ProNoBiS
Activities in Verona

Roberto Segala
University of Verona

with Augusto Parma and Andrea Turrini

List of Activities

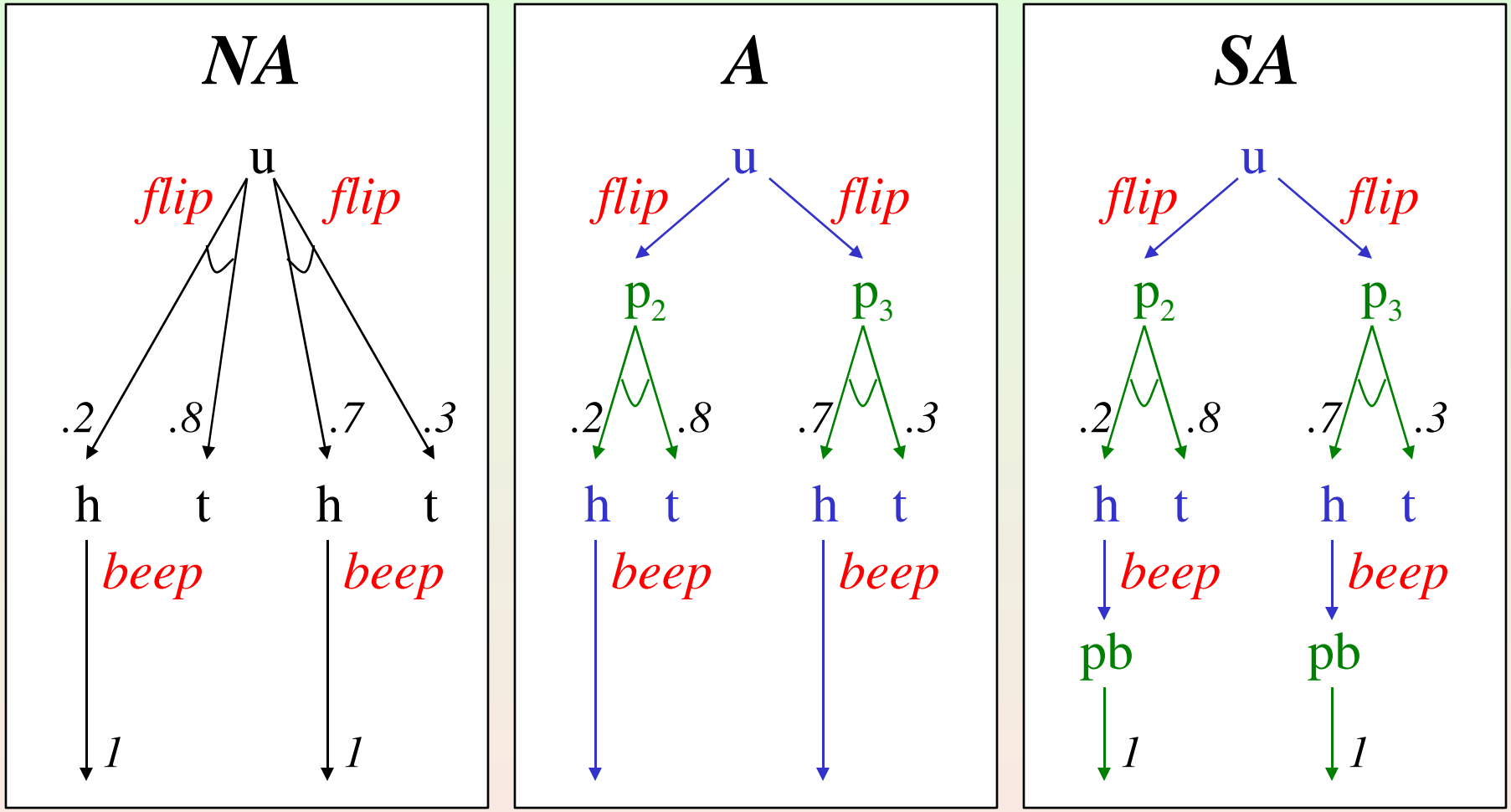
- Comparative semantics
  - Alternating and non-alternating models
  - Simulation and bisimulation relations
- Logical characterizations
  - Extensions of HM logic
- Non-discrete measures
  - Stochastic Transition Systems
- Verification of crypto protocols
  - Task-based PIOAs
    - Oblivious transfer
  - Aproximate simulations
    - Authentication, matching conversations

Probabilistic Automata (NA)

$$NA = (Q\ ,\ q_0,\ E\ ,\ H\ ,\ D)$$

- Q: States
- $q_0 \in Q$: Initial state
- $E \cap H = \emptyset$: External actions
- H: Internal (hidden) actions
- $D \subseteq Q \times (E \cup H) \times \mathrm{Disc}(Q)$: Transition relation

Alternating vs. non-alternating



Relations between models

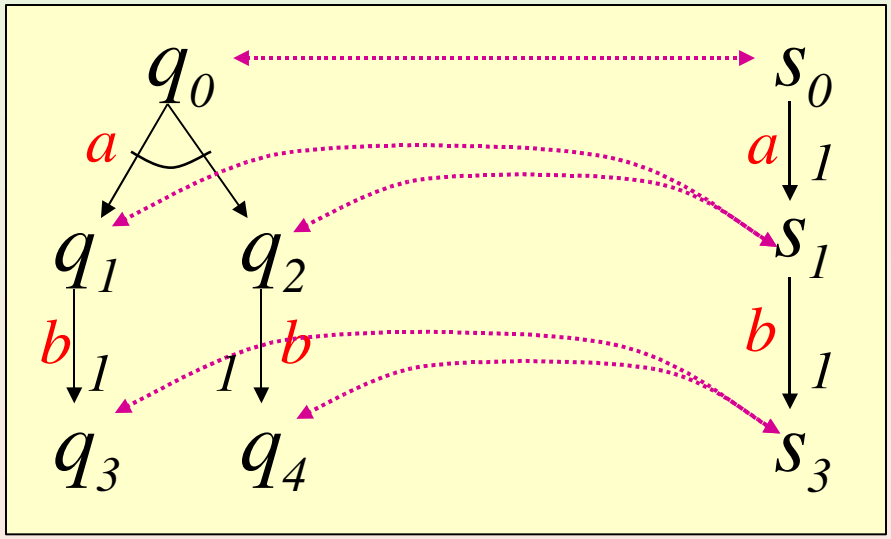
- Embeddings (E)
  - SA as an instance of A and of NA
  - A as an instance of NA
  - Embeddings as structure restrictions
- Transformations (T)
  - Folkloristic ways to represent the same object within the three models

Strong Bisimulation of *NA*

Strong bisimulation between A_1 and A_2

Relation $R \subseteq Q \times Q$,

$Q = Q_1 \uplus Q_2$, such that



$\forall\, q, s, a, \mu \;\exists\, \mu'$

$q \xrightarrow{a} \mu$

R $\qquad$ R

$s \xrightarrow{a} \mu'$

$\mu \, R \, \mu'$ [LS89]

$\Leftrightarrow$

$\forall C \in Q/R \,.\, \mu(C) = \mu'(C)$

Bisimulation Literature

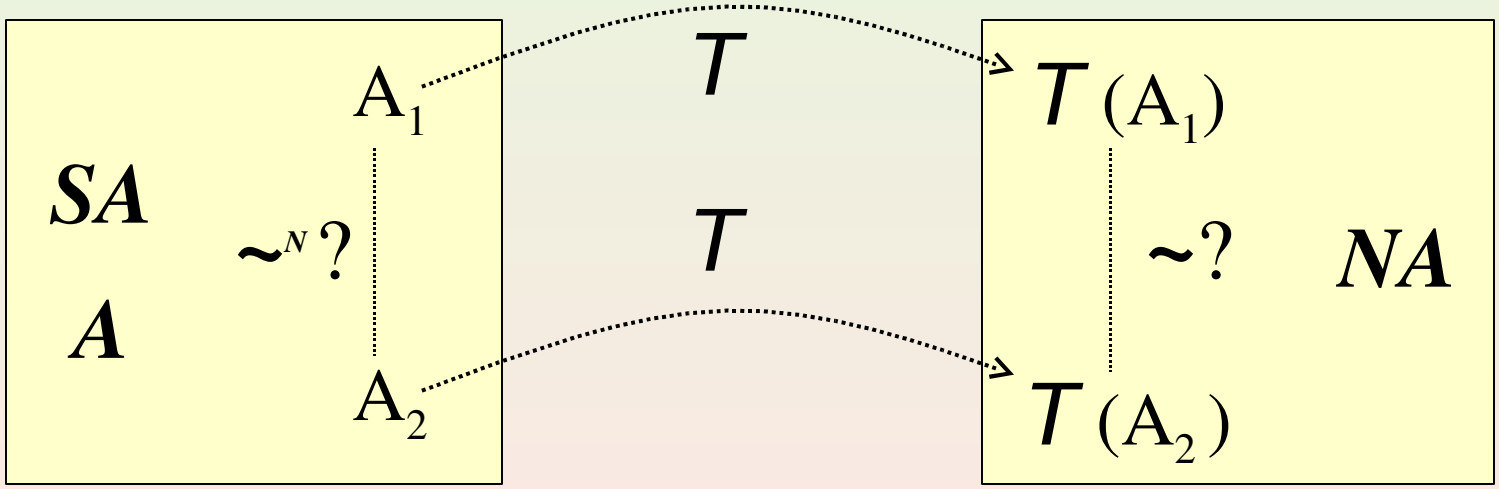
In literature there are also

- Strong bisimulation of Hansson on SA
  - Relates only nondeterministic states
- Strong bisimulation of Philippou on A
  - Relates all states
  - Probabilistic states are a technicality
- Weak bisimulation of Philippou on A
  - Relates all states
  - Probabilistic states are meaningful
  - Uses conditional probabilities on self loop

Taxonomy

Nondeterministic typology ***N***

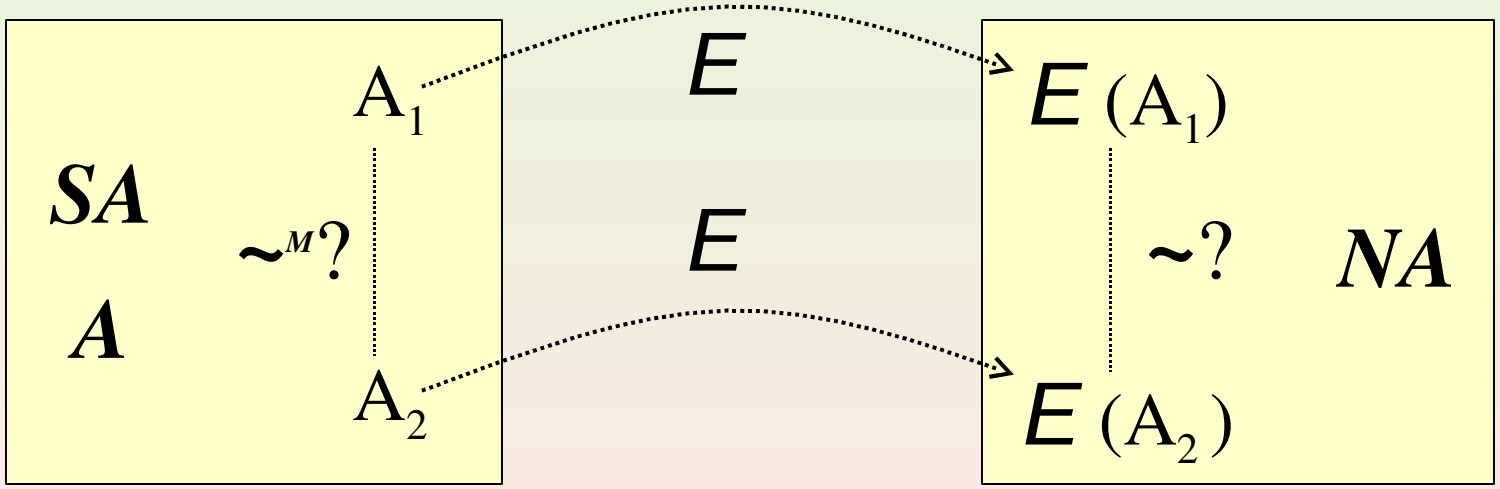
- Based on T ransformations
- Check bisimilarity of images in ***NA***



Taxonomy

Mixed typology ***M***

- Based on E mbeddings
- Check bisimilarity of images in ***NA***



Taxonomy and Literature [Segala, Turrini]

Equivalences	***SA***	***A***
Strong $\sim$	$\sim^{N}$ $\sim^{M}$	$\sim^{N}$
Weak $\approx$		$\approx^{pM}$

Logical Characterizations [Parma, Segala]

- Logic: true | $\neg\phi$ | $\phi \wedge \phi$ | $\langle a \rangle \phi$ | $[\phi]_p$
- Semantics: μ satisfies a formula
  - $\langle a \rangle \phi$: for each q in support of μ there is a transition (q,a,μ') such that $\mu' \models \phi$
  - $[\phi]_p$: $\mu(\{q \mid q \models \phi\}) \geq p$
- Observation: $\langle a \rangle_p \phi$ corresponds to $\langle a \rangle [\phi]_p$

Stochastic Transition Systems [Cattani, Segala, Kwiatkowska, Norman]

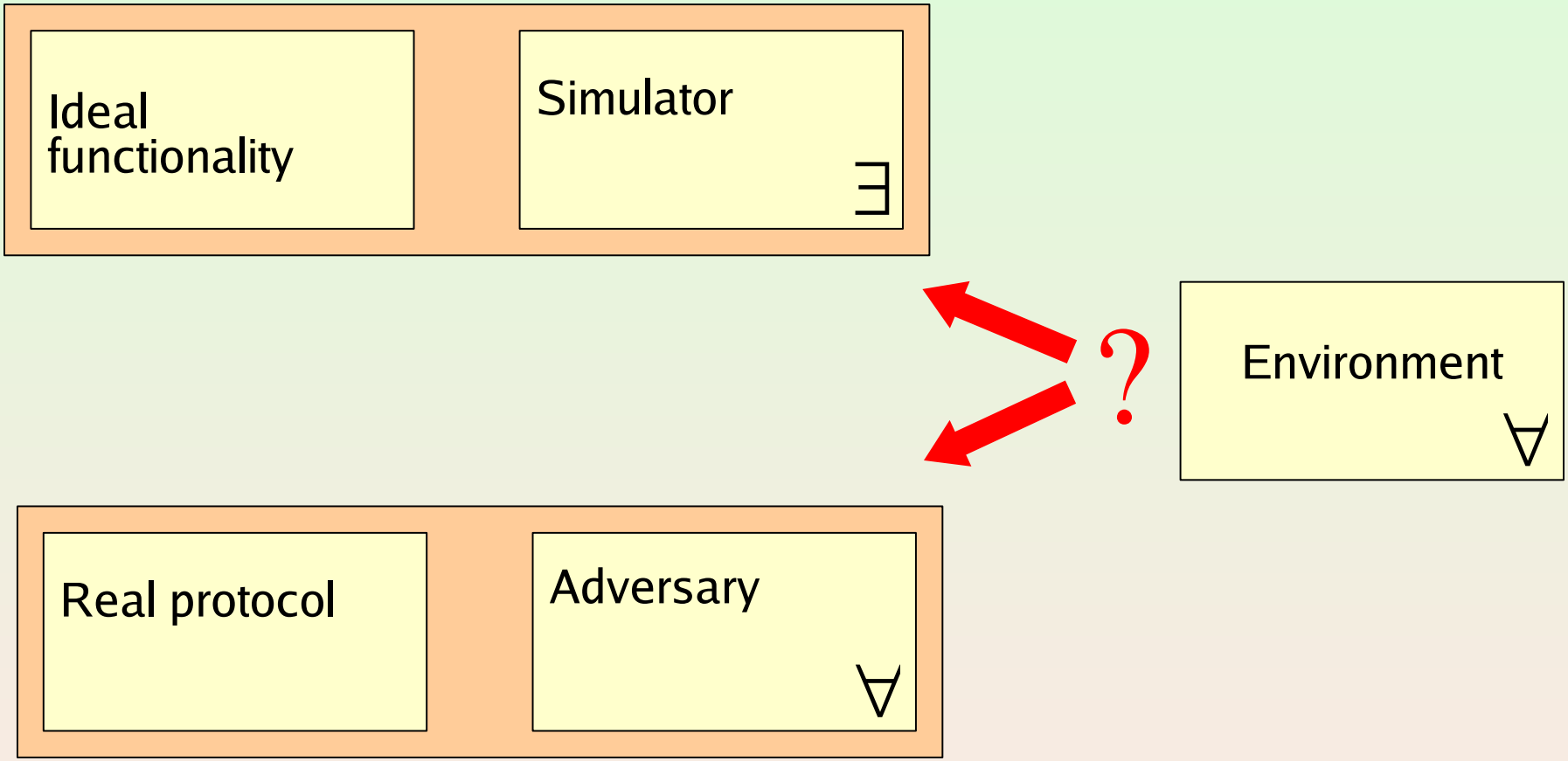
$$ST = (Q\ ,\ q_0,\ E\ ,\ H\ ,\ F_Q,\ F_A,\ D)$$

- Transition relation $D \subseteq Q \times (E \cup H) \times \mathrm{P}(Q, F_Q)$
- σ-field on actions
- σ-field on states
- Internal (hidden) actions
- External actions: $E \cap H = \emptyset$
- Initial state: $q_0 \in Q$
- States

STS: Problems

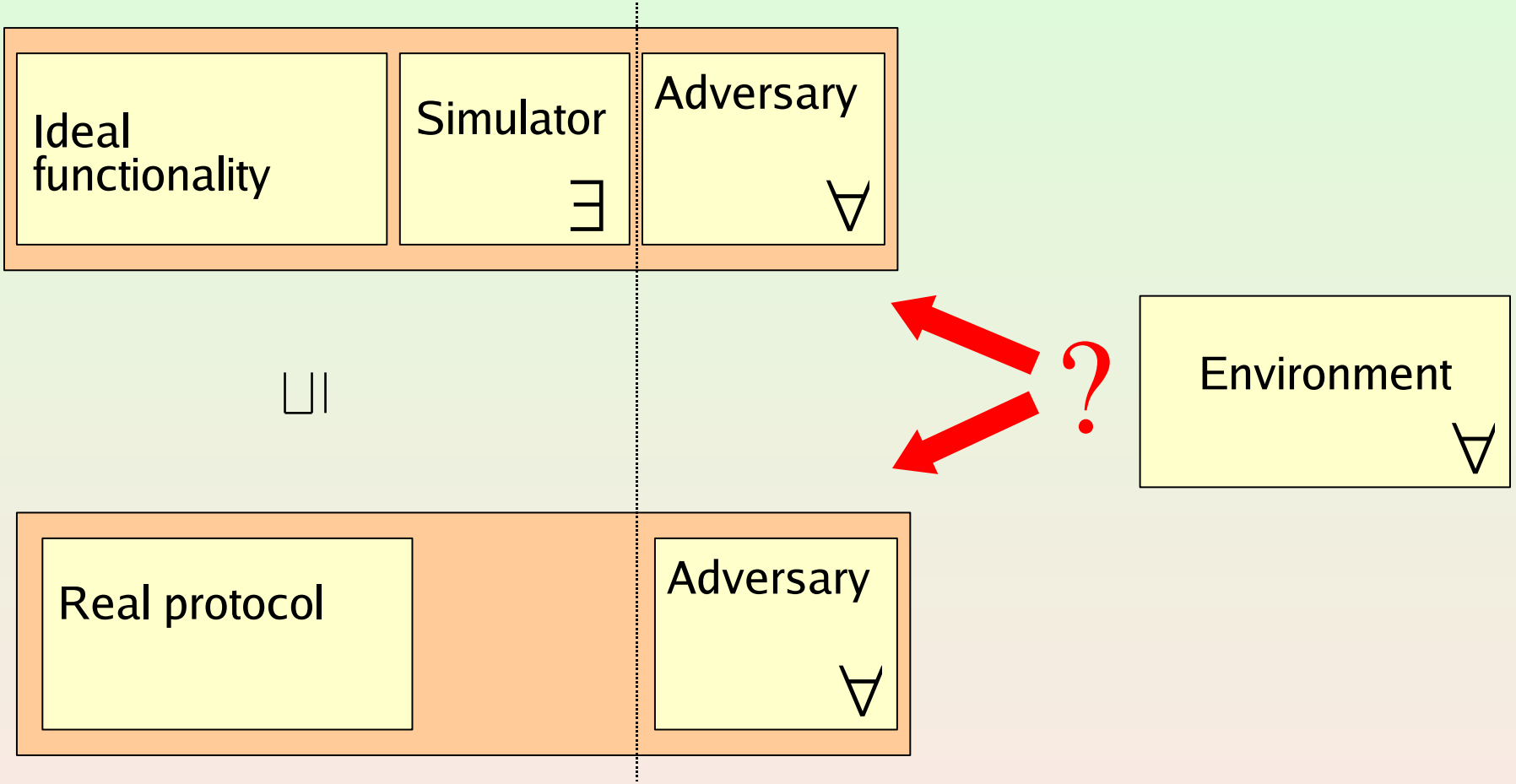
- Not all schedulers lead to measurability
  - Let $X \subseteq [0,1]$ be non measurable
  - Choose x uniformly in $[0,1]$
  - Schedule a only if $x \in X$
  - What is the probability of $\Diamond a$?
- Define measurable schedulers
  - From F_{EXEC} to $F_{A \times Q}$
  - Then we obtain Markov Kernels
- Markow kernels preserved by projection
  - Important for modular reasoning
- How about bisimulation?

UC-Security [Canetti]



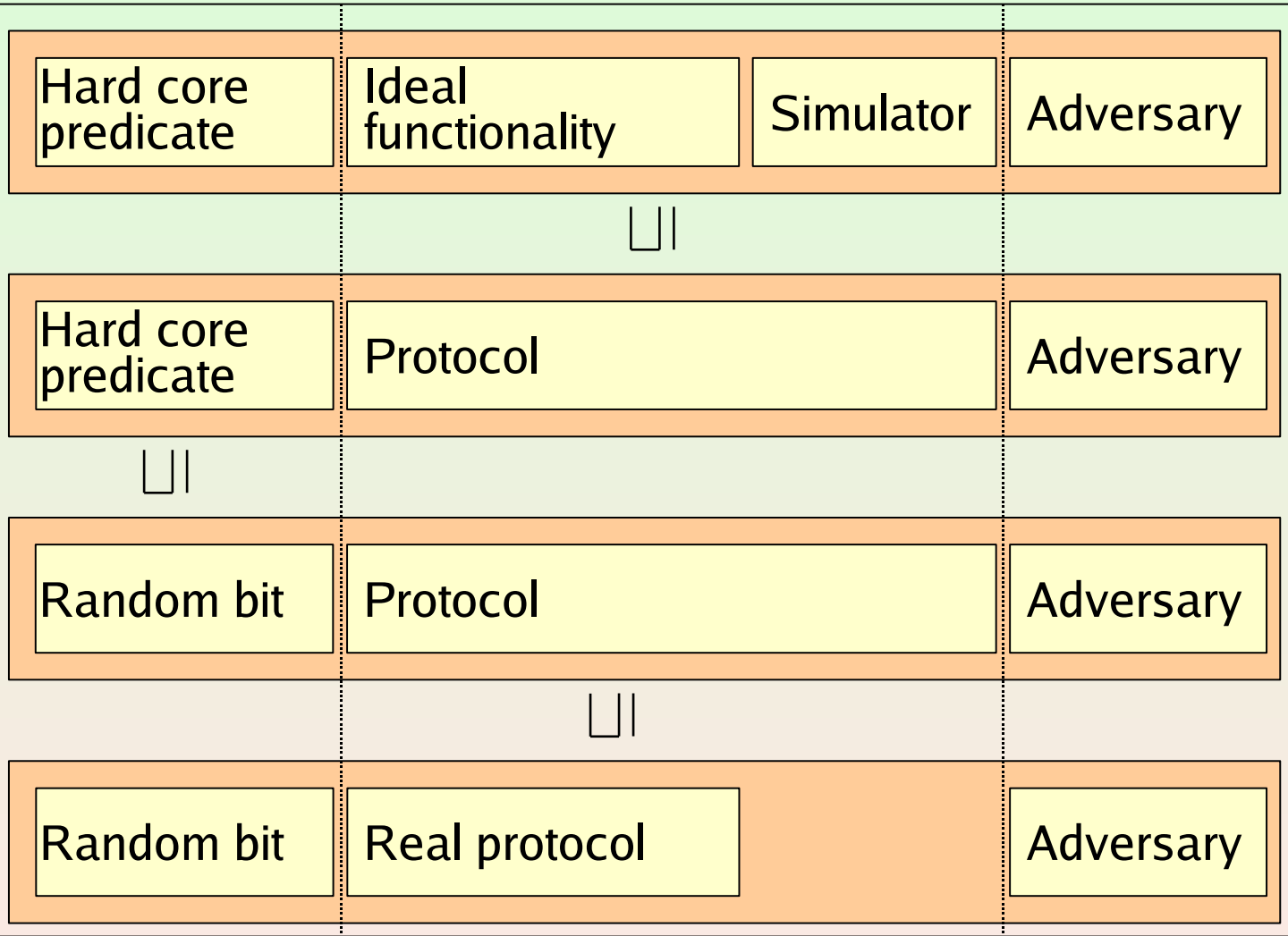
UC-Security with PIOAs

[Canetti, Cheung, Kaynar, Liskov, Lynch, Pereira, Segala]



Oblivious Transfer

[Canetti, Cheung, Kaynar, Liskov, Lynch, Pereira, Segala]



Aproximate Simulations [Segala, Turrini]

Given $\{A_k\}$ and $\{B_k\}$ consider $\{R_k\}$. $\quad R \subseteq Q_{Ak} \times Q_{Ak}$

For each c∈N, p∈Poly, exists k∈N, for each k>k, ε >0, μ1, μ2

If +

$\forall\ \mu_1$ *reached in at most p(k) steps*

$\forall\ \mu_1\ L(R_k,\varepsilon)\ \mu 2$

$\forall\ \mu_1 \longrightarrow \mu_1'$

Then

$\forall\ \mu_2 \longrightarrow \mu_2'$

$\forall\ \mu_1'\ L(R_k,\varepsilon+k^{-c})\ \mu 2'$

$\mu_1\ L(R,e)\ \mu_2$

$\forall\ \mu_1 = (1-\varepsilon)\mu_1' + \varepsilon\mu_1''$

$\forall\ \mu_2 = (1-e)\mu_2' + \varepsilon\mu_2''$

$\forall\ \mu_1'\ L(R)\ \mu_2'$

Implications on executions

Let $\{R_k\}$ be an aprox sim from $\{A_k\}$ to $\{B_k\}$

For each c∈ N, p∈ Poly, exists k∈ N, for each k>k, μ1

If

∀ μ1 is reachable in A_k in p(k) steps

Then exists μ_2

∀ μ_2 reachable in B_k in p(k) steps

∀ μ1 L(R,p(k)k^{-c}) μ_2

Application to Authentication Matching Conversation

- Specification:
  - Actual protocol
  - States keep history
  - Adversary does almost everything
  - All invalid transitions removed
- Implementation
  - Actual protocol
  - States keep history
  - Adversary is a PPT algorithm
- Simulation
  - Identity on states
- Properties
  - All executions of specification satisfy matching conversations
  - Failure of simulation imply breaking a signature protocol

Open problems

- Logics
  - Complete the picuture with simulations
- Stochastic Transition Systems
  - Understand bisimulation
  - Get soundness results
  - Understand restrictions to the model
- Verification
  - Refine the methods
  - Test on more complex case studies
  - Compare with soundness proofs for symbolic methods