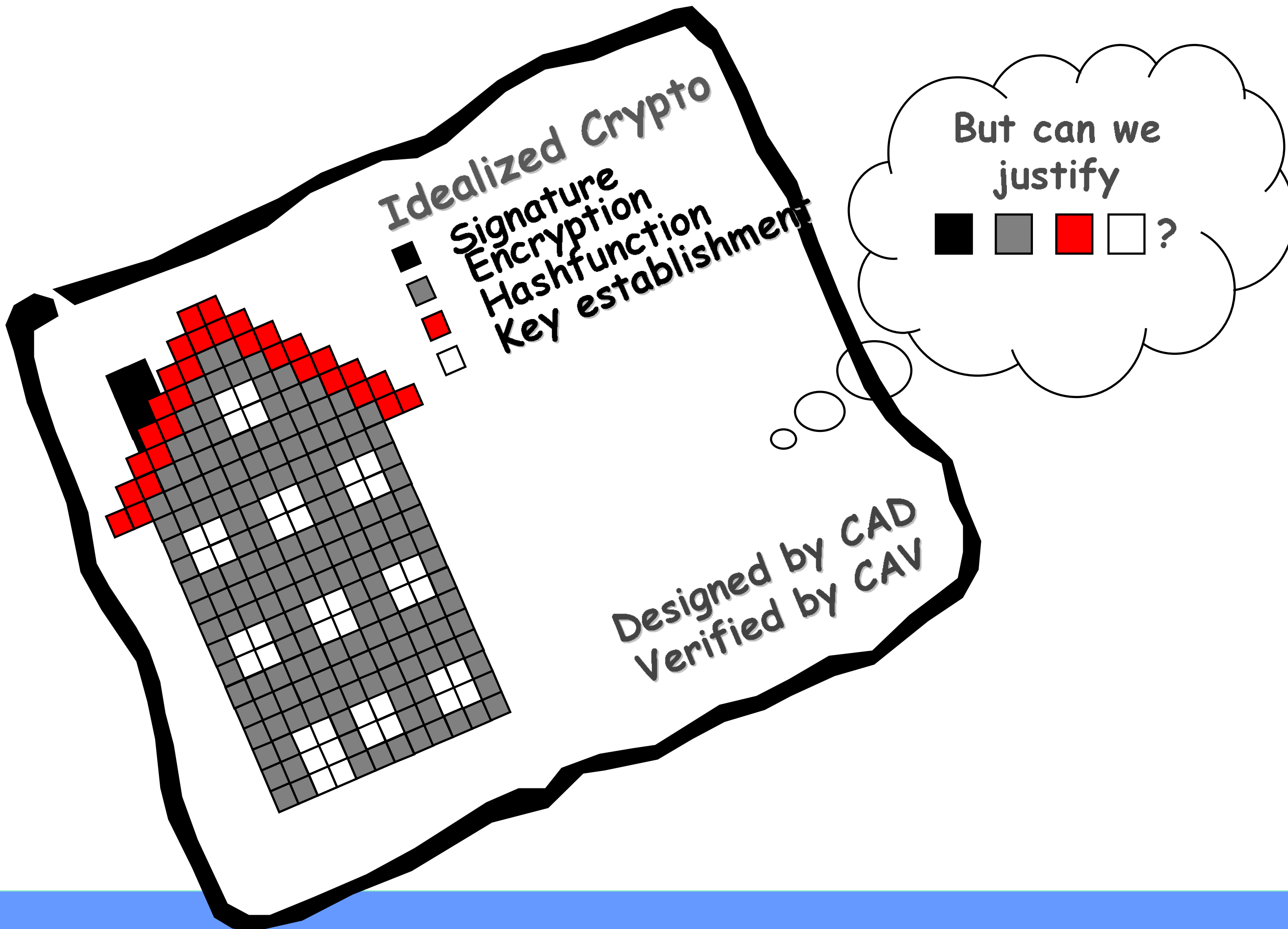
Michael Backes
Saarland University, Germany
joint work with Birgit Pfitzmann and Michael Waidner

Secure Reactive Systems, Day 2:

Reactive Simulatability – Composition and First Applications

Tartu, 02/28/06

Recall the Big Picture



Recall the RS Framework

- **Precise system model allowing cryptographic and abstract operations**
- **Reactive simulatability** with composition theorem
- Preservation theorems for security properties
- Concrete pairs of idealizations and secure realizations
- Sound symbolic abstractions (Dolev-Yao models) that are suitable for tool support
- Sound security proofs of security protocols: NSL, Otway-Rees, iKP, etc.
- Detailed Proofs (Poly-time, cryptographic bisimulations with static information flow analysis, …)

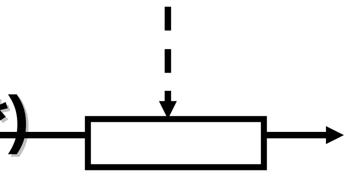
Recall the RS Framework

- Precise system model allowing cryptographic and abstract operations
- **Reactive simulatability with composition theorem**
- Preservation theorems for security properties
- **Concrete pairs of idealizations and secure realizations**
- Sound symbolic abstractions (Dolev-Yao models) that are suitable for tool support
- Sound security proofs of security protocols: NSL, Otway-Rees, iKP, etc.
- **Detailed Proofs** (**Poly-time**, cryptographic bisimulations with static information flow analysis, …)

Definitions Bottom-up

1. General Model:

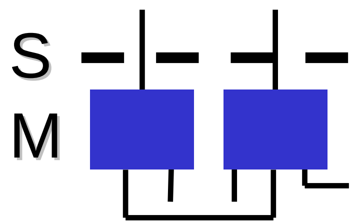
- **Collections of probabilistic I/O automata**
  - **connections via "ports"**
- **Turing machine realization (realistic)**
- **Timing**
  - **Asynchronous: Distributed scheduling via clock ports**
  - **Synchronous: Clk: Subrounds → P(M*)**



Definitions Bottom-up

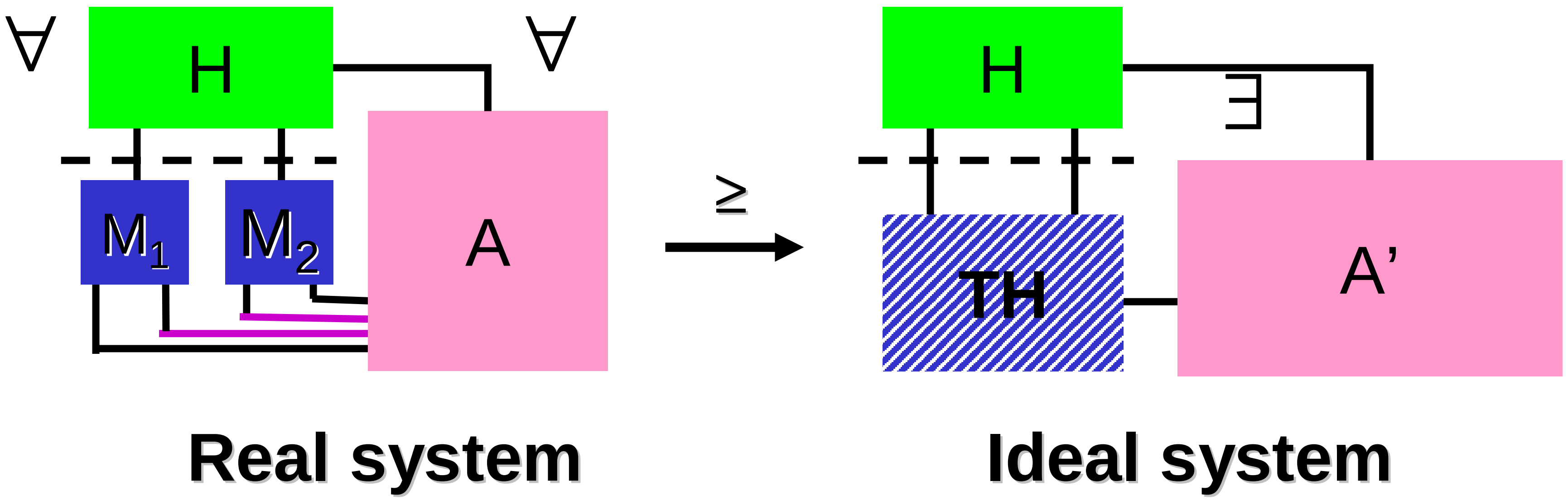
2. Security-Specific System Model:

- **Structure: (*M*, *S*) with *S* $\subseteq$ Ports(*M*) "service ports"**



- **Configurations: (*M*, *S*, H, A)**

Soundness: Reactive Simulatability



$$\text{view}_{\text{real}}(H) \approx \text{view}_{\text{ideal}}(H)$$

Indistinguishability of random variables

Indistinguishability [Yao_82]

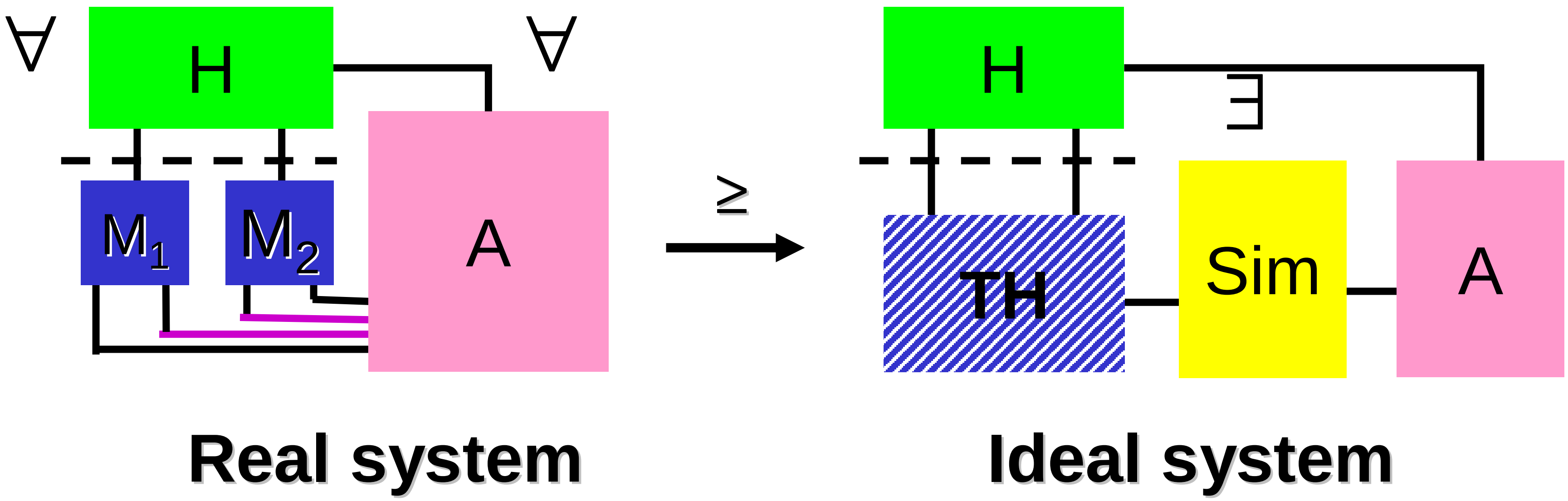
Families of random variables:

$$(v_k)_{k \in \mathrm{IN}} \approx_{\mathrm{poly}} (v'_k)_{k \in \mathrm{IN}}$$

$\Leftrightarrow \forall D$ **(prob. poly. in first input):**

$$|\ \Pr(D(1^k, v_k) = 1) - \Pr(D(1^k, v'_k) = 1)\ | \le 1 / \mathrm{poly}(k).$$

Blackbox Reactive Simulatability



$$\text{view}_{\text{real}}(H) \approx \text{view}_{\text{ideal}}(H)$$

Sufficient for black-box:

M_1+M_2 behave the same as TH+Sim

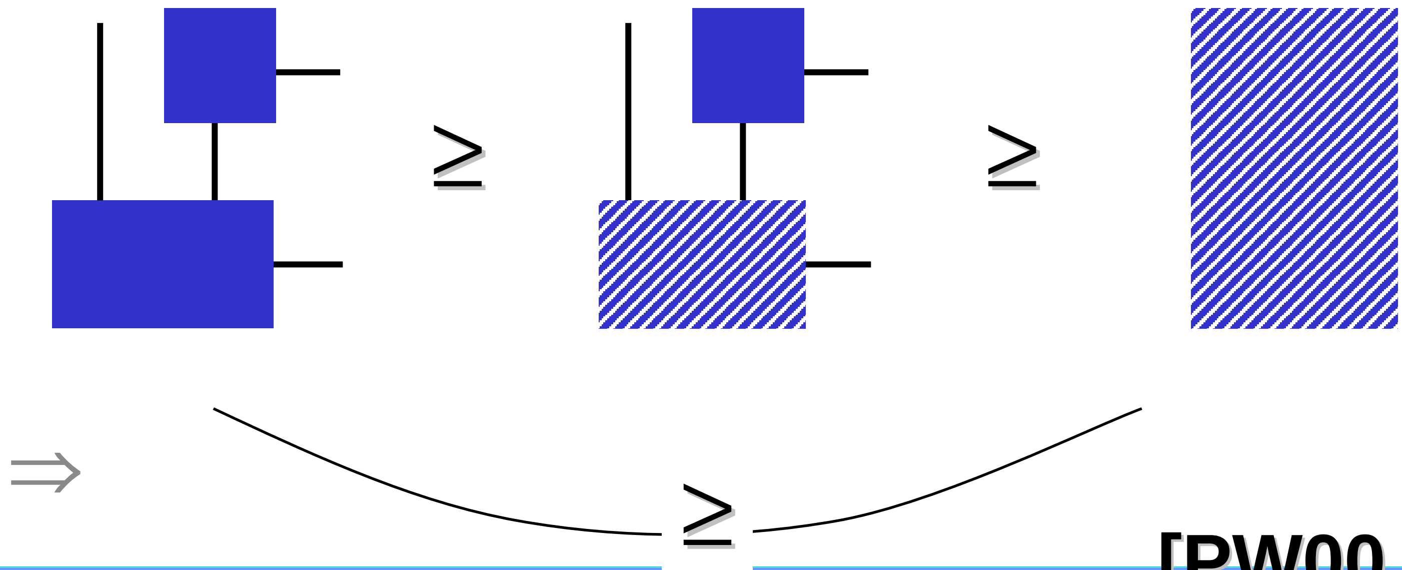
Some Simple Simulations

- **On the board…**

Base Lemmas about Reactive Simulatability

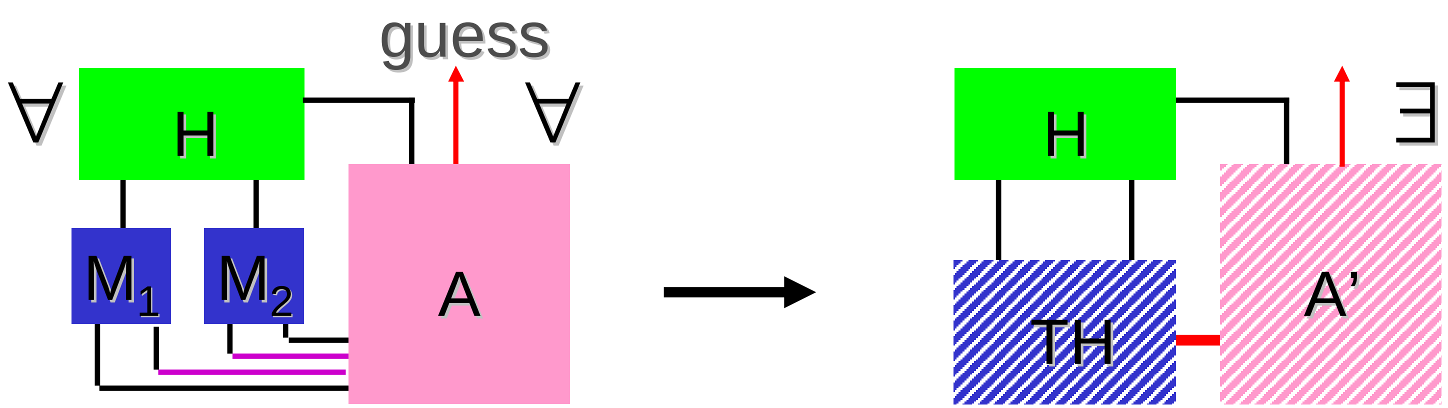
Base Lemmas (Examples)

- **Machine combination is defined and**
  - **is associative**
  - **retains poly-time (for strong version)**
  - **retains sub-machine views**
- **“As secure as” is transitive. E.g., with composition:**



[PW00,PW01]

Reactive Simulatability Variants



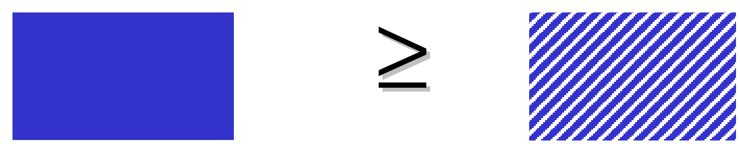
- **Equivalent with "guess"**
- **Standard simulatability: ∀A ∀H ∃A'**
- **Universal simulatability: ∀A ∃A' ∀H**
- **Blackbox simulatability: ∃Sim ∀H ∀A A'=Sim&A**
- **Perfect / statistic / computational**

Some Other Model Variants

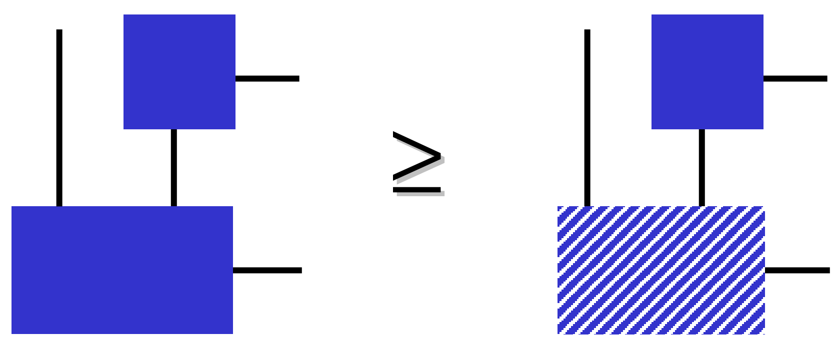
- Quantifier order [PSW00,L03,DKMRS04]
- Guessing output of adversary [PSW00]
- Different types of timing [PSW00,B03]
- Different use of “service ports” (≈ environments) [PSW00]
- Auxiliary inputs or not [PSW00]
- Mapping of LMMS,PW,C: [DKMRS04, A...04]
- Secure, insecure, authentic, reliable, broadcast channels [PSW00,BPSW02]
- Static and adaptive corruptions [PW01,C01]
- Proactive [BCS03]

Composition – One System

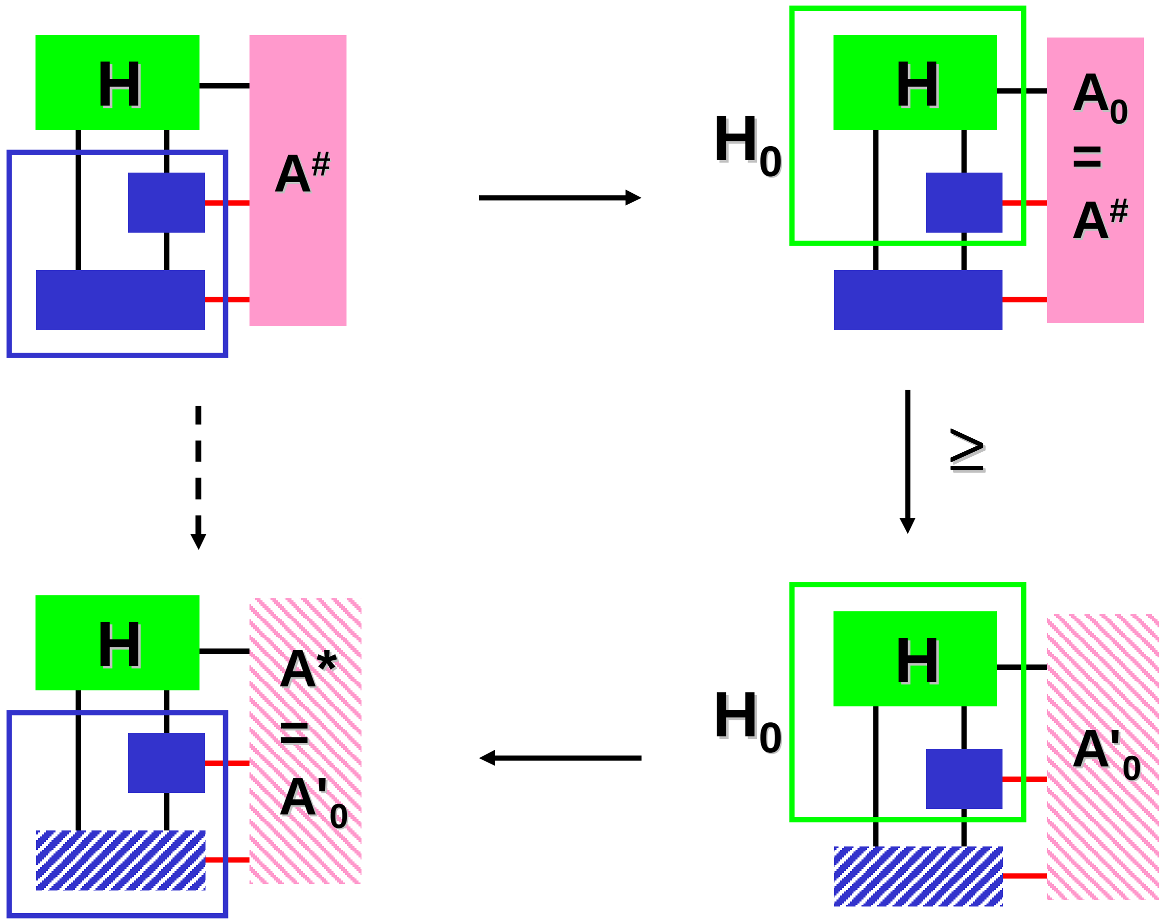
Given:



Then this holds:

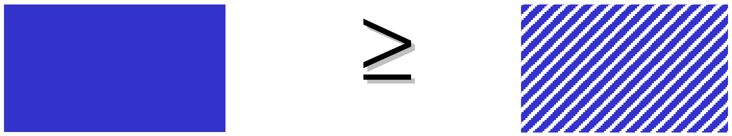


Proof Idea (Single Composition)

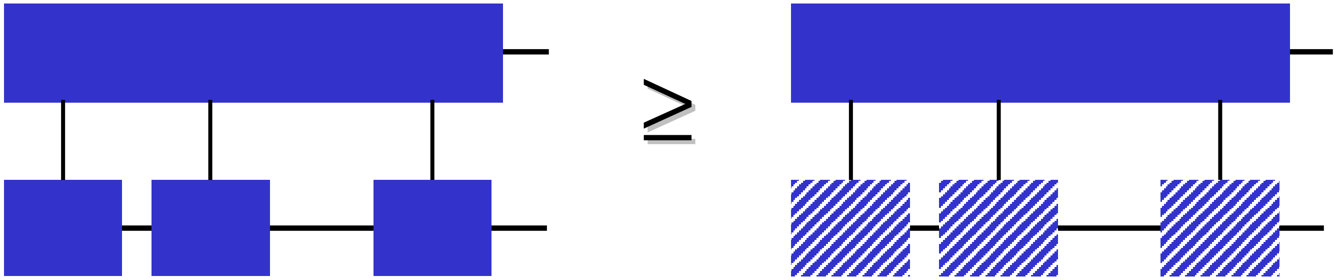


Composition – Multiple Systems

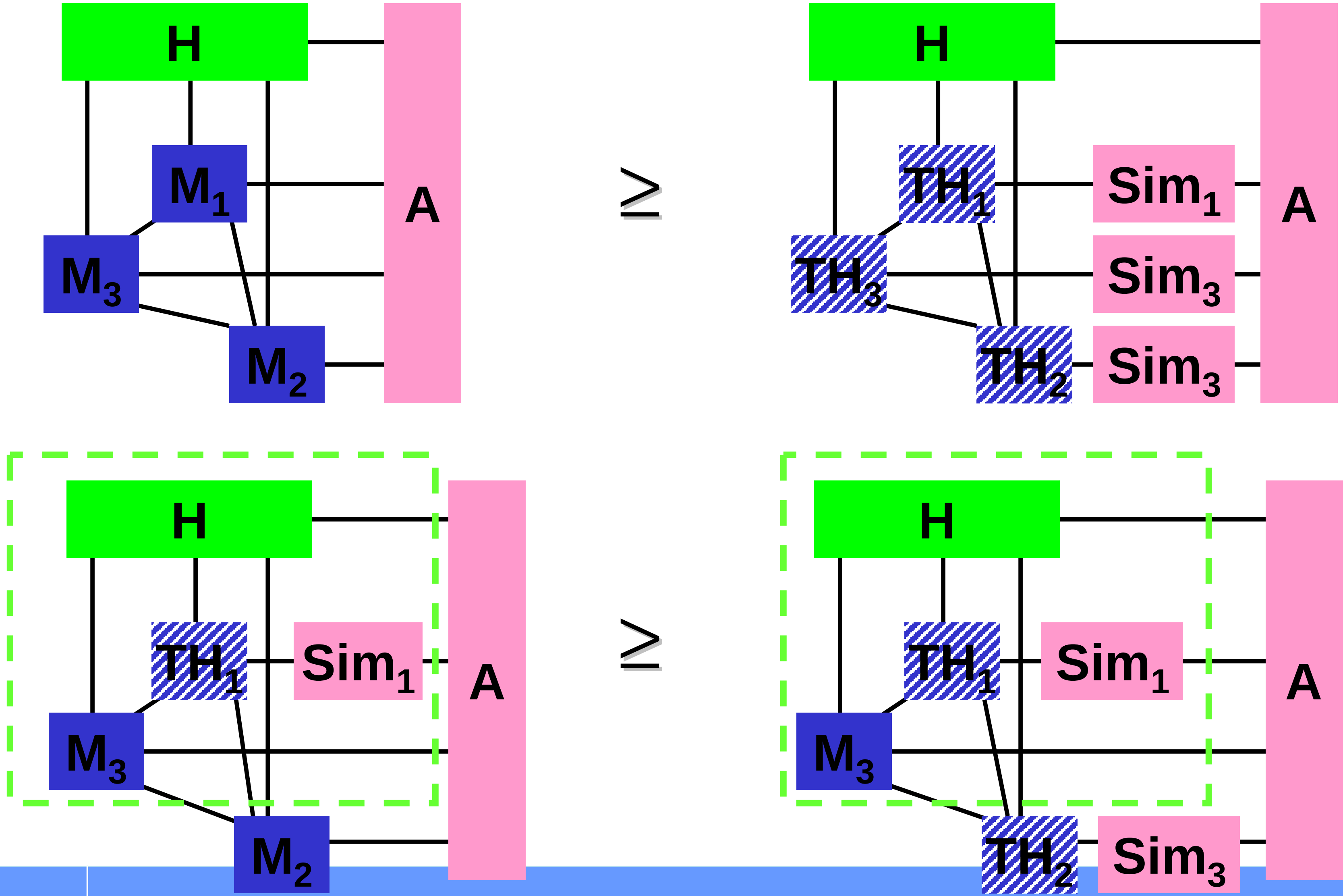
Given:



Also this holds:



General Composition Proof via Hybrid Systems



Composability Types

	Constant many identical prot.	Constant many different prot.	Poly many identical prot.	Poly many different prot.
General	[PW00, PW01] [L03]	[PW00,PW01] [L03]		
Universal	[PW00, PW01] [C01]	[PW00,PW01]	[C01] [BPW04]	[BPW04]
Blackbox	[PW00, PW01]	[PW00,PW01]	[BPW04]	[BPW04]