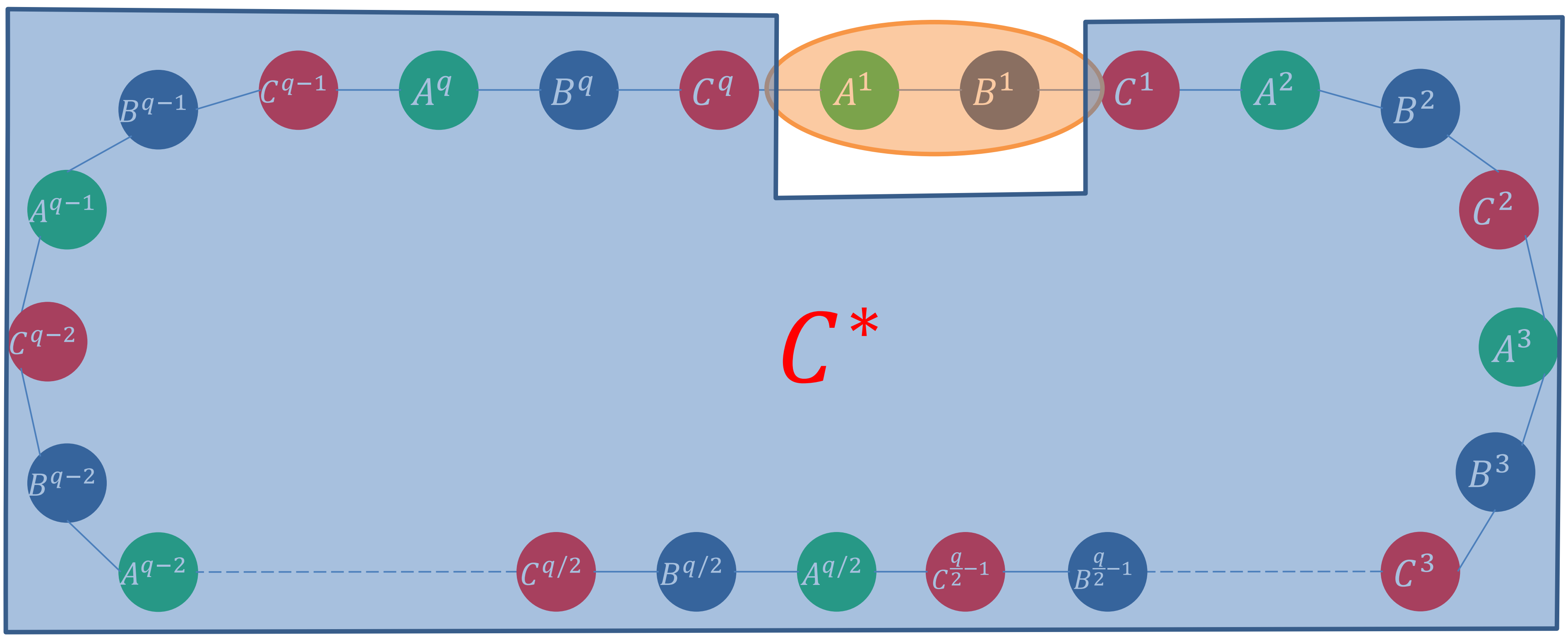


# Claim 1: $S(\boldsymbol{r})$ is monochromatic

View of $(A^1, B^1)$ in $S(\boldsymbol{r})$, for $\boldsymbol{r} \leftarrow (\{0,1\}^\kappa)^{3q}$, is view of $(A, B)$ in a **random** interaction of $(A, B, C^*)$ with some $C^*$

$\pi$ is $1$-consistent $\Rightarrow$ $A^1$ and $B^1$ output same value

$\Rightarrow$ each pair of adjacent parties output the same value

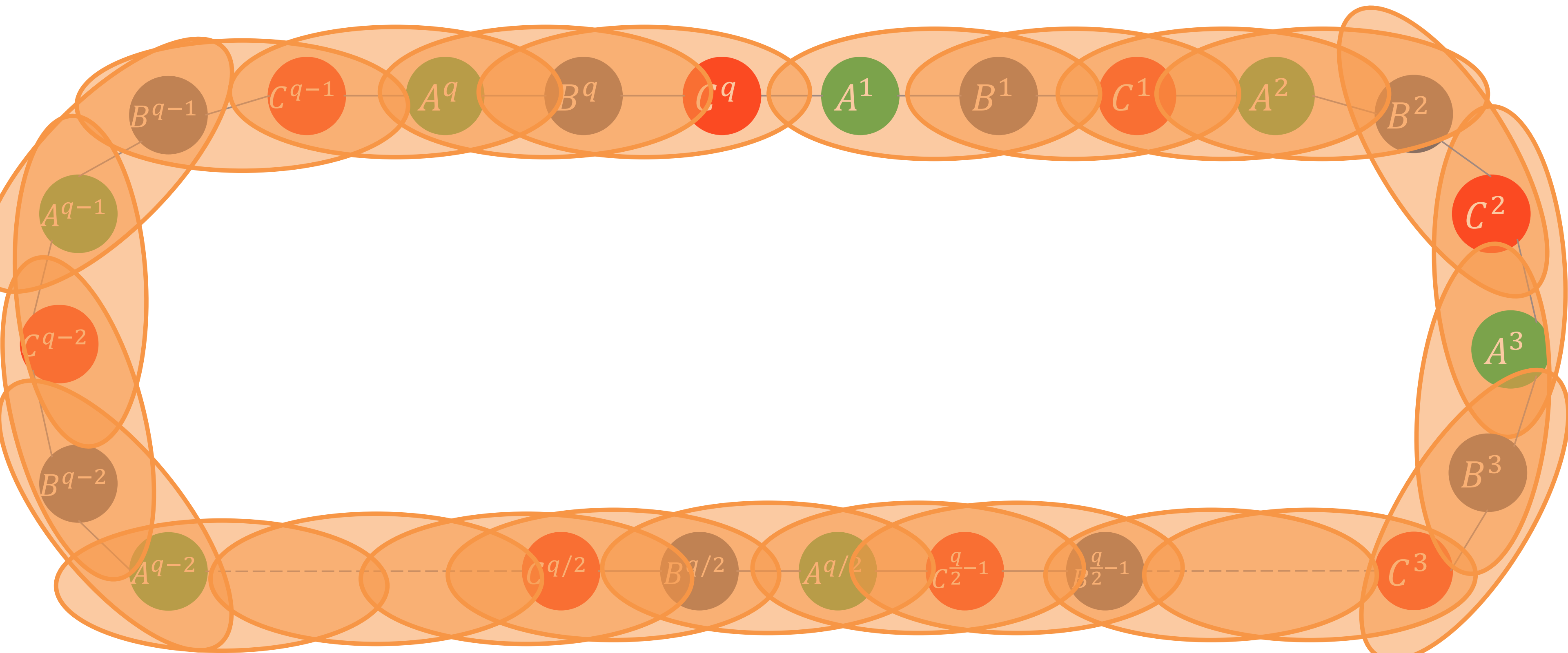


# Claim 1: $S(\boldsymbol{r})$ is monochromatic

View of $(A^1, B^1)$ in $S(\boldsymbol{r})$, for $\boldsymbol{r} \leftarrow (\{0,1\}^\kappa)^{3q}$, is view of $(A, B)$ in a **random** interaction of $(A, B, C^*)$ with some $C^*$.

$\pi$ is $1$-consistent $\Rightarrow$ $A^1$ and $B^1$ output same value.

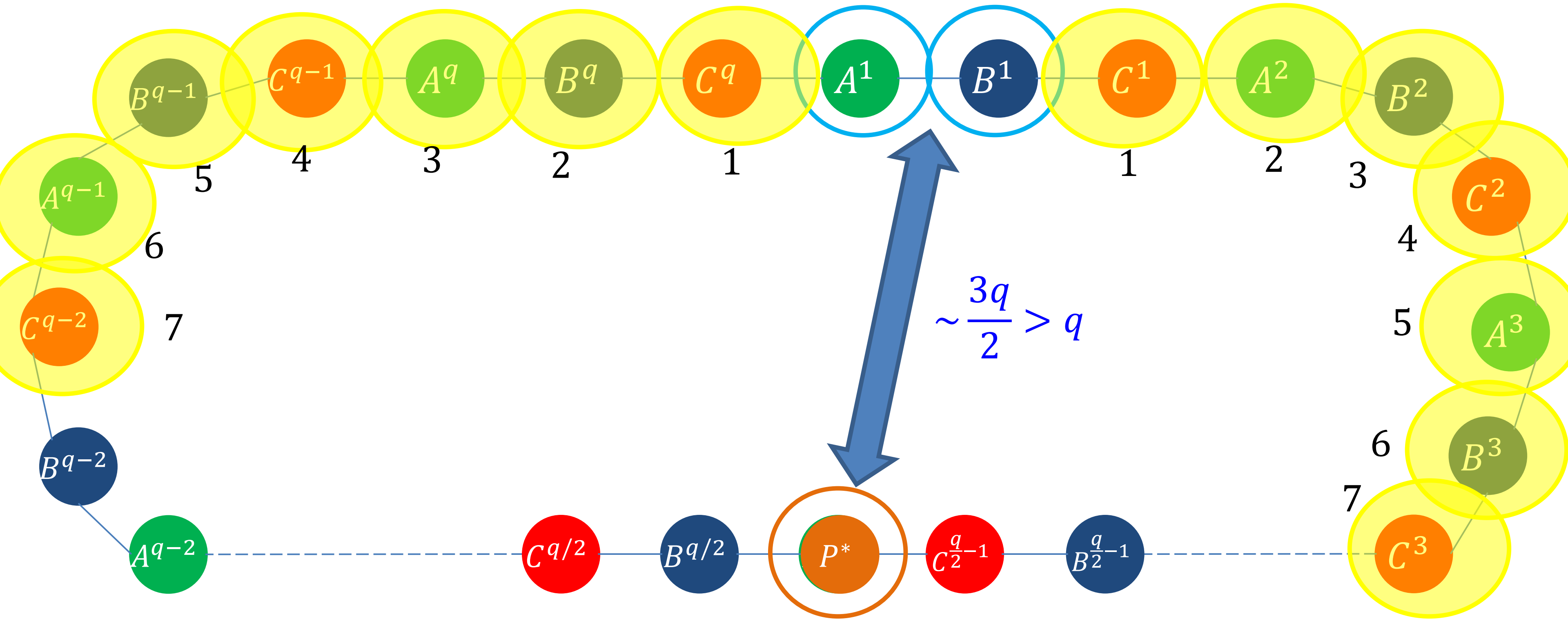
$\Rightarrow$ each pair of adjacent parties output the same value.



# **Claim 2**: $A^1, B^1$ messages don't reach $P^* = A^{q/2}$

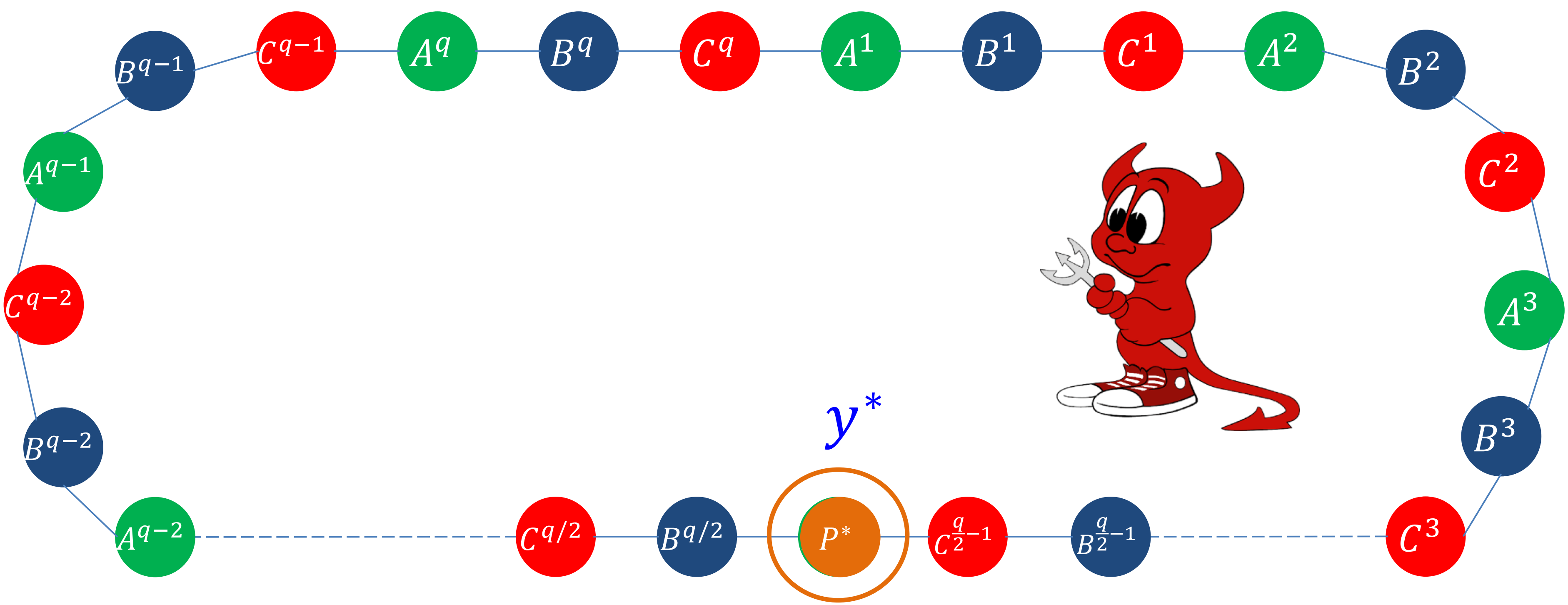
**Proof:**

- $\pi$ ends after at most $q$ rounds
- The distance between $(A^1, B^1)$ and $P^*$ is $\sim \frac{3q}{2} > q$



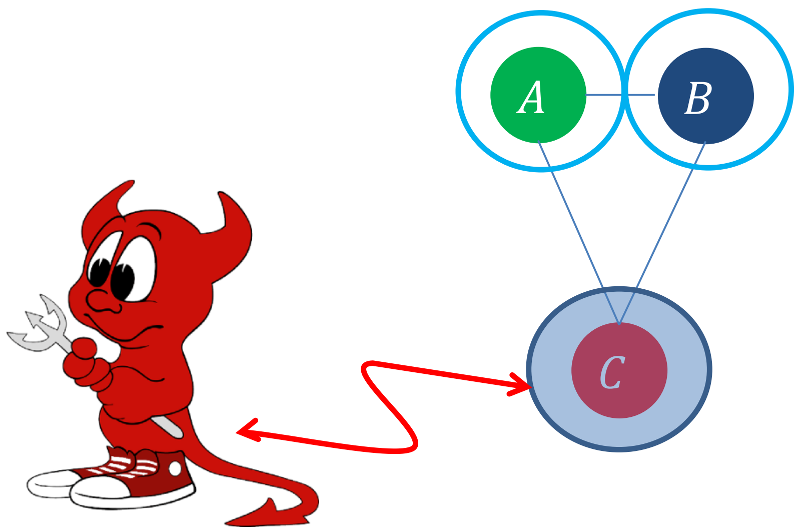
# Attack (step 1): output $y^*$

1. Sample $\boldsymbol{r} \leftarrow (\{0,1\}^\kappa)^{3q}$
2. Output $y^*$ – the output of $P^*$ in $S(\boldsymbol{r})$



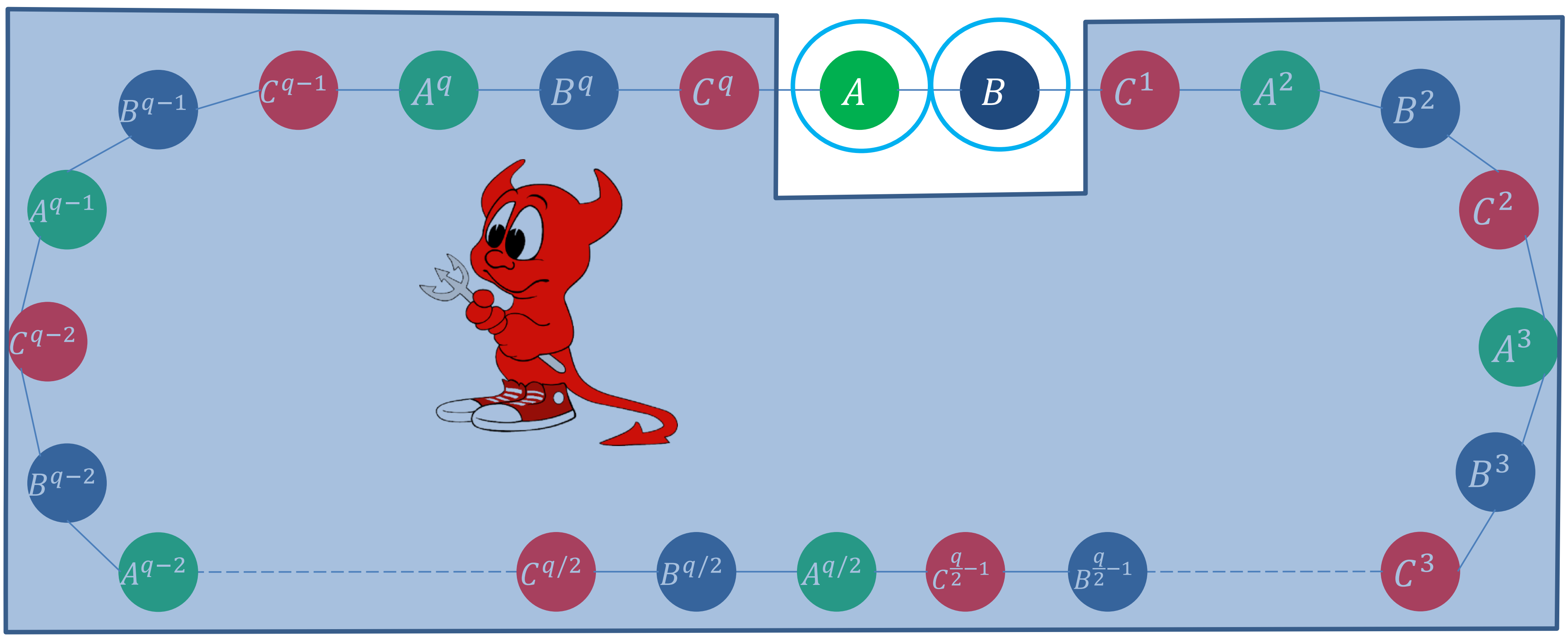
# Attack (step 2): force $(A, B)$ output

Run $S(\boldsymbol{r})$ while $(A, B)$ **take the role of** $(A^1, B^1)$ (without knowing that).



# Attack (step 2): force $(A, B)$ output

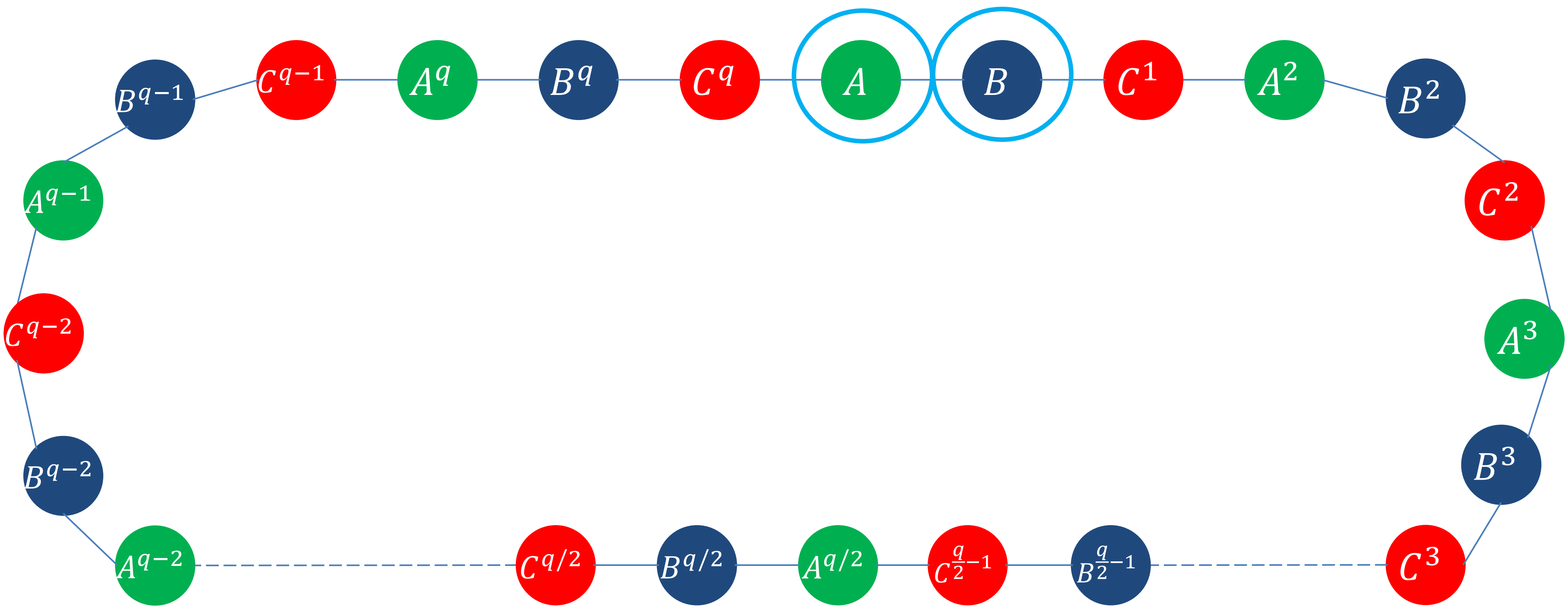
Run $S(\boldsymbol{r})$ while $(A, B)$ **take the role of** $(A^1, B^1)$ (without knowing that).



# Claim 3: $S$ is monochromatic

**Proof:**

The execution of $S$ induced by the attack on (honest) $(A, B)$, is that of $S(\boldsymbol{r}')$ for $\boldsymbol{r}' \leftarrow (\{0,1\}^{\kappa})^{3q}$



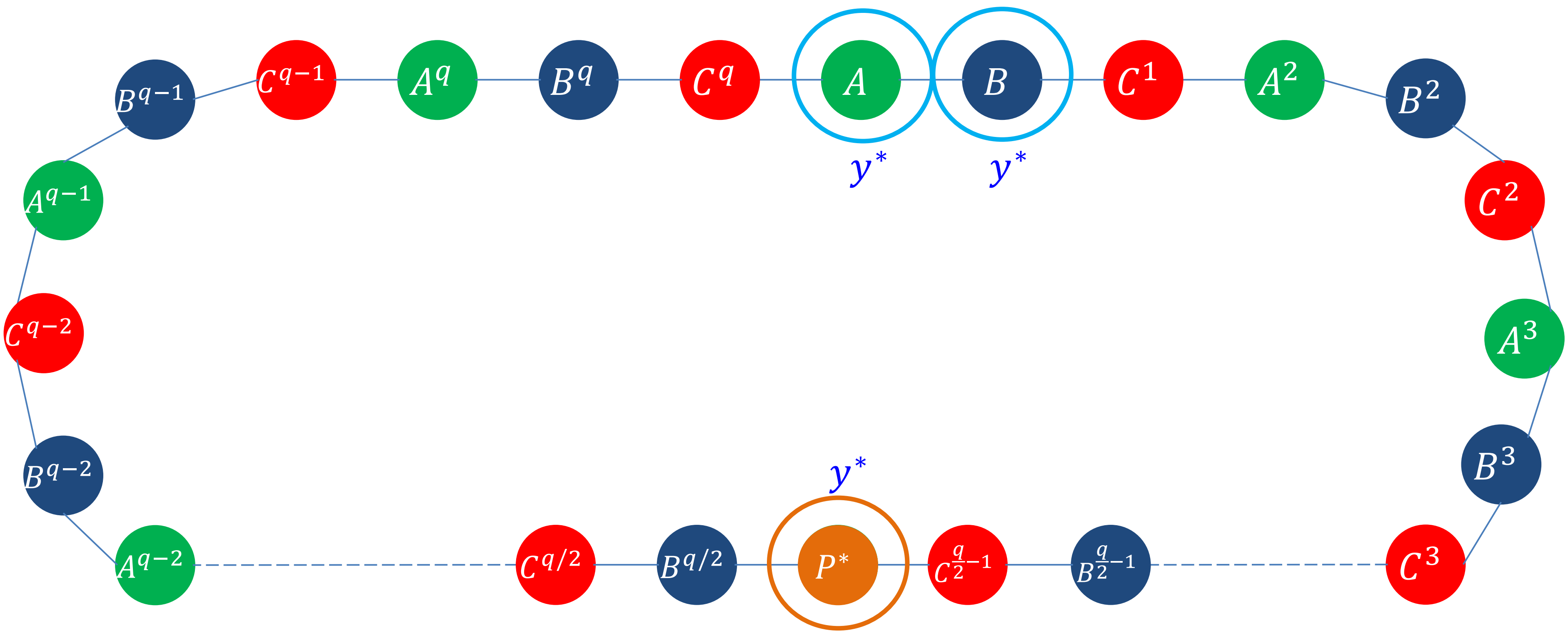
# Claim 4: $A$ and $B$ output $y^*$

**Proof:**

The messages of $(A, B)$ do not reach $P^*$ (too far apart)

$\Rightarrow$ $P^*$ has the same view in $S(\boldsymbol{r})$ and $S(\boldsymbol{r}')$ (outputs $y^*$)

$(A, B)$ output the same value as $P^*$ ($S$ monochromatic) ■



# Summary & open question

We considered $t$-consistent $n$-party protocols in the P2P model (for $n \geq 3$ and $t \geq n/3$)

1. Characterization of symmetric functionalities with full security
2. Coin flipping requires broadcast

Open question: **Non**-symmetric functionalities?

Thank You