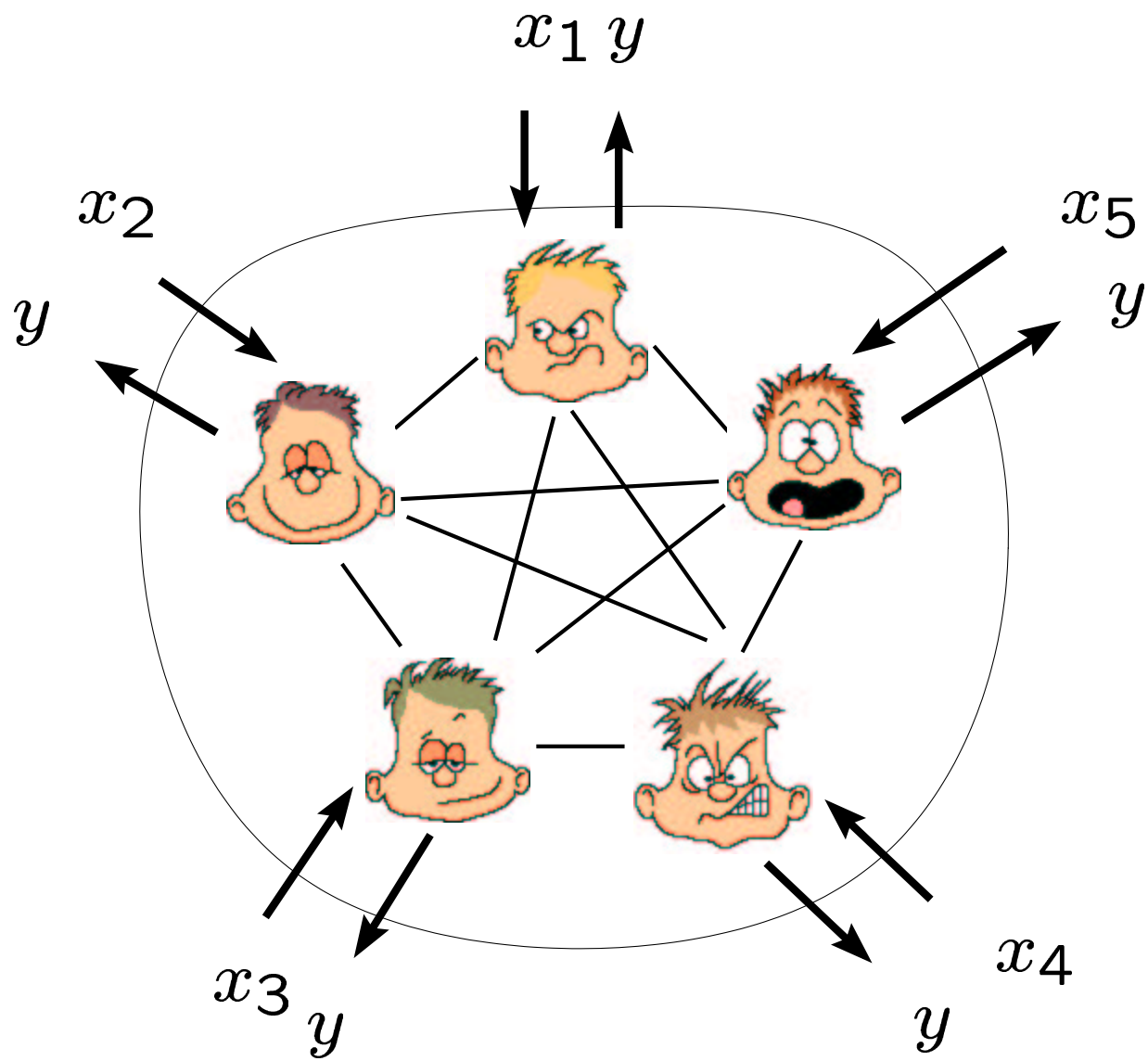
Multi-Party Computation with Hybrid Security

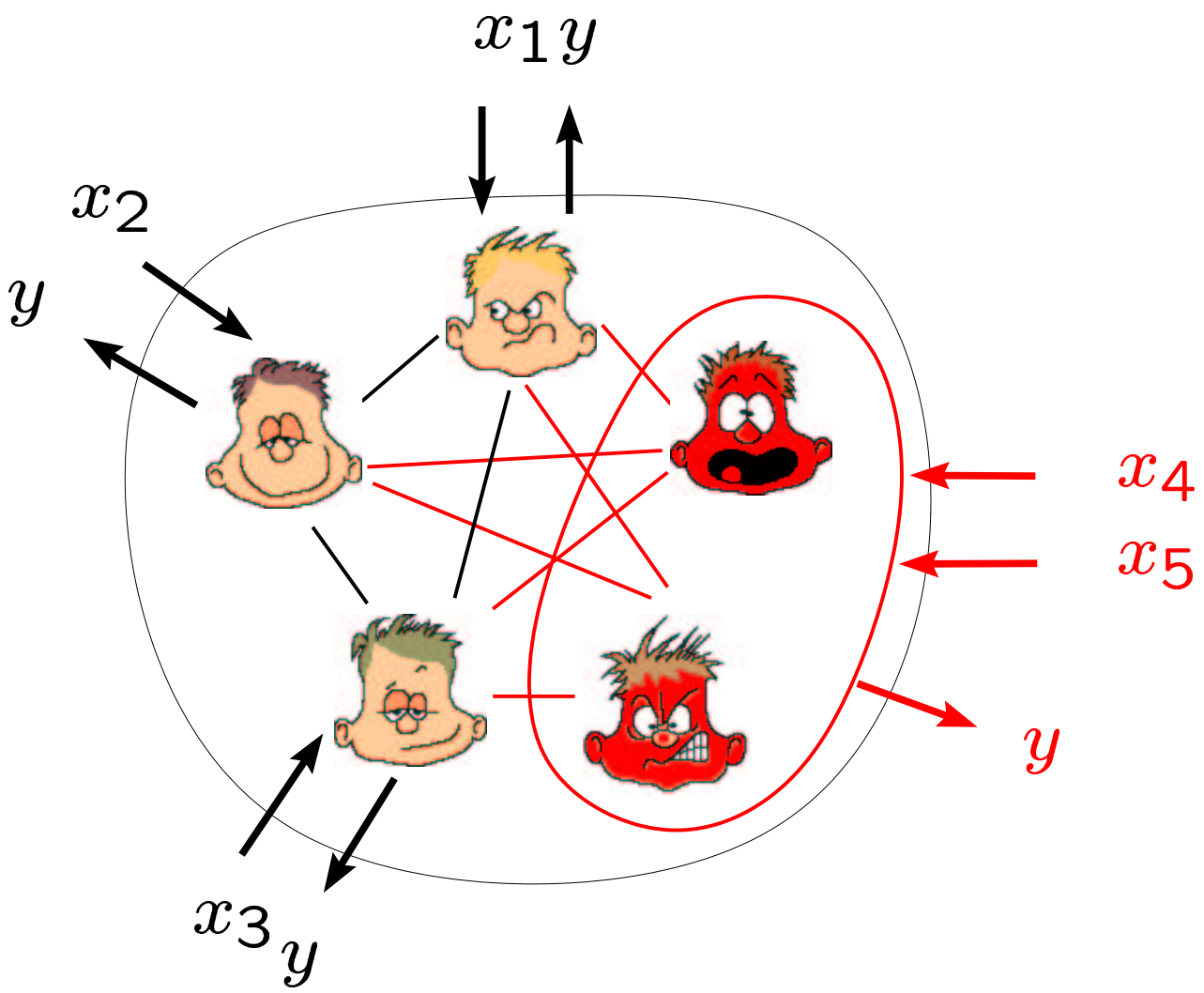
Matthias Fitzi, Thomas Holenstein, and
Jürg Wullschleger

Multi-Party Computation (MPC) [Yao82,GMW87]



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

MPC: Adversary



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

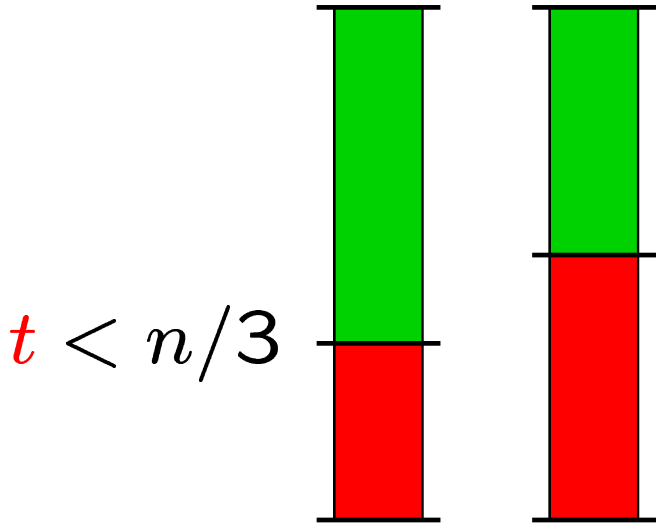
MPC: Adversary

- Central adversary $\mathcal{A}$:
  - corrupt up to t players actively
  - **Privacy**: $\mathcal{A}$ no information about good x_i
  - **Correctness**: $y = f(x_1, \ldots, x_n)$

MPC: General Achievability

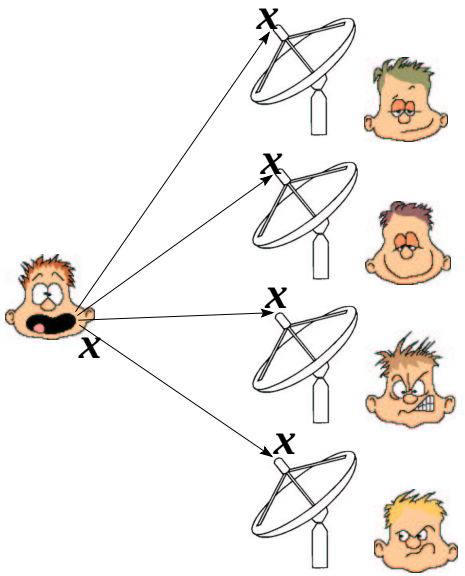
MPC achievable iff

Standard model:



[BGW88,CCD88]
tight [LSP82]

Broadcast Model:



[B89,RB89]
tight [Cleve86]

How to do Broadcast with $t \geq n/3$?

Construction using:

- Hardware.

How to do Broadcast with $t \geq n/3$?

Construction using:

- Hardware. How???

How to do Broadcast with $t \geq n/3$?

Construction using:

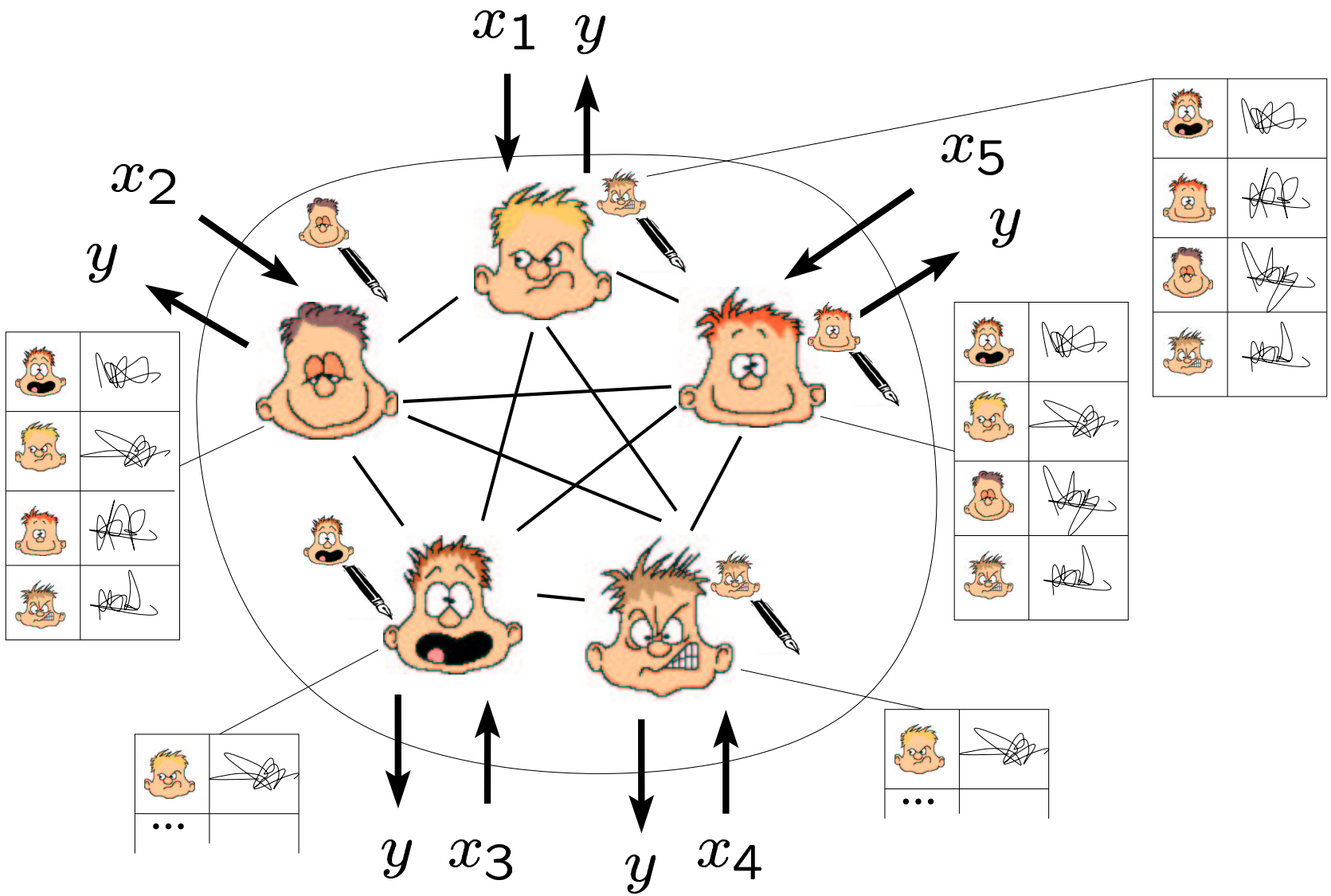
- Hardware. How???
- Signature Scheme [LSP82,DS82,PW96]

How to do Broadcast with $t \geq n/3$?

Construction using:

- Hardware. How???
- Signature Scheme [LSP82,DS82,PW96]
  + Consistent PKI.

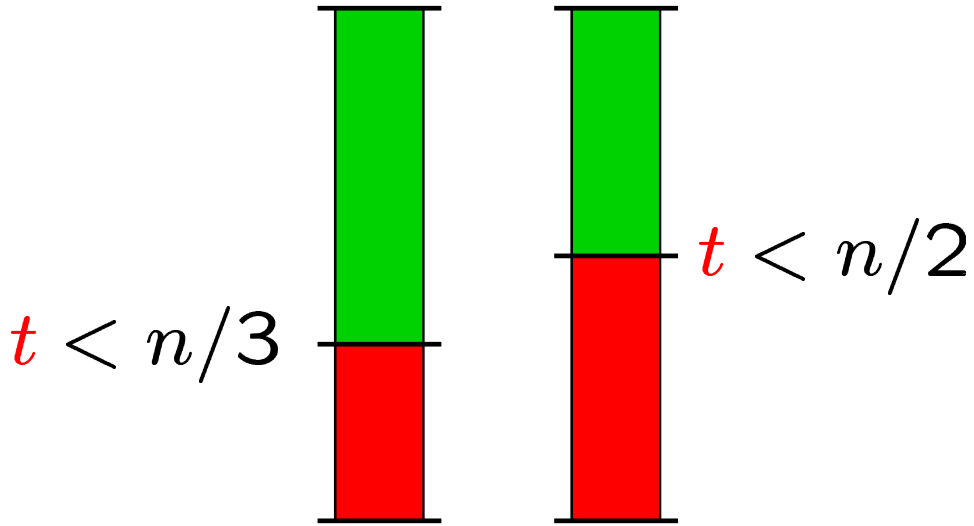
MPC with Signature Scheme



MPC: Compare Models

Standard model:

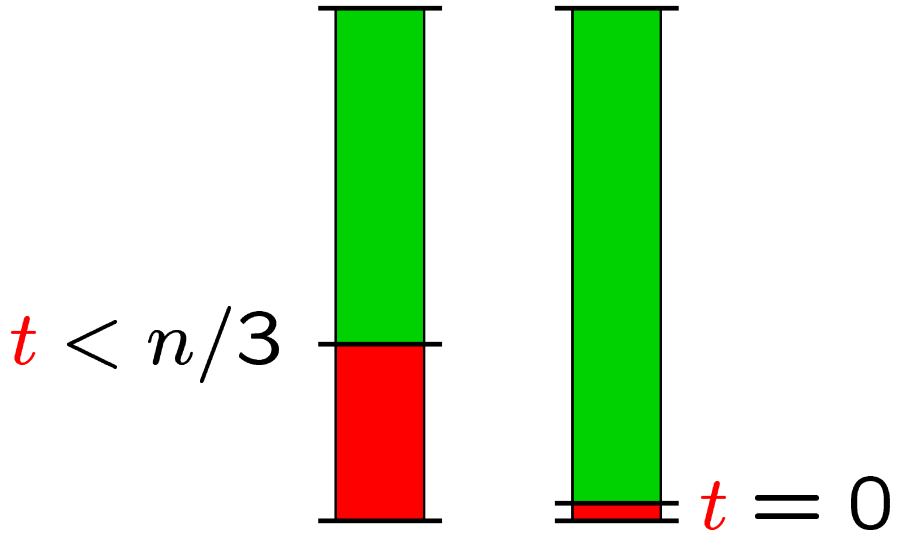
Standard Model
with Signature Scheme
and consistent PKI:



MPC: Compare Models

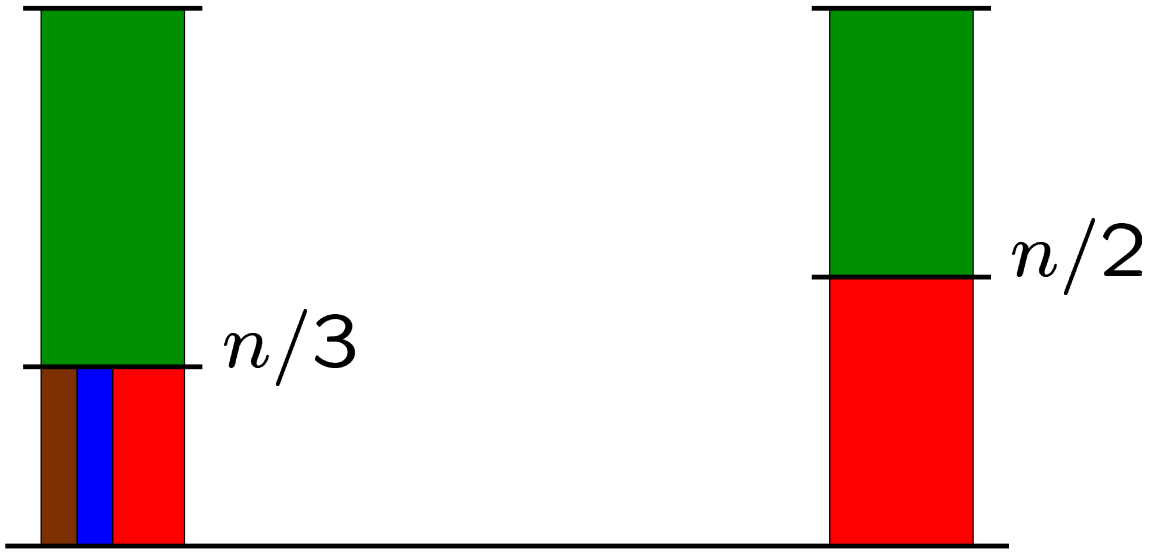
Standard model:

Standard Model
with Signature Scheme
and consistent PKI:



Adversary can forge Signature
or make PKI inconsistent.

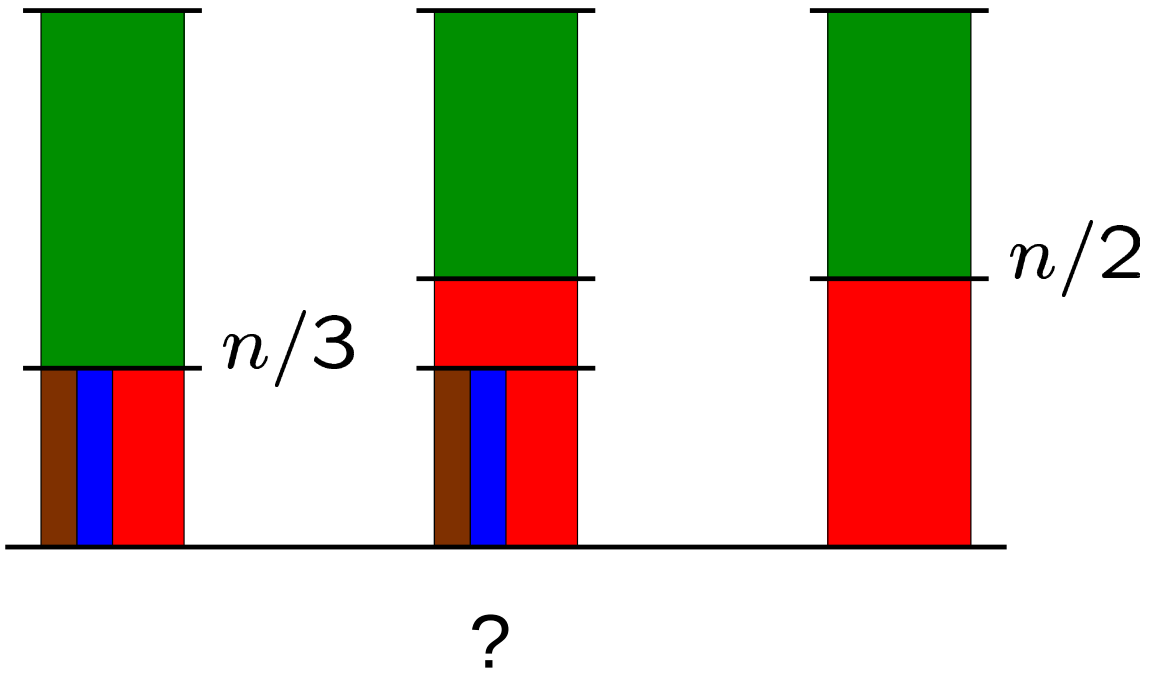
Model - Idea



Adversary

- can Forge Signature
- can make PKI inkonsistent

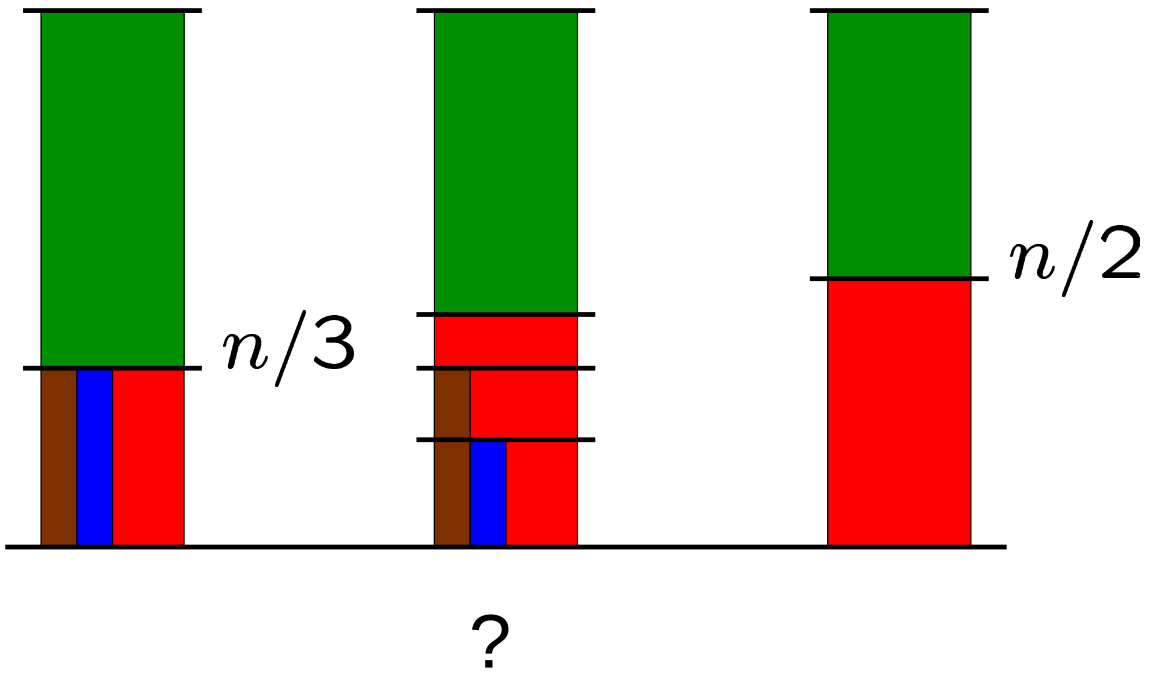
Model - Idea



Adversary

- can Forge Signature
- can make PKI inkonsistent

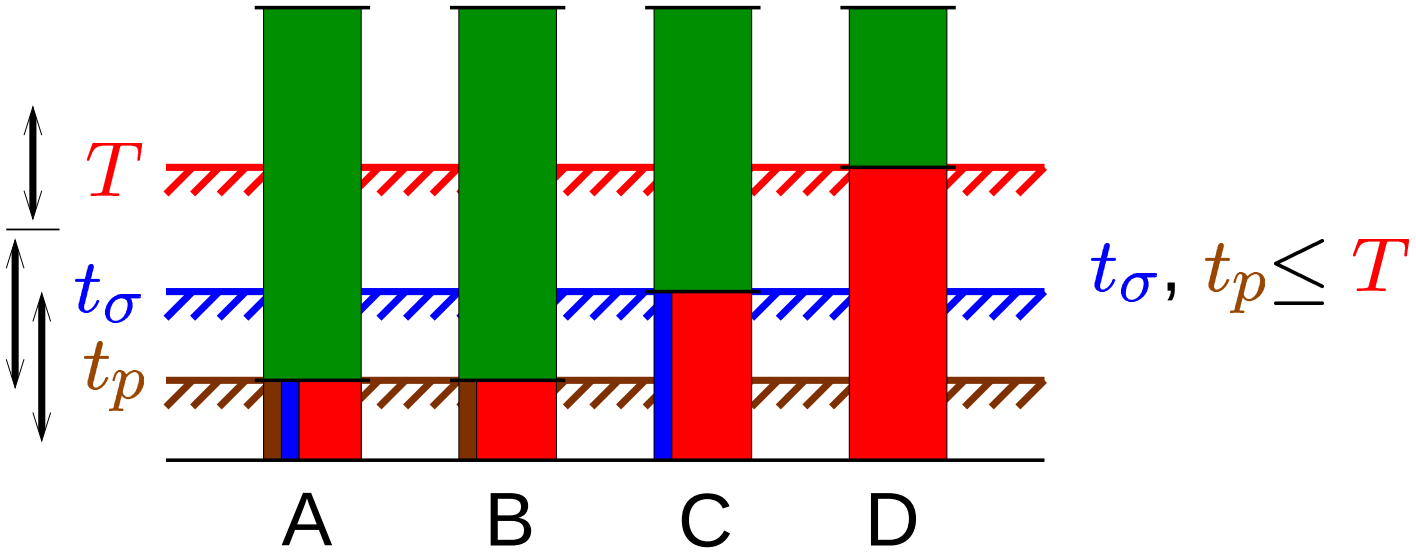
Model - Idea



Adversary

- can Forge Signature
- can make PKI inkonsistent

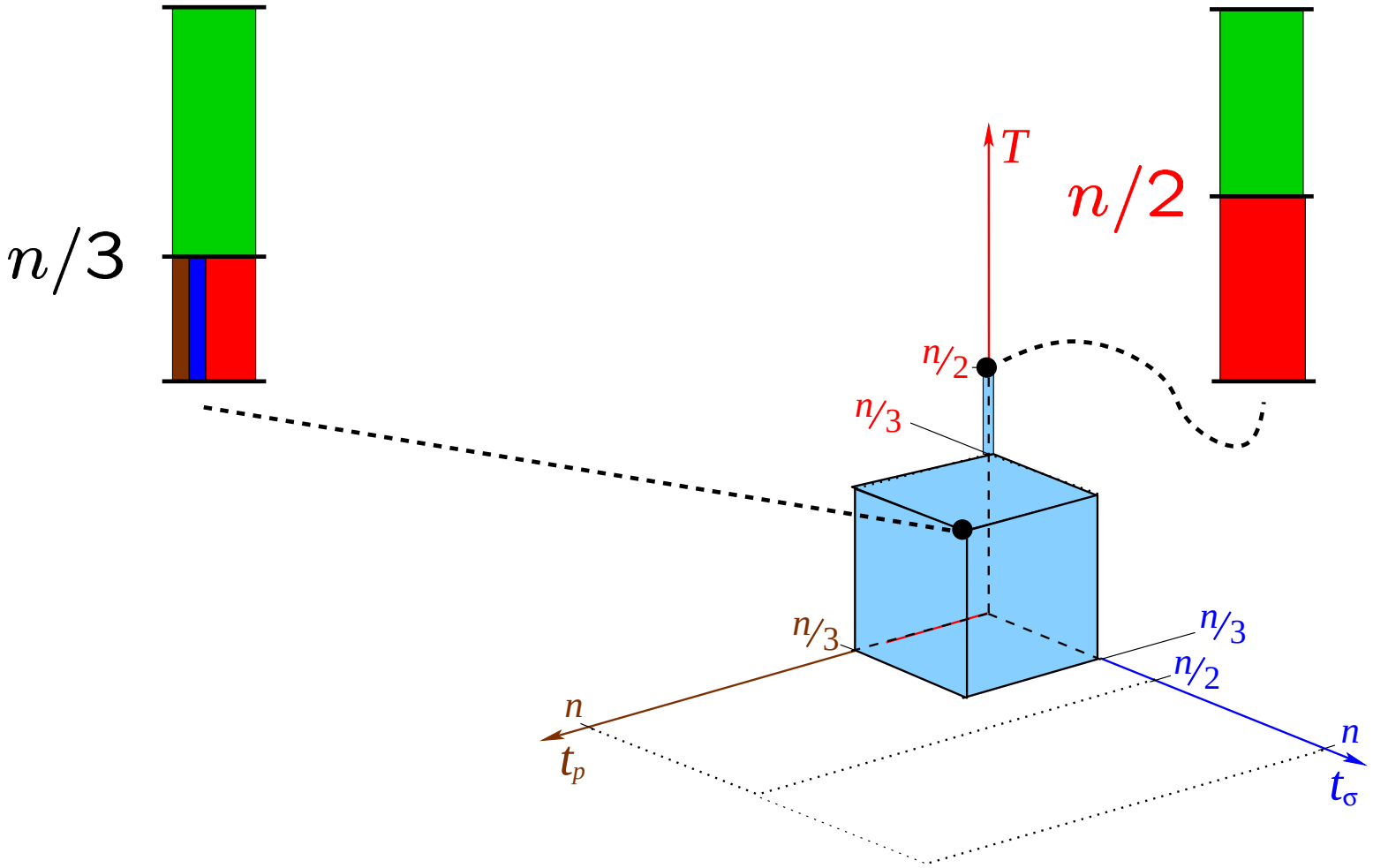
Hybrid Security Model



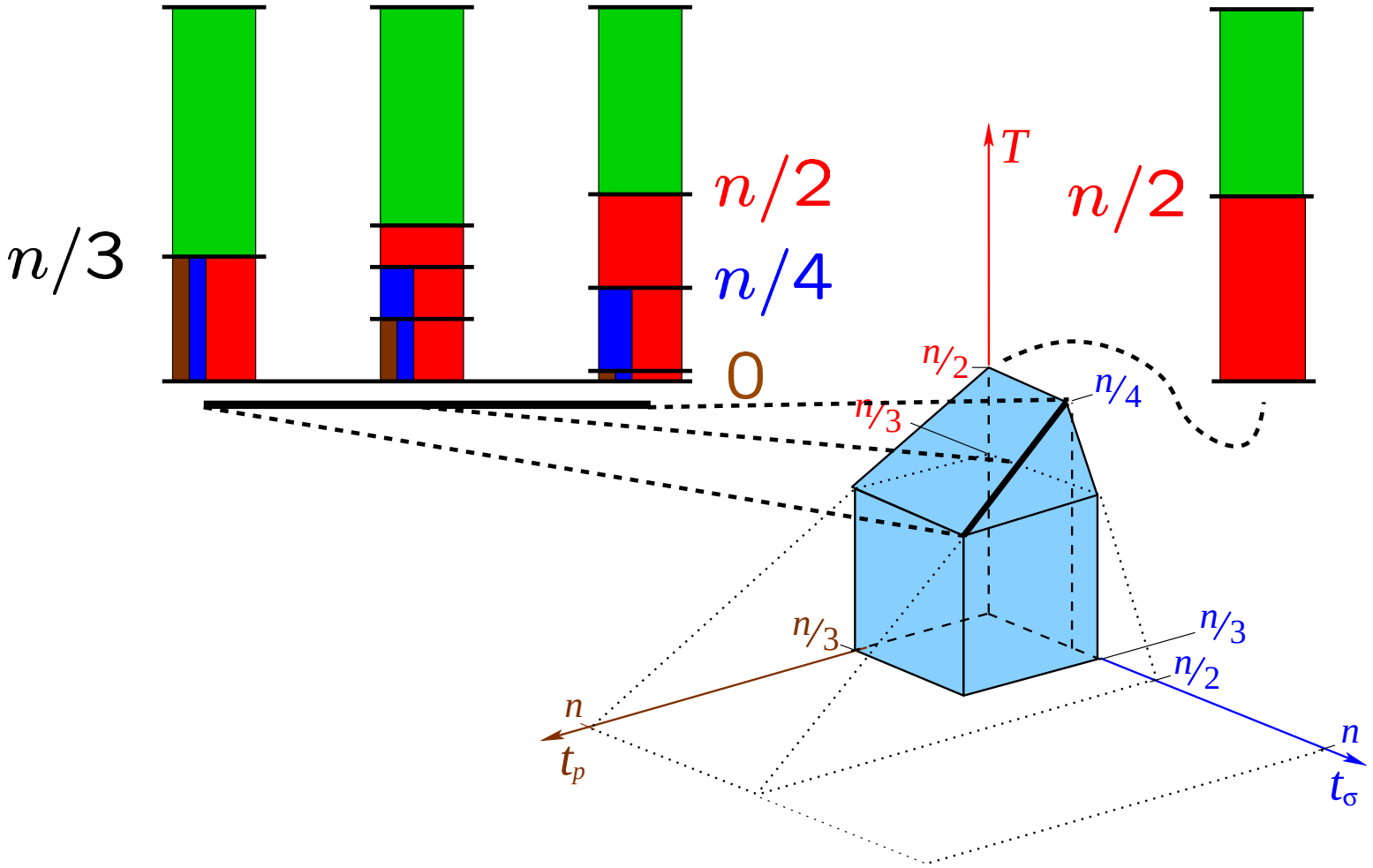
Adversary can:

- corrupt up to $f \leq T$ players.
- if $f \leq t_\sigma$, forge signatures.
- if $f \leq t_p$, make the PKI inconsistent.

Previous Results: Tight Bounds



Tight Bounds for Hybrid Security



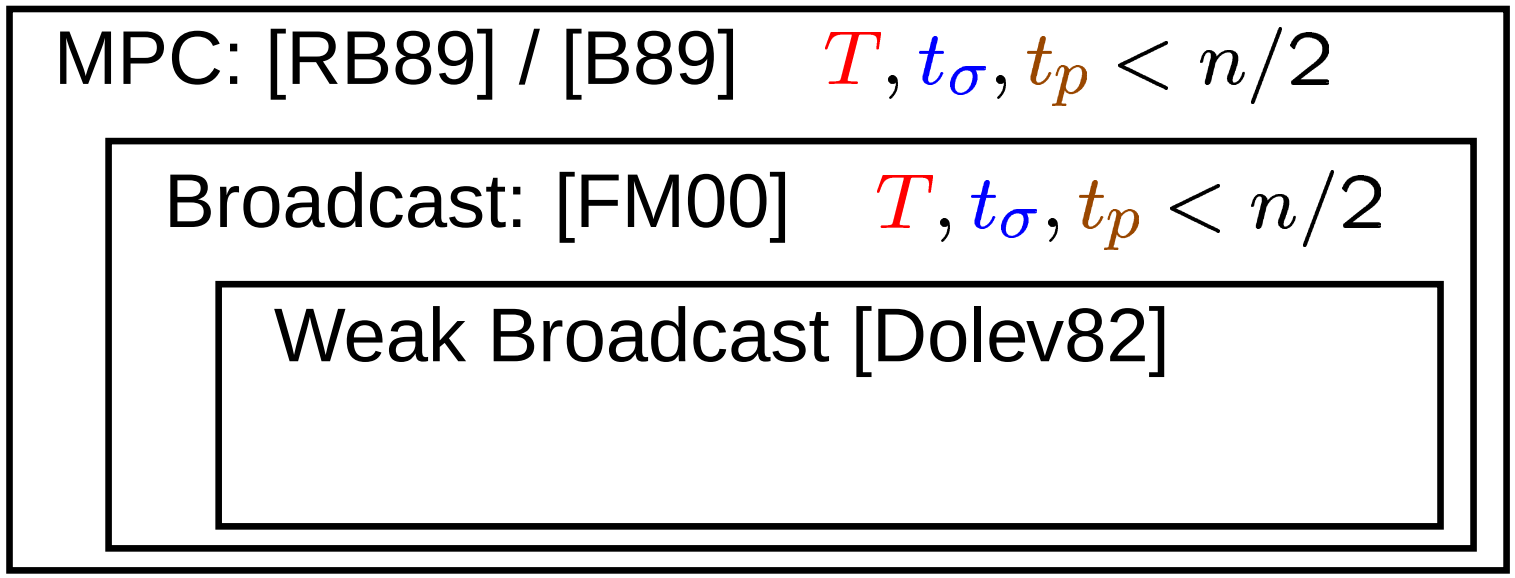
$$(2T + t_p < n) \quad \wedge \quad (T + 2t_\sigma < n)$$

The Protocol - Idea

MPC: [RB89] / [B89] $T, t_\sigma, t_p < n/2$

Broadcast

The Protocol - Idea



The Protocol - Idea

MPC: [RB89] / [B89] $T, t_\sigma, t_p < n/2$

Broadcast: [FM00] $T, t_\sigma, t_p < n/2$

Weak Broadcast [this paper]

$(2T + t_p < n) \wedge (T + 2t_\sigma < n)$

The Protocol - Idea

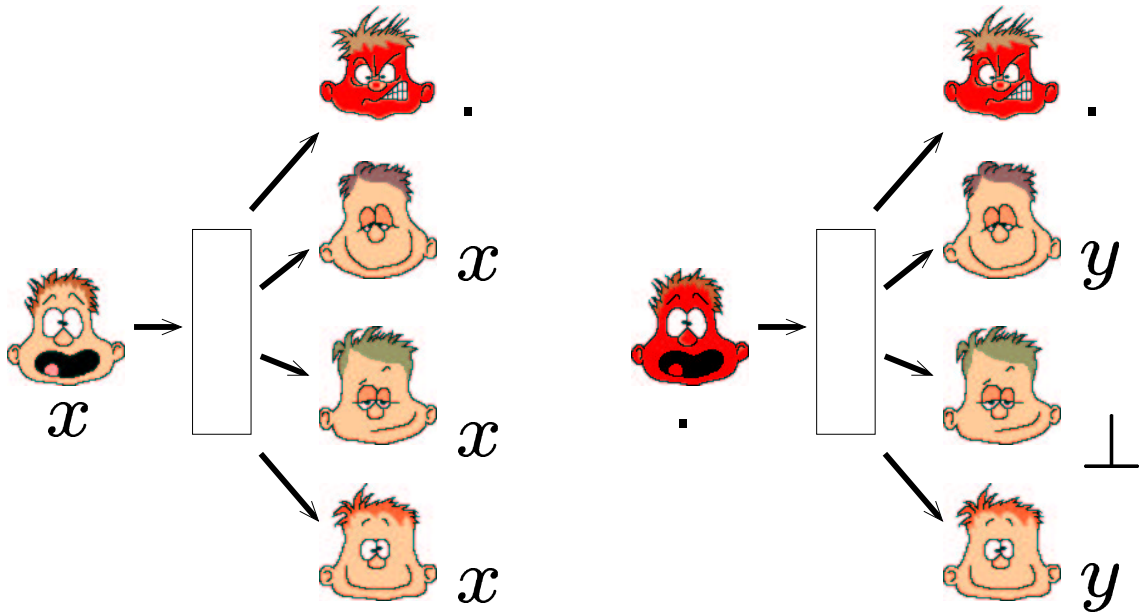
MPC: [RB89] / [B89] $T, t_\sigma, t_p < n/2$

Broadcast: [FM00] $T, t_\sigma, t_p < n/2$

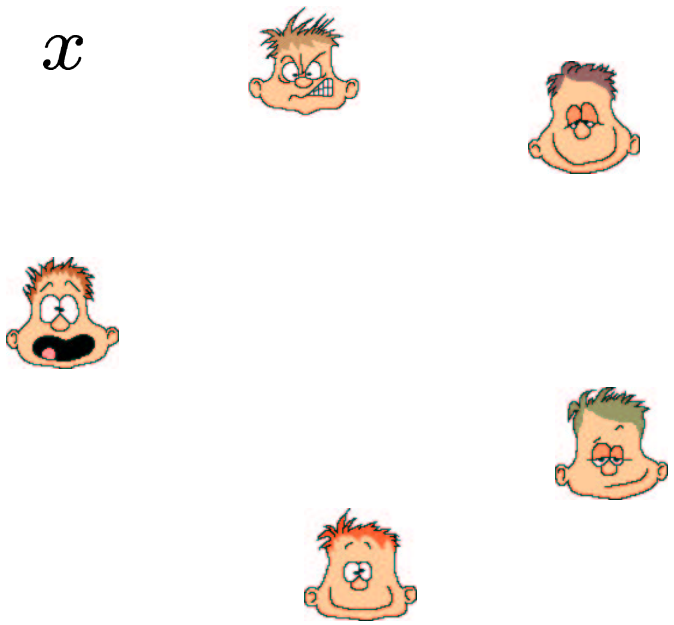
Weak Broadcast [this paper]

$(2T + t_p < n) \wedge (T + 2t_\sigma < n)$

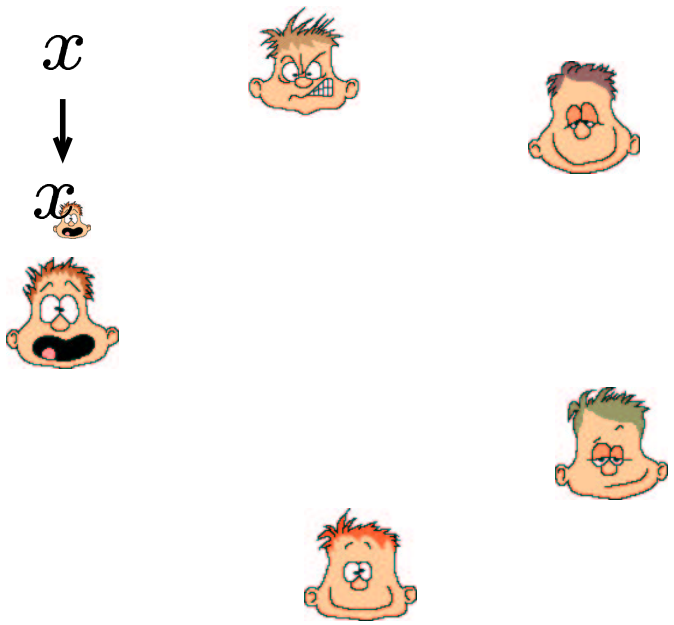
Weak Broadcast:



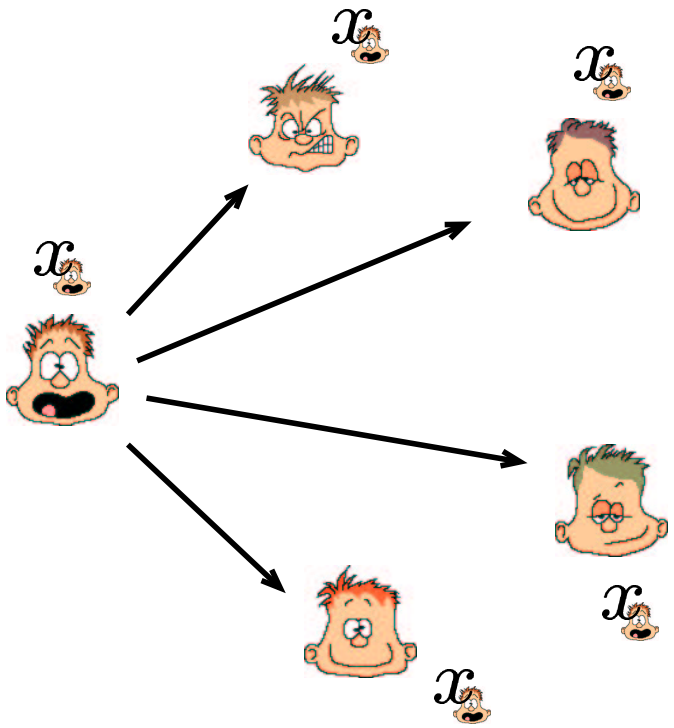
Weak Broadcast - Protocol



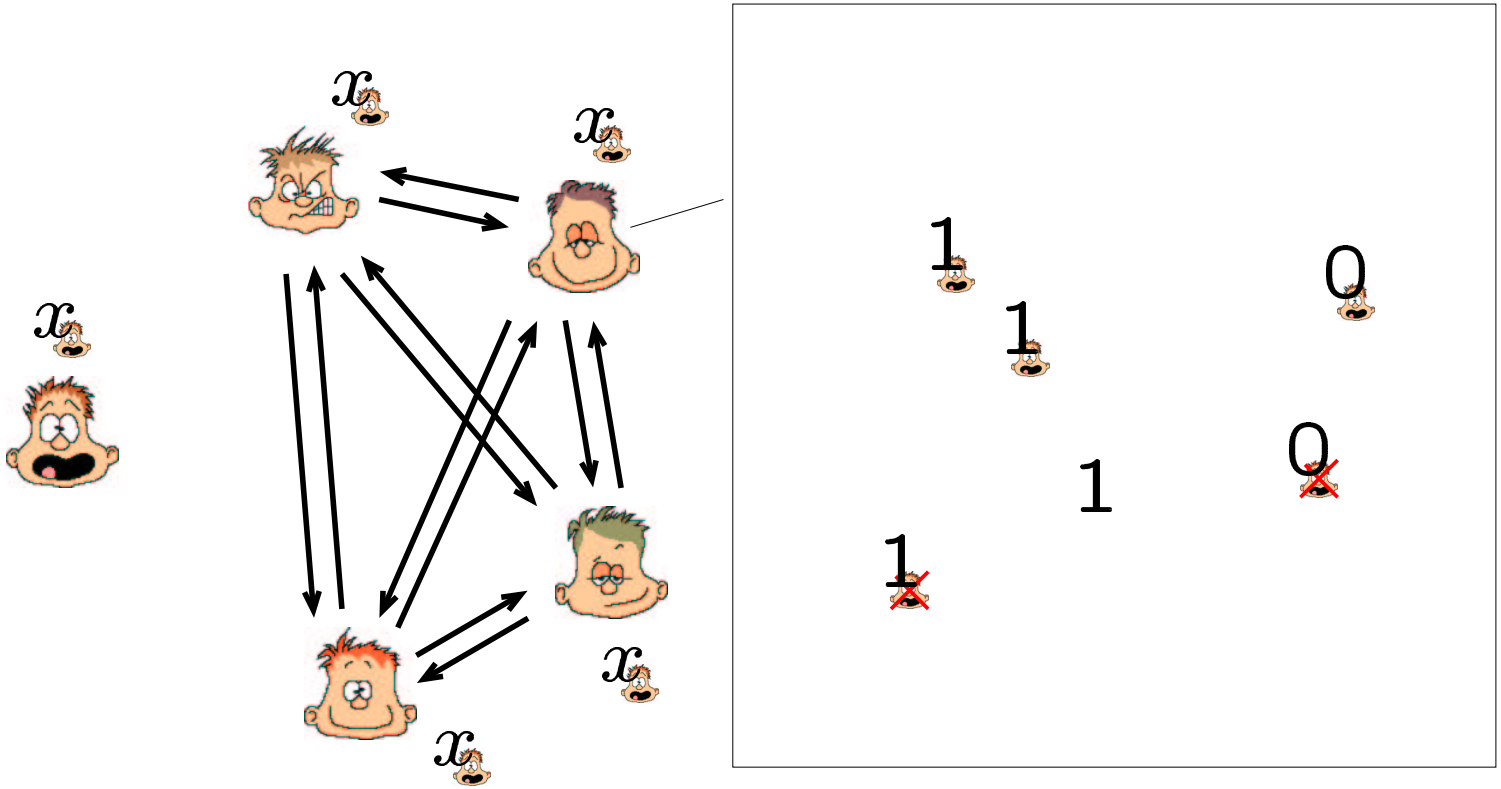
Weak Broadcast - Protocol



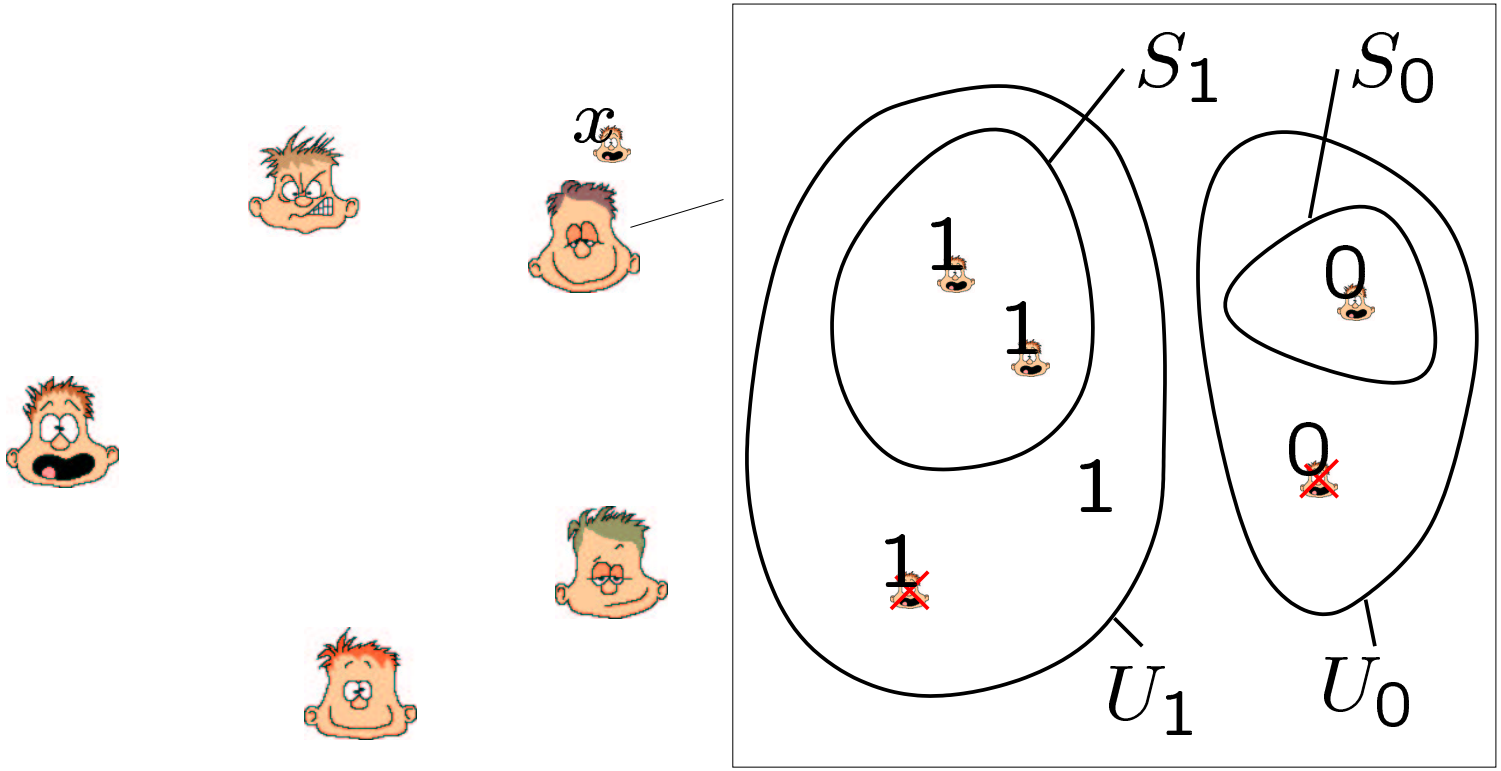
Weak Broadcast - Protocol



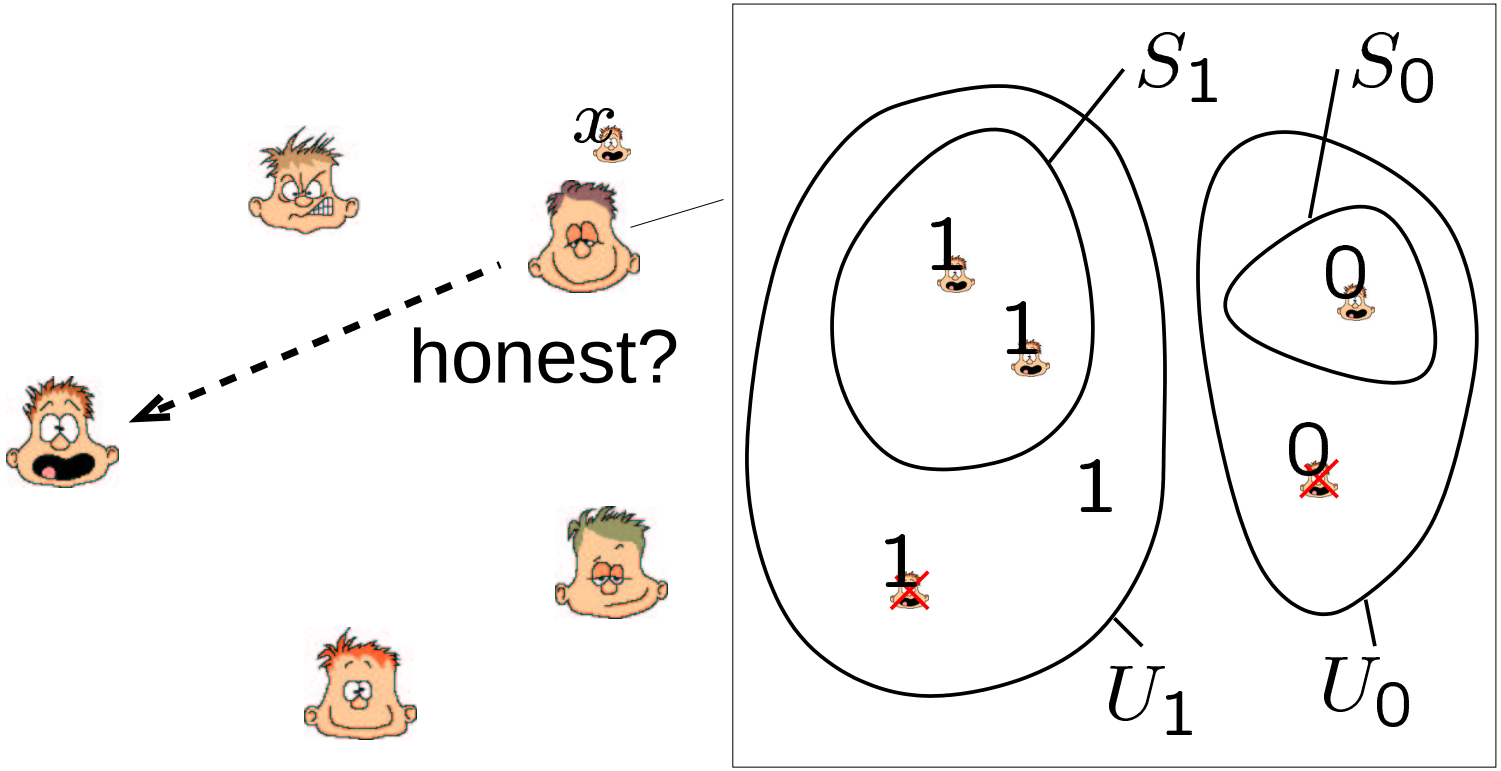
Weak Broadcast - Protocol



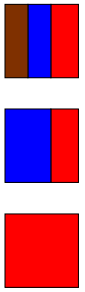
Weak Broadcast - Protocol



Weak Broadcast - Protocol



Output x, if: $\begin{cases} |U_x| \geq n - t_p \\ |S_x| \geq n - t_\sigma \\ |S_x| \geq n - T \wedge |S_{1-x}| = 0 \end{cases}$

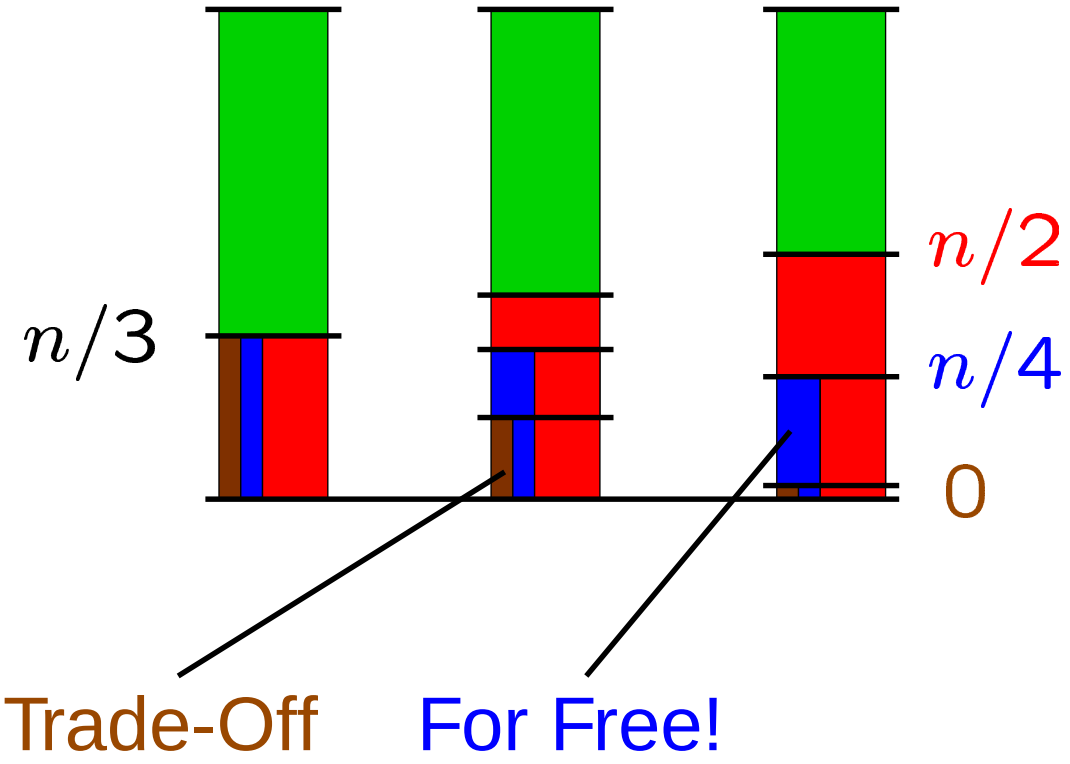


and $\perp$ otherwise.

Conclusion

MPC with Hybrid Security:

Tight Bound: $(2T + t_p < n) \quad \wedge \quad (T + 2t_\sigma < n)$



Efficient!