Temporal Information Flow

Markus N. Rabe

Universität des Saarlandes, Germany

Haifa, November 4th, 2012

Security-Critical Reactive Systems

- Reactive: ongoing interaction with external environment
- Security-critical: operates with confidential information
- (Multiple agents: Scripts, Plug-ins, User, OS, . . .)

In a nutshell

Security

- Many different security properties.
- We need a language for security properties.

In a nutshell

Security

- Many different security properties.
- We need a language for security properties.

Temporal Logics

- Temporal logics cannot compare paths.

In a nutshell

Security

- Many different security properties.
- We need a language for security properties.

Temporal Logics

- Temporal logics cannot compare paths.

LTL + Secrecy

- SecLTL, VMCAI 2012
- Property language for security-critical reactive systems

Example - an online registration form

- Last input to the text field of a form remains secret until “commit” button is pressed, and
- all other inputs stay secret forever.

Property language for security

Noninterference - Hide operator

The observable behaviour is independent of the secret.

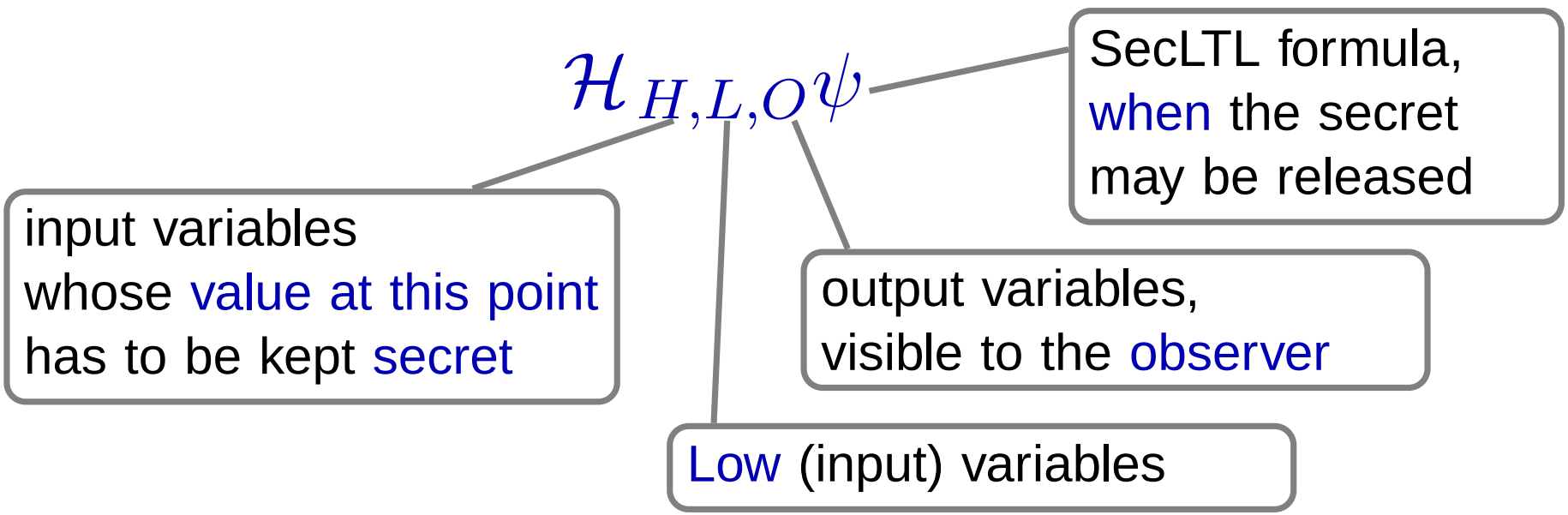
$$\varphi \quad ::= \quad p \quad | \quad \neg\varphi \quad | \quad \varphi \vee \psi \quad | \quad \bigcirc\varphi \quad | \quad \varphi \,\mathcal{U}\, \psi \quad | \quad \mathcal{H}_{H,L,O}\psi$$

SecLTL

- What is the secret?
- For how long?
- Under which conditions?

The Temporal Logic SecLTL

$$\varphi \quad ::= \quad p \quad | \quad \neg\varphi \quad | \quad \varphi \vee \psi \quad | \quad \bigcirc\varphi \quad | \quad \varphi \,\mathcal{U}\, \psi \quad | \quad \mathcal{H}_{H,L,O}\psi$$



$\mathsf{Vars} = \mathsf{InputVars} \,\dot\cup\, \mathsf{SysVars}; \quad O \subseteq \mathsf{SysVars}; \quad \mathsf{InputVars} = H \,\dot\cup\, L$

Temporal information flow - Examples

- Noninterference (Goguen & Meseguer):
  $$\Box \mathcal{H}_{H,L,O} \bot$$

Temporal information flow - Examples

- Noninterference (Goguen & Meseguer):
  $$\Box \mathcal{H}_{H,L,O} \bot$$
- Content of a critical browser session stays secret:
  $$\Box \big(\mathsf{session\_start} \rightarrow \mathcal{H}_{H,L,O} \bot \ \mathcal{U} \ \mathsf{session\_closed} \big)$$

Semantics of the Hide Operator $\mathcal{H}$

$$\pi \quad \models \quad \mathcal{H}_{H,L,O}\psi$$

Compares the sequence π to a set of alternative paths w.r.t. observational equivalence.

Semantics of the Hide Operator $\mathcal{H}$

$$\pi \models \mathcal{H}_{H,L,O}\psi$$

Definition (Alternative Paths)

$$\mathsf{Alt}(\pi, L, H) = \{\ \pi' \in \mathsf{Paths}_{\pi[0]} \mid \pi[0,\infty] =_L \pi'[0,\infty], \\ \pi[1,\infty] =_H \pi'[1,\infty]\ \}.$$

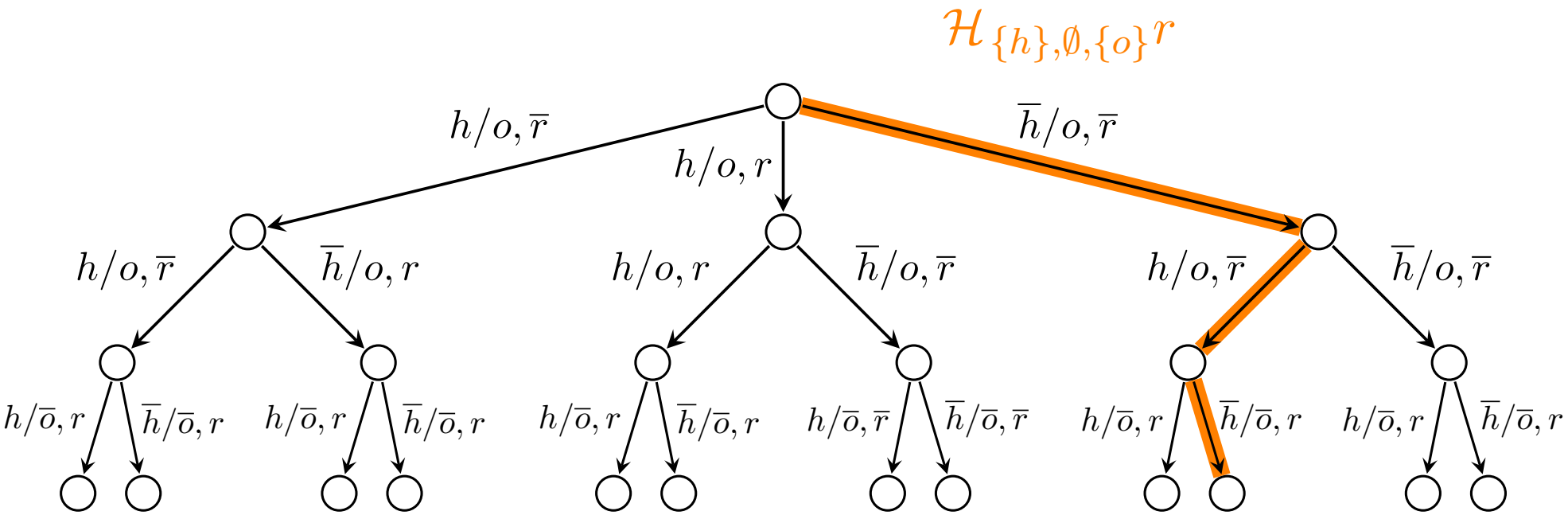
Semantics of the Hide Operator $\mathcal{H}$

$$\begin{aligned} \pi \models \mathcal{H}_{H,L,O}\psi \quad \text{if} \quad & \forall \pi' \in \mathsf{Alt}(\pi, L, H) : \\ & \pi =_O \pi' \quad \text{or} \\ & \exists i \in \mathbb{N} : \ \pi[0,i] =_O \pi'[0,i] \ \wedge \ \pi[i,\infty] \models \psi \end{aligned}$$

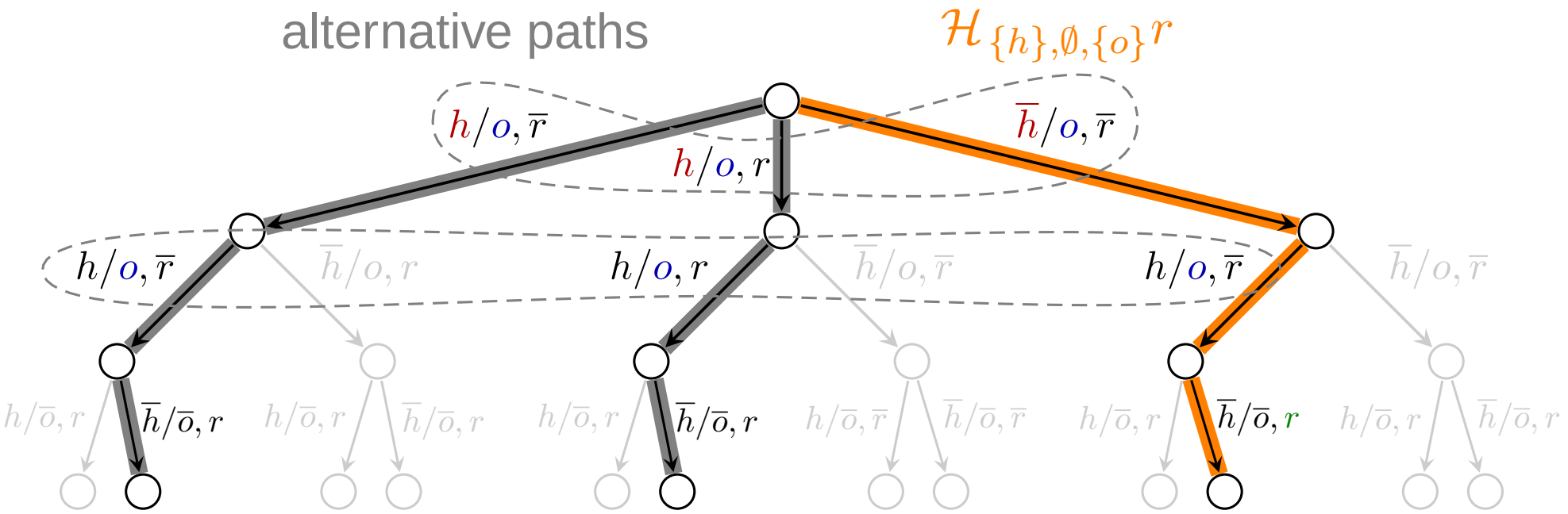
Definition (Alternative Paths)

$$\begin{aligned} \mathsf{Alt}(\pi, L, H) = \{ \pi' \in \mathsf{Paths}_{\pi[0]} \mid & \pi[0,\infty] =_L \pi'[0,\infty], \\ & \pi[1,\infty] =_H \pi'[1,\infty] \}. \end{aligned}$$

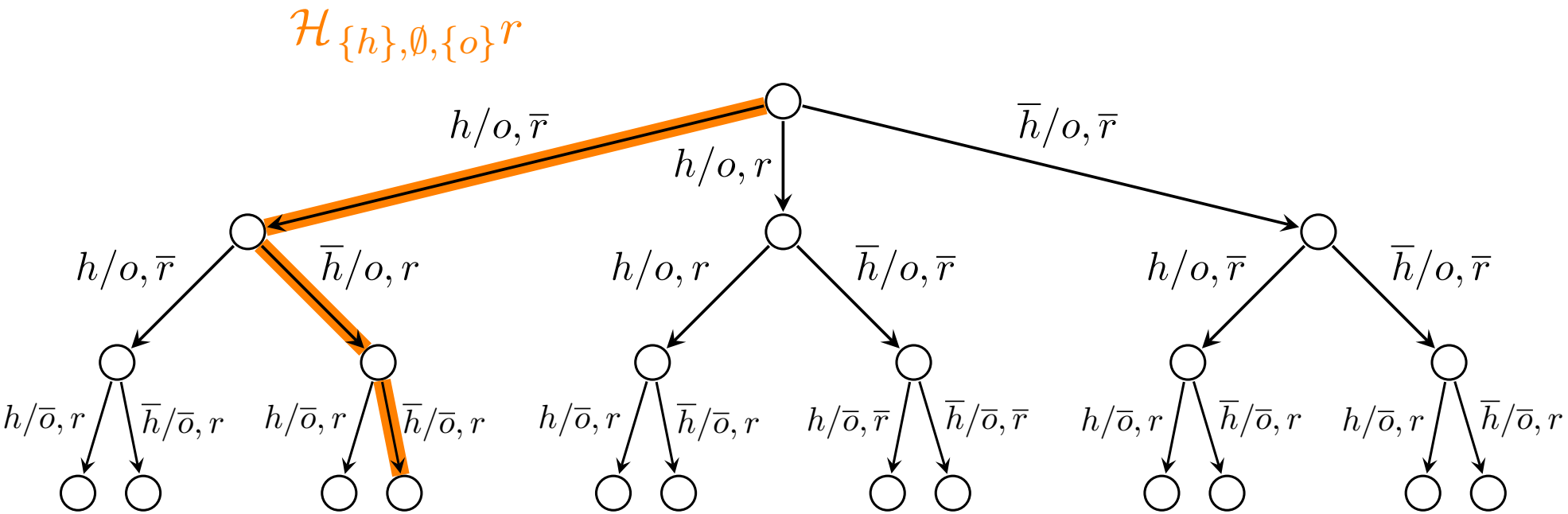
Semantics of the Hide Operator $\mathcal{H}$ (2)



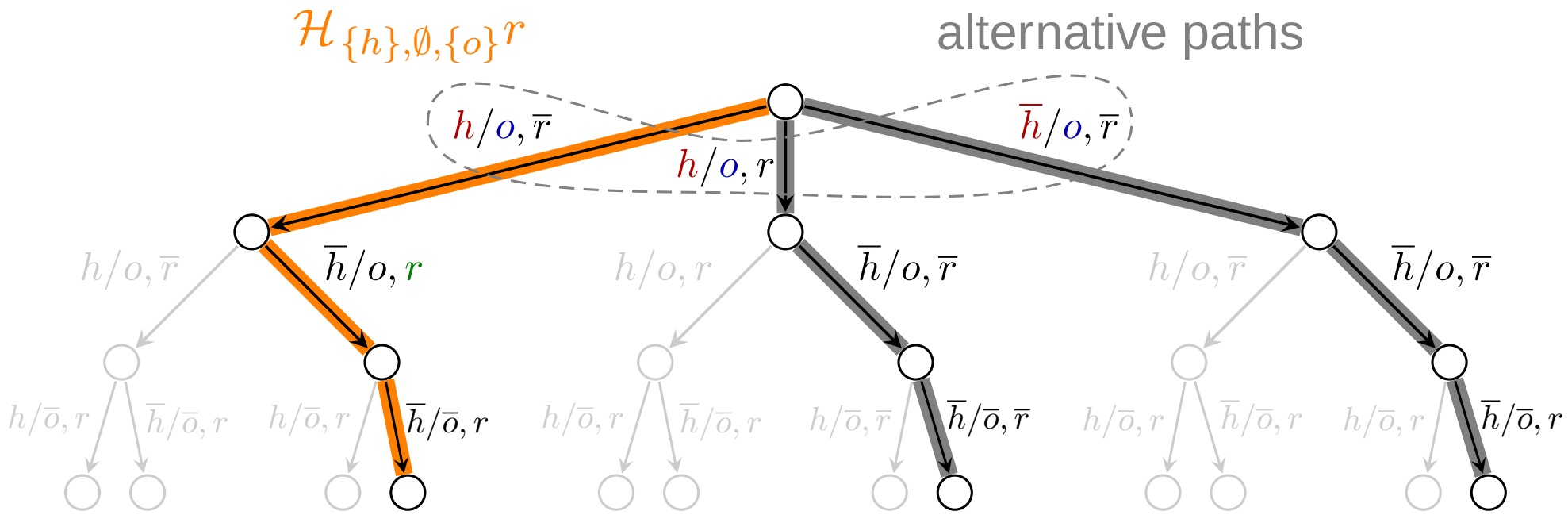
Semantics of the Hide Operator $\mathcal{H}$ (2)



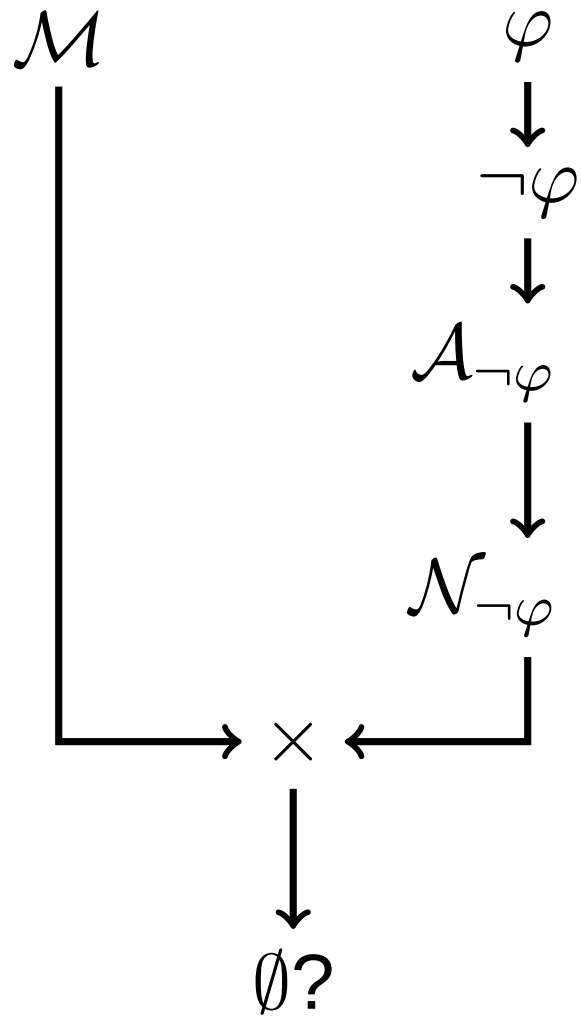
Semantics of the Hide Operator $\mathcal{H}$ (2)



Semantics of the Hide Operator $\mathcal{H}$ (2)



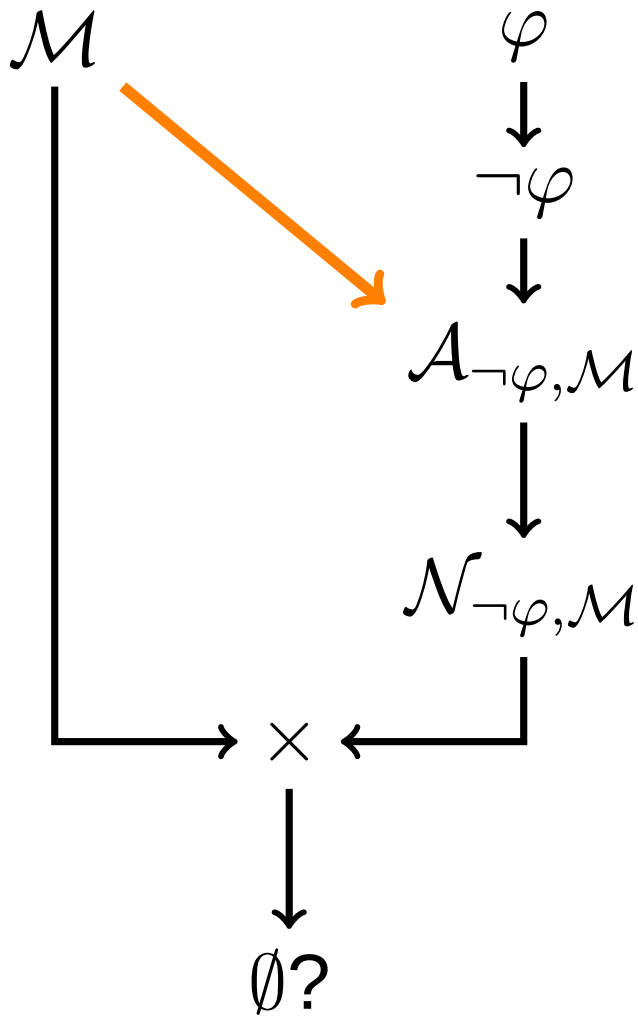
Model Checking LTL



Model Checking SecLTL

Algorithm

1. construct ABA $\mathcal{A}_{\mathcal{M},\neg\varphi}$
2. translate to NBA $\mathcal{N}_{\mathcal{M},\neg\varphi}$
3. check $\mathcal{L}(\mathcal{N}_{\mathcal{M},\neg\varphi} \times \mathcal{M}) = \emptyset$

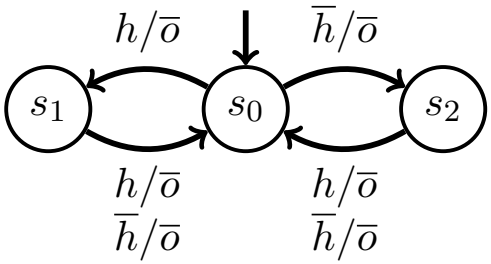


Model Checking SecLTL - An Example

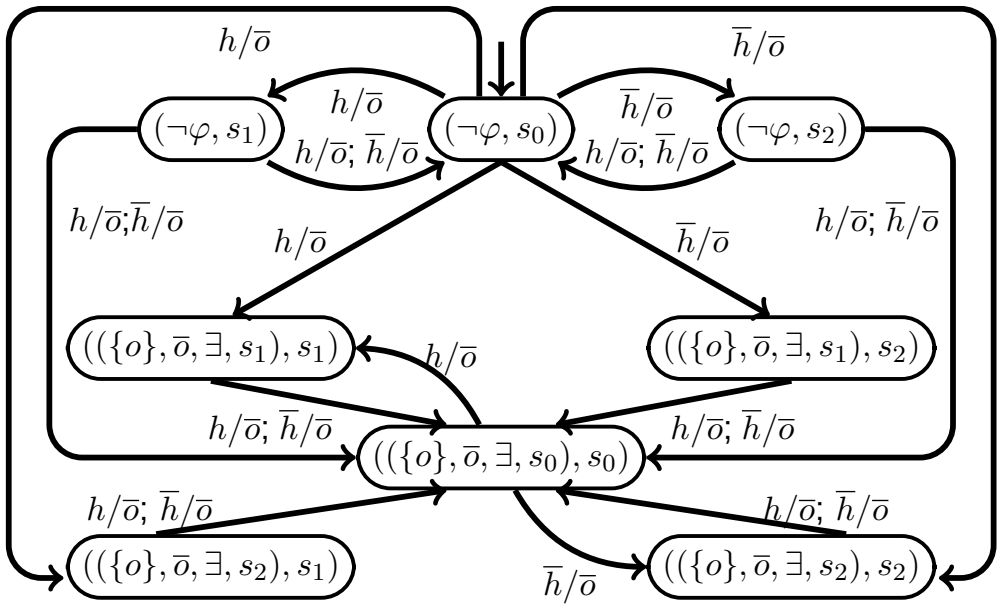
$$\varphi = \Box \mathcal{H}_{\{h\},\emptyset,\{o\}} o$$

$$\neg\varphi = \Diamond \neg \left(\mathcal{H}_{\{h\},\emptyset,\{o\}} o \right)$$

$\mathcal{M}$:



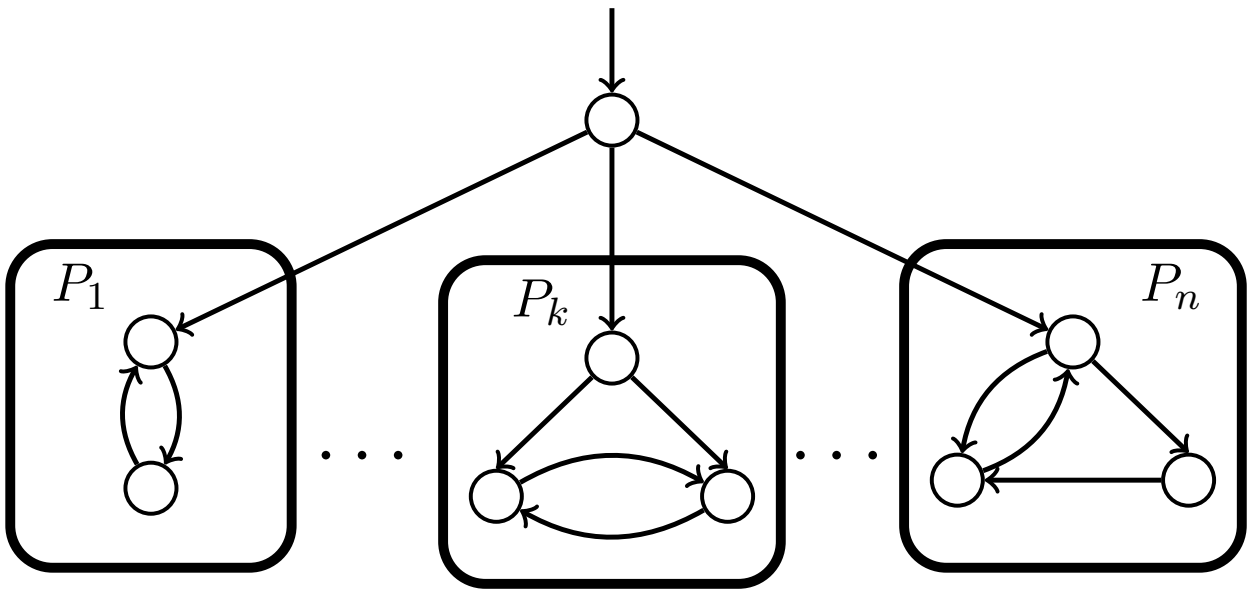
$\mathcal{A}_{\neg\varphi,\mathcal{M}} \times \mathcal{M}$:



Model Checking SecLTL: Complexity

System complexity: PSPACE-complete by reduction from model checking problem for LTL for concurrent systems

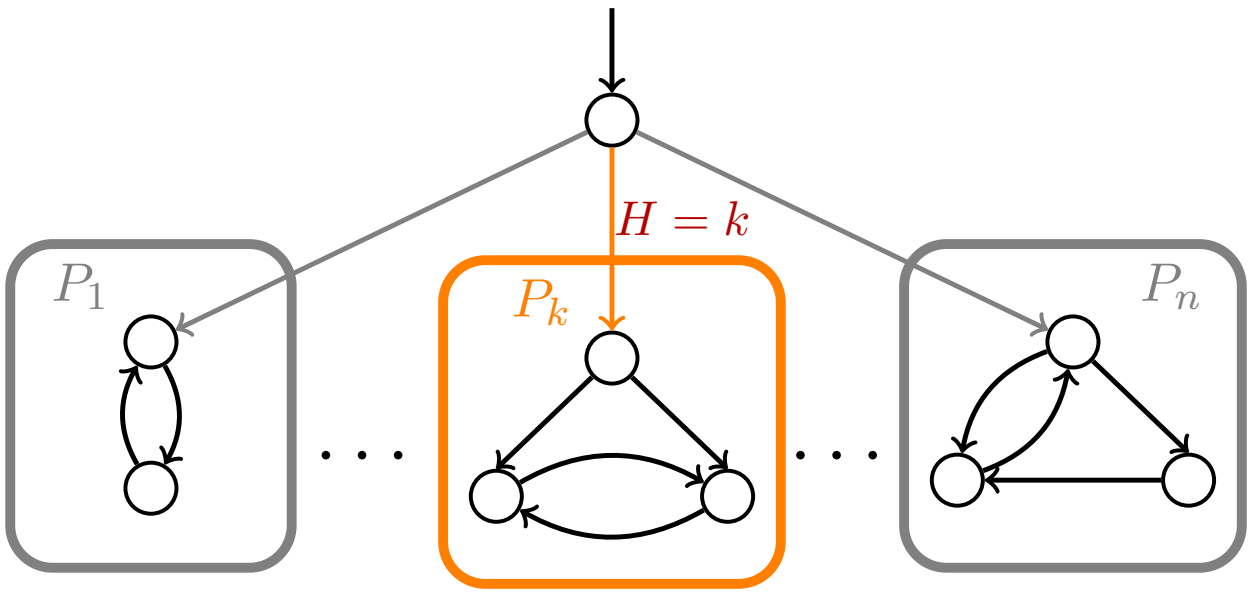
SecLTL can express synchronization of components:



Model Checking SecLTL: Complexity

System complexity: PSPACE-complete by reduction from model checking problem for LTL for concurrent systems

SecLTL can express synchronization of components:



Efficient Fragment of SecLTL

Definition

- $\mathcal{H}$ occurs only under an even number of negations
- φ does not contain nested $\mathcal{H}$ operators
- in NNF(φ), for $\mathcal{U}$ and $\mathcal{R}$ (release – the dual of $\mathcal{U}$):
  - ($\mathcal{U}$) for every subformula $\varphi_1 \,\mathcal{U}\, \varphi_2$, φ_2 is a LTL formula
  - ($\mathcal{R}$) for every subformula $\varphi_1 \,\mathcal{R}\, \varphi_2$, φ_1 is a LTL formula

Complexity

System complexity NLOGSPACE-complete as for LTL.

- Self-composition

Efficient SecLTL: Expressiveness

Can express many properties of interest:

$\square \mathcal{H}_{H,L,O} \bot$	noninterference
$\square \mathcal{H}_{H,L,O}$ release	declassification ($\approx$ "when")
$(\mathcal{H}_{H_1,L,O} \bot) \vee (\mathcal{H}_{H_2,L,O} \bot)$	disjunctive secrets
$\square(\text{session\_active} \rightarrow \mathcal{H}_{H,L,O} \bot)$	conditional secrets
$\square((\neg \Diamond \text{allowance}) \rightarrow \mathcal{H}_{H,L,O} \bot)$	peek into the future

Integration with other temporal logics

What about . . . ?

- SecCTL
- SecCTL*
- SecATL*

Integration with other temporal logics

What about . . . ?

- SecCTL
- SecCTL*
- SecATL*

	LTL	SecLTL	Eff. SecLTL		
φ	PSPACE	PSPACE	PSPACE		
$\mathcal{M}$	NLOGSPACE	PSPACE	NLOGSPACE		

Integration with other temporal logics

What about . . . ?

- SecCTL
- SecCTL*
- SecATL*

	LTL	SecLTL	Eff. SecLTL		
φ	PSPACE	PSPACE	PSPACE		
$\mathcal{M}$	NLOGSPACE	PSPACE	NLOGSPACE		

Integration with other temporal logics

What about . . . ?

- SecCTL
- SecCTL*
- SecATL*

	LTL	SecLTL	Eff. SecLTL	CTL	SecCTL
φ	PSPACE	PSPACE	PSPACE	$O(\|\varphi\|)$	$O(\|\varphi\|)$
$\mathcal{M}$	NLOGSPACE	PSPACE	NLOGSPACE	$O(\|\mathcal{M}\|)$	PSPACE

Upcoming work

- Extension to multiple agents: SecATL*
- Abstract interpretation framework for SecLTL
- Efficient symbolic model checking
- Relations to declassification
- Semantic extensions: i.e. quantitative measures, time, . . .