# Universally Composable Security

Ran Canetti in FOCS '01

Presented by Glen Nuckolls

# Goals and Claims

- Security definition guarantees security with arbitrary “composition”
- unbounded number of protocol invocations by any application protocol
- concurrent with same and other protocols
- adaptive adversary can corrupt honest parties

# A few Technicalities

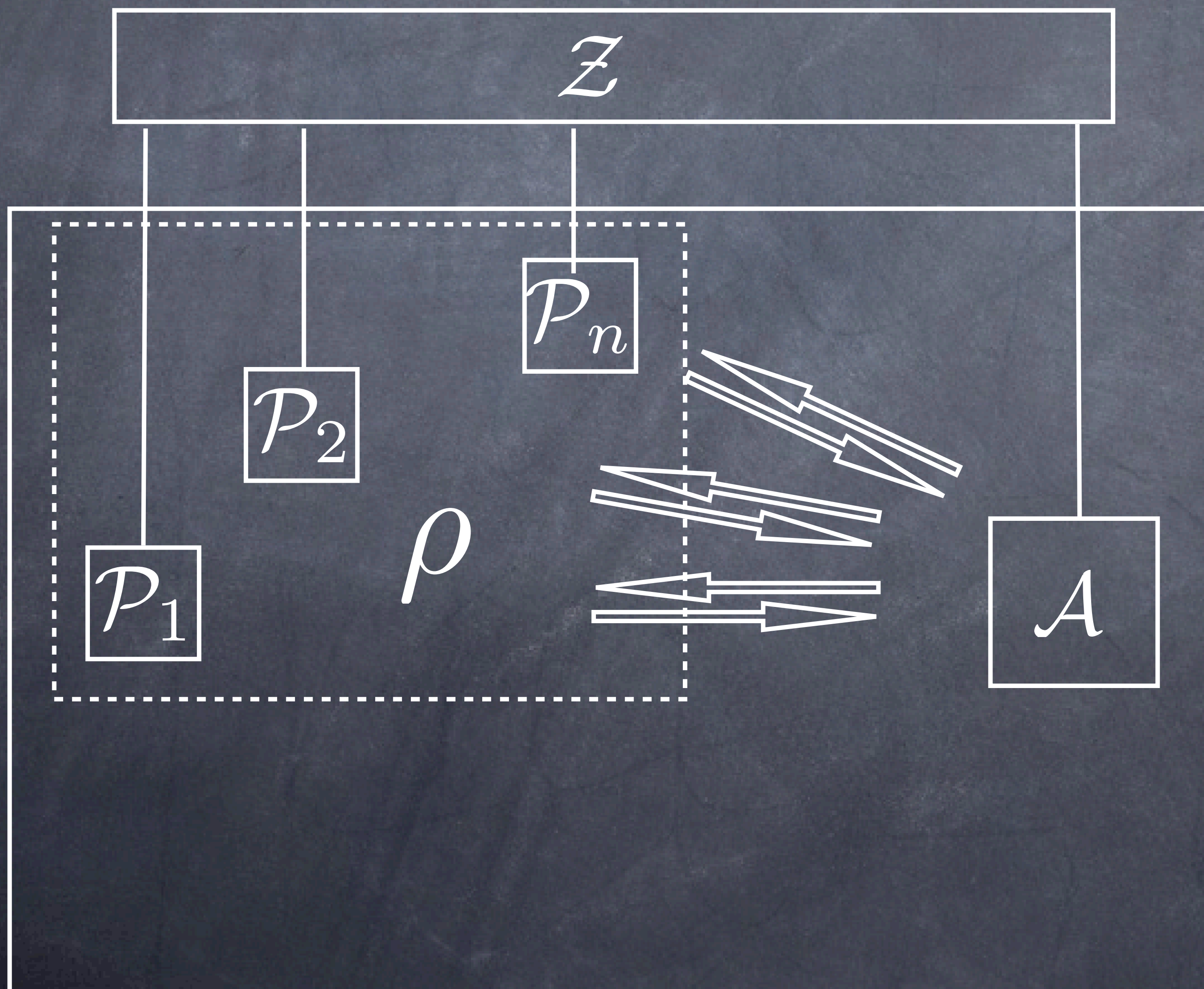
- Parties are interactive Turing Machines (ITM): many read/write tapes, either active, waiting, or halted.
- Indistinguishability $\approx$ is negligible probability difference in security parameter of environment's binary output
- Ideal functionality an ITM: "magic" modeled by restricting adversarial view of messages

# UC Security

- For all adversaries, no environment can tell between real protocol interacting with real adversary and ideal protocol in presence of "ideal" adversary.

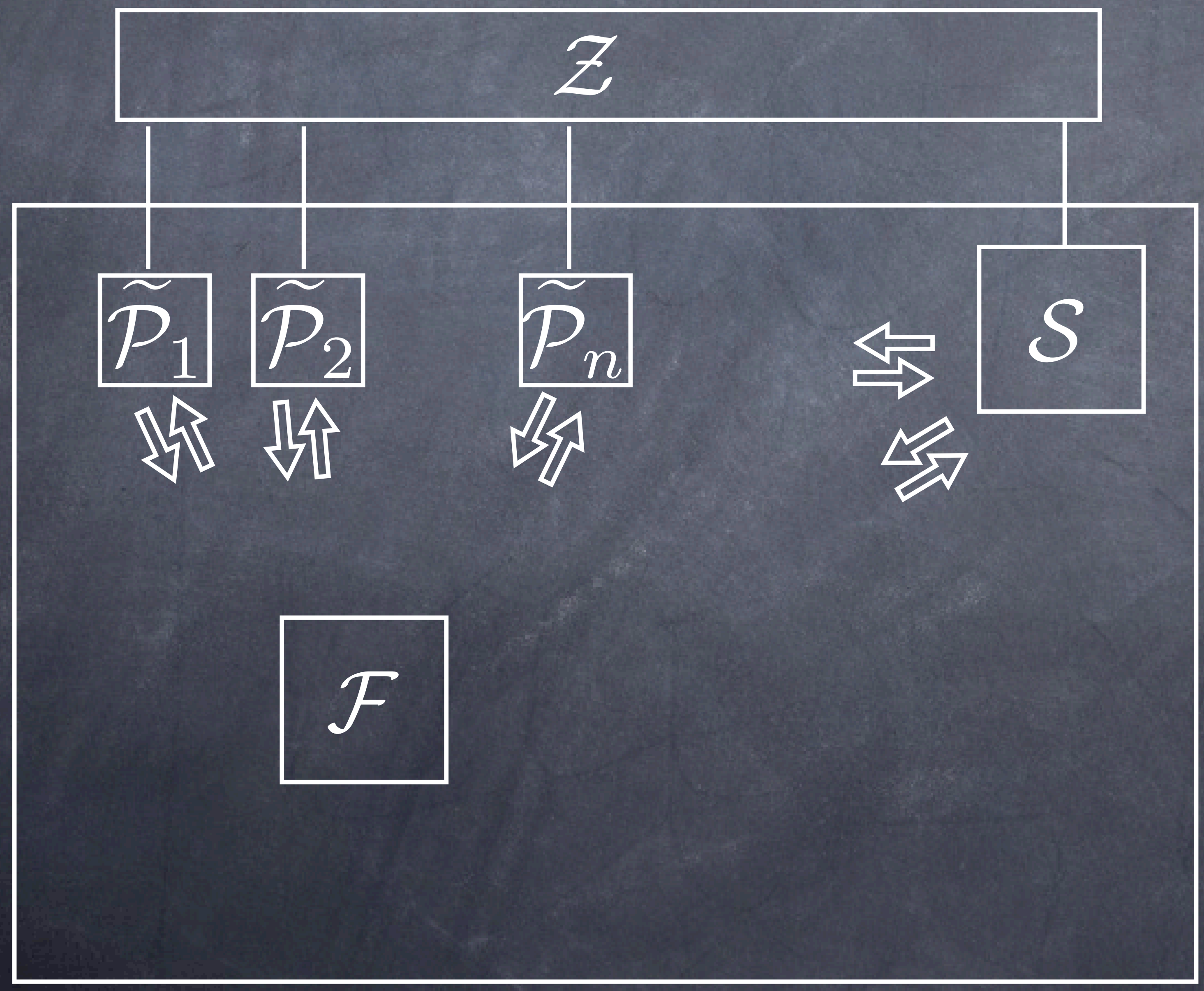
$$\forall \mathcal{A}. \exists \mathcal{S}. \forall \mathcal{Z} \quad \mathrm{REAL}_{\rho,\mathcal{A},\mathcal{Z}} \approx \mathrm{IDEAL}_{\mathcal{F},\mathcal{S},\mathcal{Z}}$$

# The Real-life Model




$\mathrm{REAL}_{\rho,\mathcal{A},\mathcal{Z}}$

# The Ideal Model



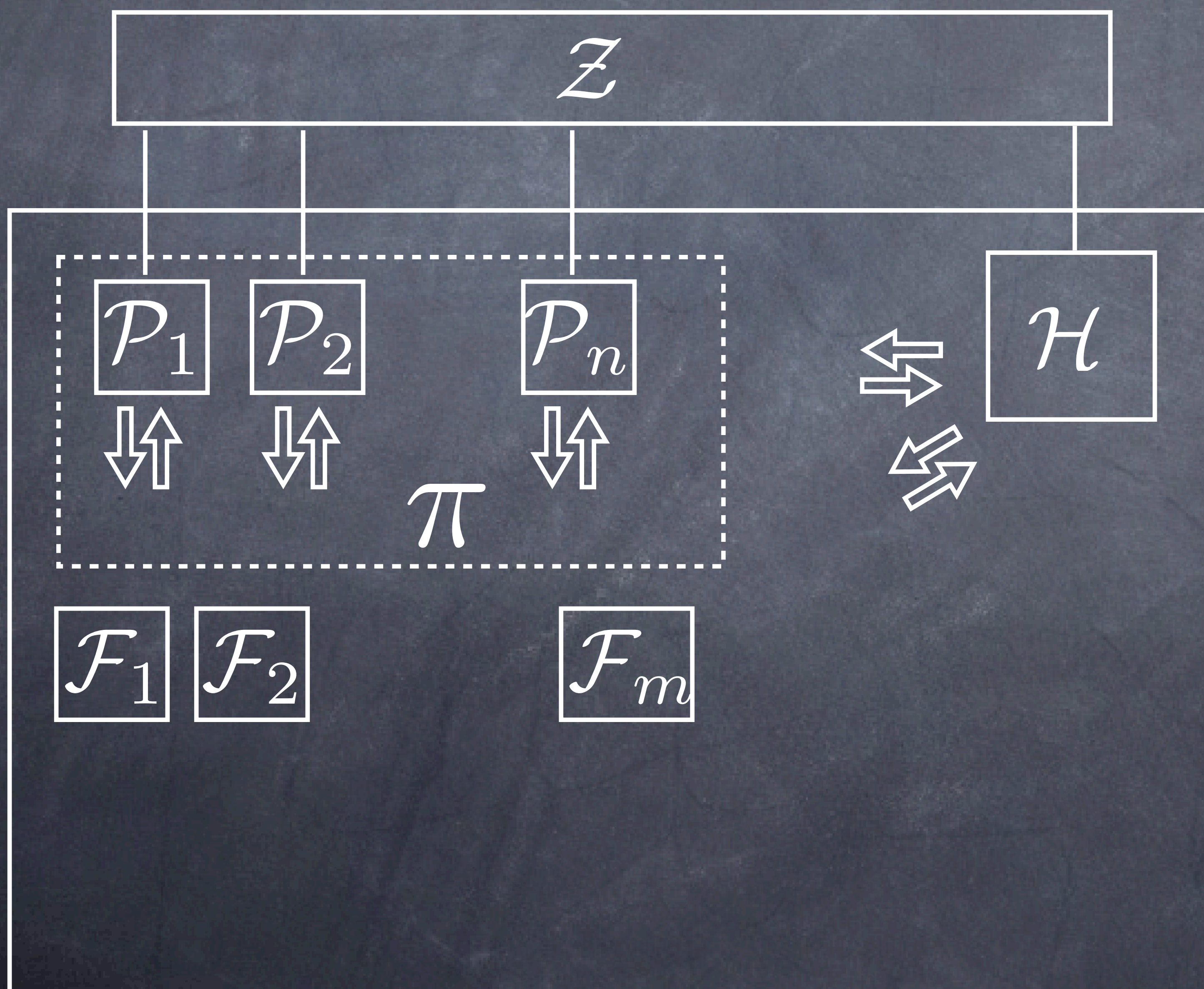

$\widetilde{\mathcal{P}}_i$ :"dummy" parties just relay i/o and msgs

$\mathrm{IDEAL}_{\mathcal{F},\mathcal{S},\mathcal{Z}}$

# F-Hybrid Model

- A protocol $\pi$ has access to ideal functionality $\mathcal{F}$
- Compare when $\mathcal{F}$ replaced with secure, real $\rho$
- F-Hybrid adversary denoted $\mathcal{H}$

# F-Hybrid Model




$\mathrm{HYBRID}^{\mathcal{F}}_{\pi,\mathcal{H},\mathcal{Z}}$

# Universal Composition Theorem

If $\rho$ realizes an ideal functionality $\mathcal{F}$, and $\pi$ is a protocol in the F-hybrid model, then:

$$\forall \mathcal{A}. \exists \mathcal{H}. \forall \mathcal{Z} \qquad \mathrm{REAL}_{\pi^\rho, \mathcal{A}, \mathcal{Z}} \approx \mathrm{HYB}^{\mathcal{F}}_{\pi, \mathcal{H}, \mathcal{Z}}$$

$\rho$ is indistinguishable from $\mathcal{F}$ in any protocol $\pi$

# Corollary: Secure Composition

If $\rho$ securely realizes $\mathcal{F}$ and $\pi$ securely realizes $\mathcal{G}$ in the F-hybrid model, then

$\forall \mathcal{A}.\exists \mathcal{H}, \mathcal{S}.\forall \mathcal{Z}$

$$\mathrm{REAL}_{\pi^\rho,\mathcal{A},\mathcal{Z}} \approx \mathrm{HYBRID}^{\mathcal{F}}_{\pi,\mathcal{H},\mathcal{Z}} \approx \mathrm{IDEAL}_{\mathcal{G},\mathcal{S},\mathcal{Z}}$$

If $\pi$ , is secure using ideal functionality $\mathcal{F}$ and $\rho$ is secure, then the composition $\pi^\rho$ is secure.

# Proof overview:

1. Formulate proof friendly definition of UC.
2. Define ideal adversary $\mathcal{H}$
3. Show that a good distinguisher environment $\mathcal{Z}$ between $\pi$ with $\rho$ and $\pi$ with ideal $\mathcal{F}$, can be used to construct a good environment $\mathcal{Z}_\rho$ distinguishing between $\rho$ and $\mathcal{F}$.
4. Existence of good $\mathcal{Z}$ implies good $\mathcal{Z}_\rho$
5. Thus: no good $\mathcal{Z}_\rho$ implies no good $\mathcal{Z}$.

# UC with Dummy Adversary

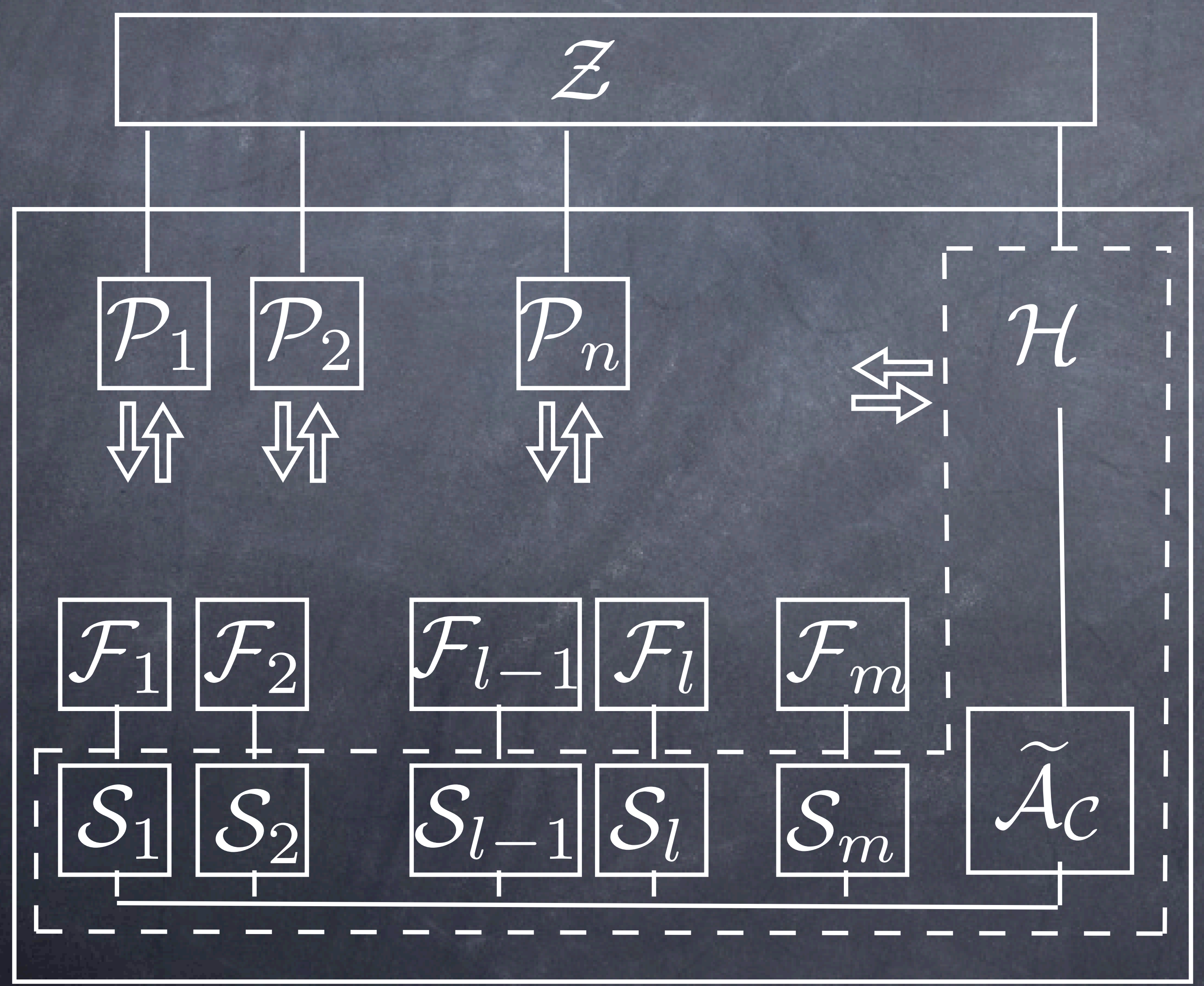
- Dummy adversary pushes adversarial role to environment, eliminates quantifying over all adversaries
- $\widetilde{A}_C$ takes input instructions from environment: report messages sent by parties, deliver message to party, corrupt some party

$$\exists \mathcal{S}. \forall \mathcal{Z} \quad \mathrm{REAL}_{\pi, \widetilde{\mathcal{A}}_C, \mathcal{Z}} \approx \mathrm{IDEAL}_{\mathcal{F}, \mathcal{S}, \mathcal{Z}}$$

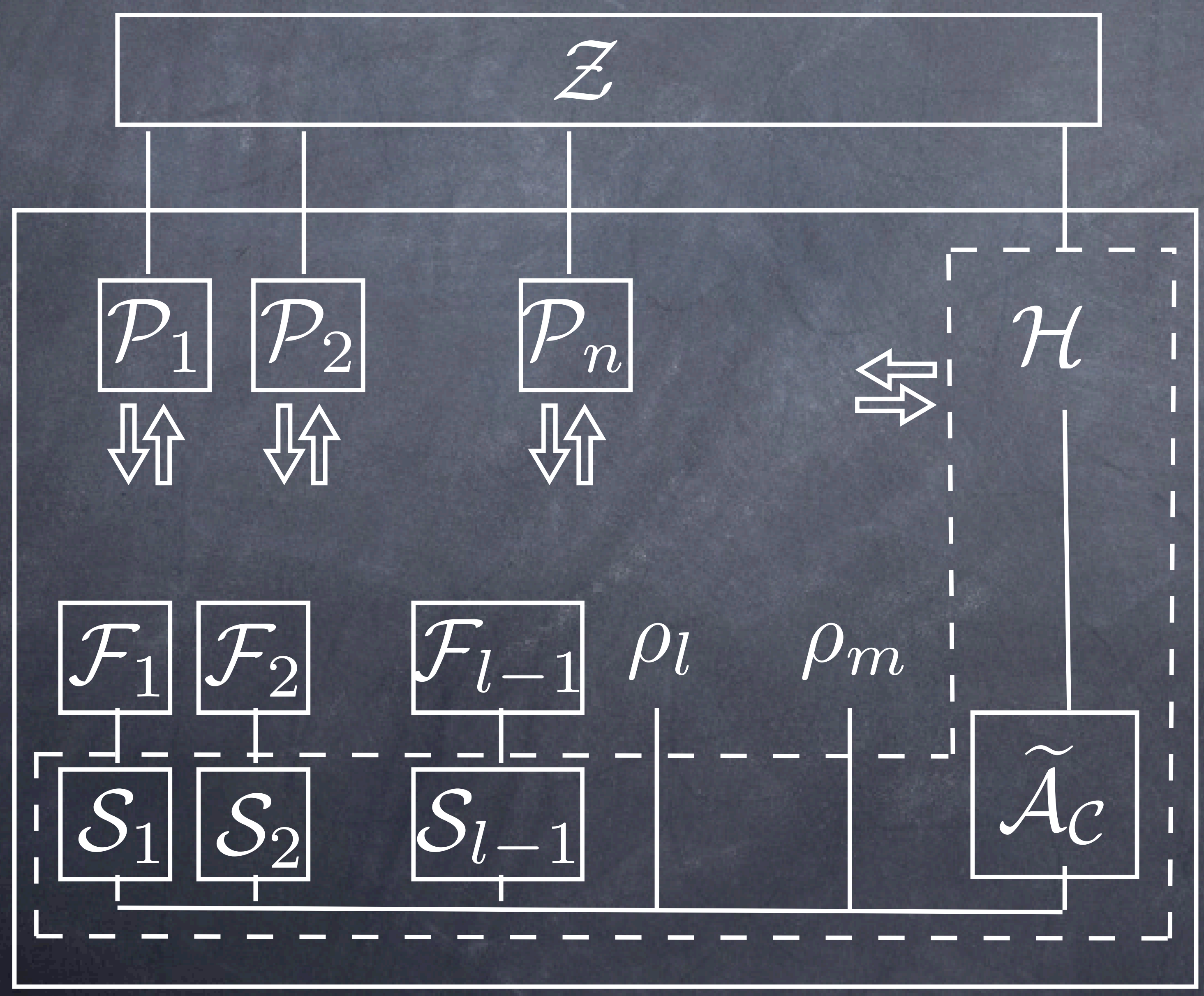
# Define Hybrid Adversary

- $\mathcal{H}$ needs to handle requests from $\mathcal{Z}$ with respect to parties $\mathcal{P}_i$ and copies of $\rho$
- $\mathcal{Z}$ requests/messages relating to $\mathcal{P}_i$ are relayed from $\mathcal{P}_i$
- Requests/messages relating to $\rho$: $\mathcal{H}$ mimics ideal $\mathcal{S}$ for request

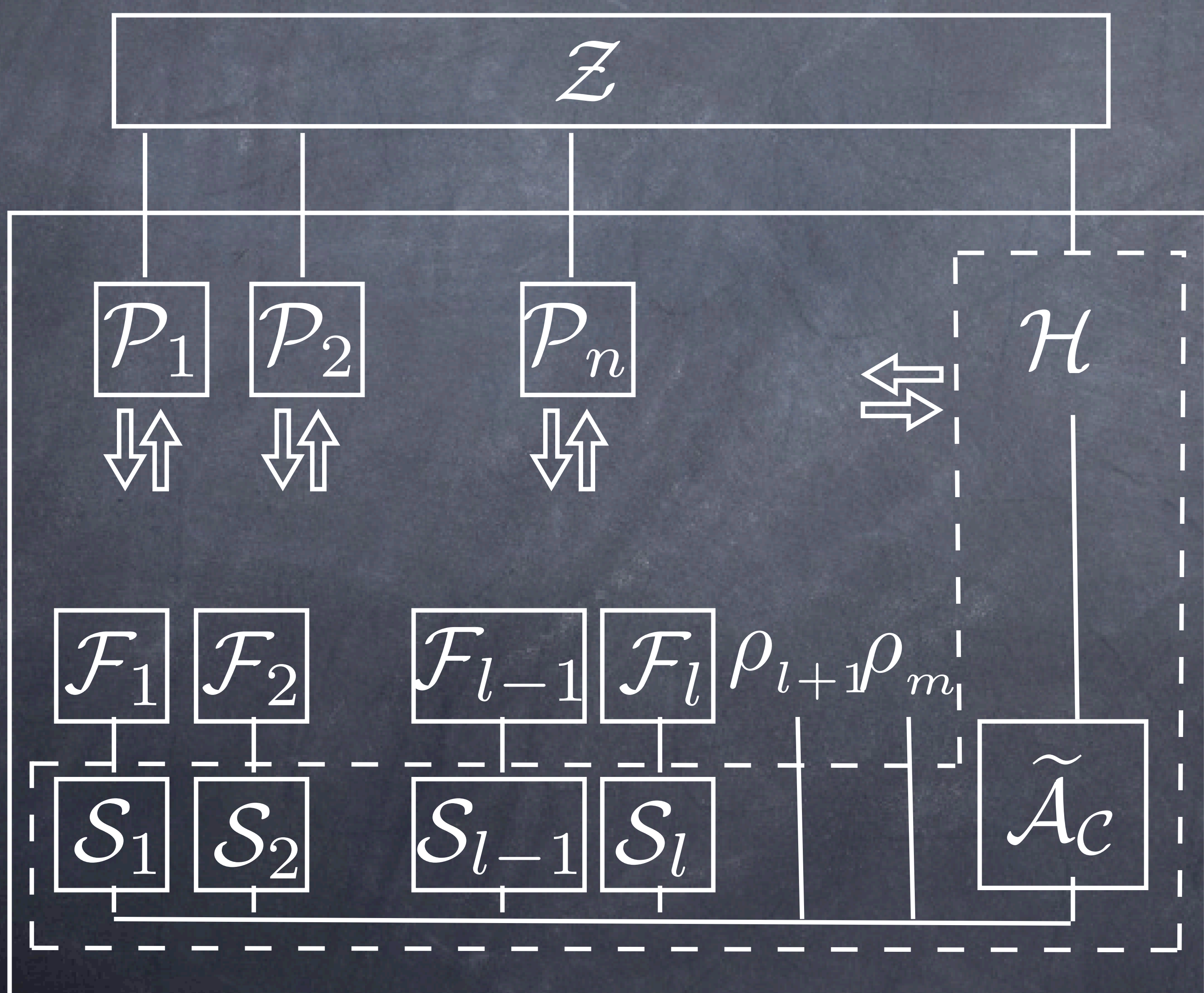
# The Hybrid adversary



# The (l-1) Hybrid model



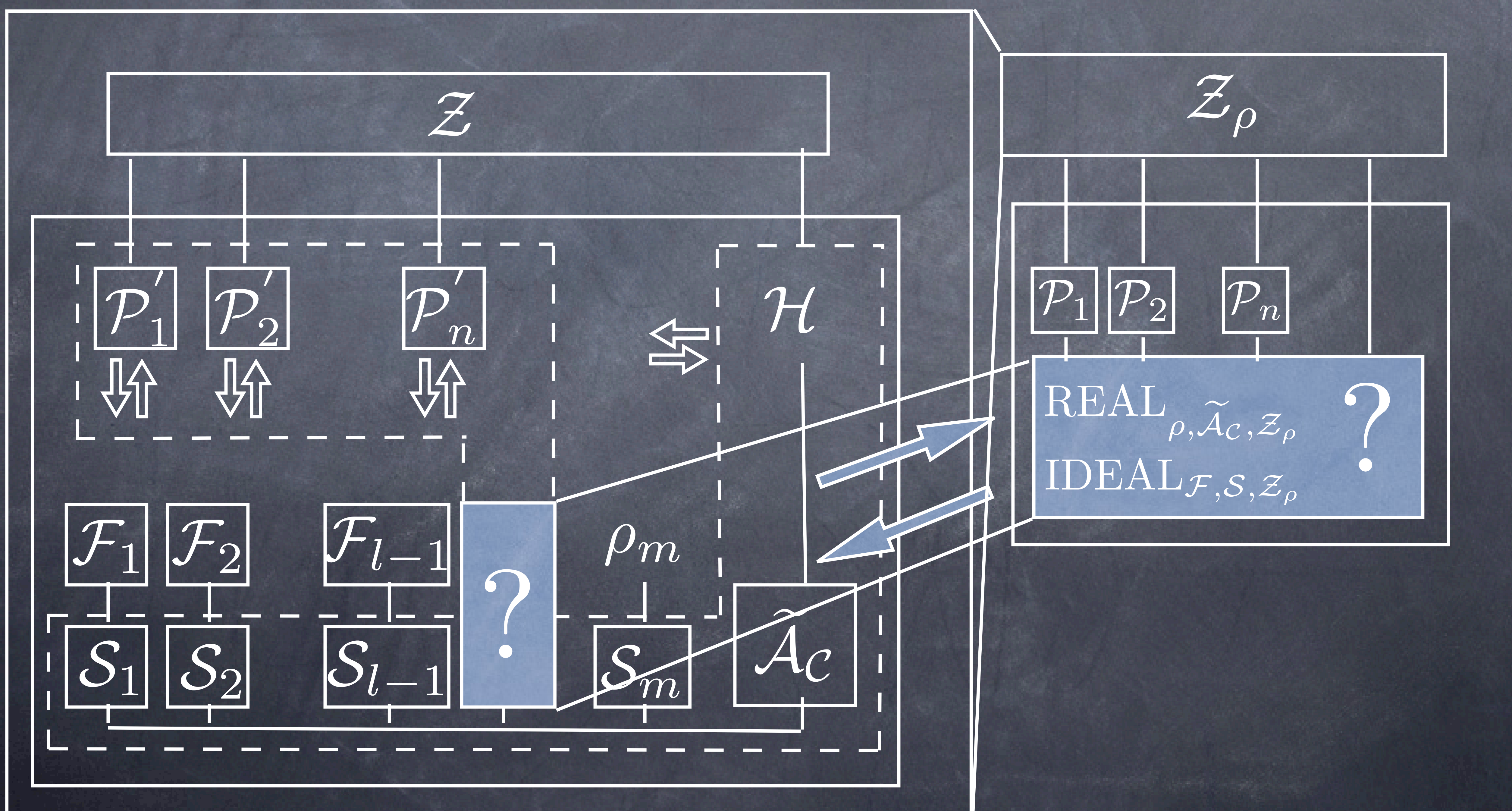
# The l-Hybrid model



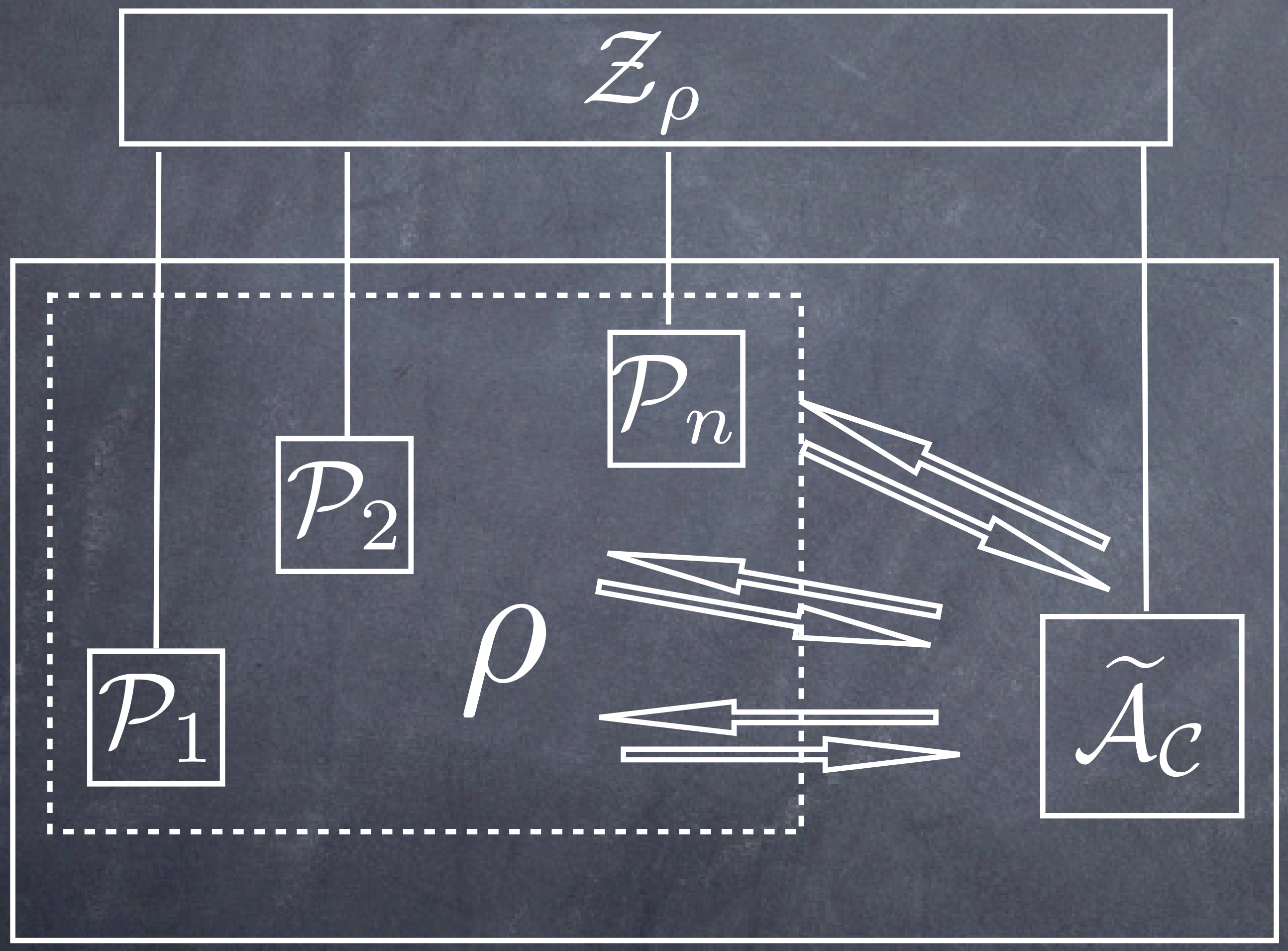
# Hybrid Argument

- Let m be a bound on invocations of $\rho$ in $\pi$
- 0-hybrid is real model for $\pi^\rho$
- m-hybrid is hybrid model
- Environments that can tell between real and Hybrid can tell between l-1 and l hybrid for some l.
- Reasoning: if all gaps small, then real vs hybrid gap is small

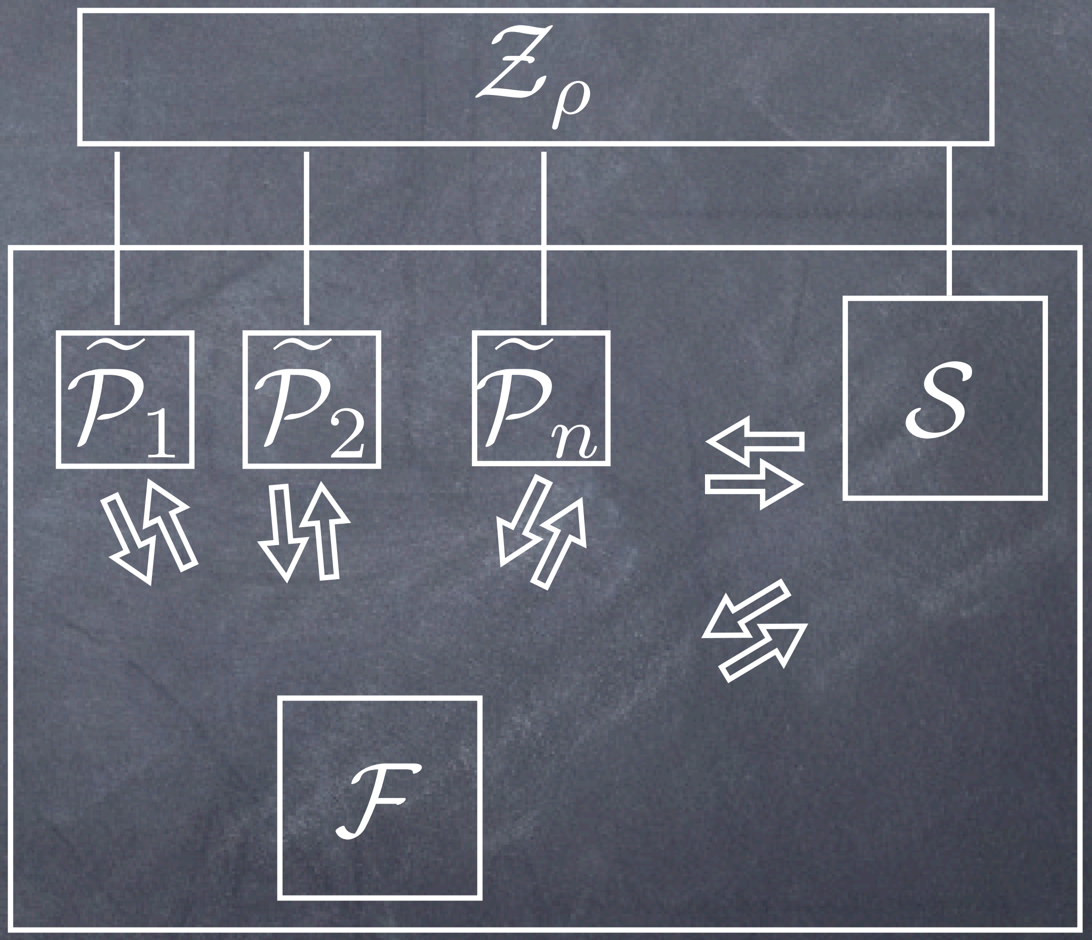
# Reduction: real vs ideal to hybrid l-1 vs l



# Real vs Ideal




$\mathrm{REAL}_{\rho,\widetilde{\mathcal{A}}_{\mathcal{C}},\mathcal{Z}_\rho}$




$\mathrm{IDEAL}_{\mathcal{F},\mathcal{S},\mathcal{Z}_\rho}$