MPRI 2.30: Proofs of Security Protocols

4. A Higher-Order Logic for Mechanization

Adrien Koutsos, Inria Paris

2024/2025

Limitations

Limitations of the framework:

- No **built-in** support for an **arbitrary number of sessions**.
  We use an ambient-level induction.
- No **systematic** and **user-friendly** encoding of protocols.
  We manually defined out@τ, in@τ, etc at ambient level.
- Similarly, **temporal aspects** are handled at the ambient level.

All the above are **obstacles** to mechanizing the logic.

Solution

A **higher-order indistinguishability logic**:

- Supports **induction** at the logical level.
- User-defined **mutually-recursive probabilistic** procedures: **execution model** (i.e. out@τ, in@τ, etc) can be internalized.
- **Temporal reasoning** can be internalized.
- **Bonus:** Support **generic higher-order** reasonings.

$\Rightarrow$ suitable for **mechanized interactive** proofs.

A Higher-Order Indistinguishability Logic

HO Indistinguishability Logic: Types

We assume a set $\mathbb{B}$ of **base-types** (e.g. `bool`, `message`).

Types are defined by

$$\tau := \tau_{\mathsf{b}} \mid \tau \to \tau \qquad (\tau_{\mathsf{b}} \in \mathbb{B})$$

The **interpretation** $[\![\tau]\!]_{\mathbb{M}}^{\eta}$ of a type τ w.r.t. a **model** $\mathbb{M}$ and $\eta \in \mathbb{N}$:

$$[\![\tau_{\mathsf{b}}]\!]_{\mathbb{M}}^{\eta} \stackrel{\text{def}}{=} \mathbb{M}_{\tau_{\mathsf{b}}}(\eta) \qquad [\![\tau_1 \to \tau_2]\!]_{\mathbb{M}}^{\eta} \stackrel{\text{def}}{=} [\![\tau_1]\!]_{\mathbb{M}}^{\eta} \to [\![\tau_2]\!]_{\mathbb{M}}^{\eta}$$

Details

- $\mathbb{M}$ must interpret all base-types as **non-empty sets**.
- There must exists an injection from $\mathbb{M}_{\tau_{\mathsf{b}}}(\eta)$ to **bit-strings**.
  (used later to send base values to the adversary)
- **Built-in** types interpretations are fixed.
  Example: $[\![\texttt{bool}]\!]_{\mathbb{M}}^{\eta} = \{0, 1\}$ for every η

HO Indistinguishability Logic: Symbols

We still have a set of symbols $\mathcal{S} = \mathcal{N} \uplus \mathcal{X} \uplus \mathcal{F} \uplus \mathcal{G}$.

We require that:

- the set of **names** $\mathcal{N}$ is such that any name $\mathsf{n} \in \mathcal{N}$ has a type of the form $\tau_0 \to \tau_1$ with τ_0 **finite**.

HO Indistinguishability Logic: Terms

Terms are defined by:

$$\mathrm{t} := \; s \mid (\mathrm{t}\ \mathrm{t}) \mid \lambda(x : \tau).\, \mathrm{t} \mid \forall(x : \tau).\, \mathrm{t} \qquad\qquad (s \in \mathcal{S},\, x \in \mathcal{X})$$

(as usual, terms are taken modulo α-renaming)

Terms are taken in an **environment** $\mathcal{E}$:

$$\mathcal{E} := \emptyset \mid \underbrace{(s : \tau);\ \mathcal{E}}_{\text{(declaration)}} \mid \underbrace{(s : \tau = \mathrm{t});\ \mathcal{E}}_{\text{(definition)}}$$

(we require that environments do not bind the same variable twice)

We require that **terms** and **environments** are **well-typed**. We write $\mathcal{E}(s)$ the type of s in $\mathcal{E}$.

A Higher-Order Indistinguishability Logic: Typing

Term typing judgements

$$\textsc{Ty.Decl}\quad \frac{}{\mathcal{E} \vdash s : \mathcal{E}(s)}$$

$$\textsc{Ty.Fun-App}\quad \frac{\mathcal{E} \vdash \mathsf{t}_1 : \tau_0 \to \tau_1 \qquad \mathcal{E} \vdash \mathsf{t}_2 : \tau_0}{\mathcal{E} \vdash \mathsf{t}_1\ \mathsf{t}_2 : \tau_1}$$

$$\textsc{Ty.Lambda}\quad \frac{\mathcal{E}, \mathsf{x} : \tau_0 \vdash \mathsf{t} : \tau_1}{\mathcal{E} \vdash \lambda(\mathsf{x} : \tau_0).\,\mathsf{t} : \tau_0 \to \tau_1}$$

$$\textsc{Ty.ForAll}\quad \frac{\mathcal{E}, \mathsf{x} : \tau \vdash \mathsf{t} : \texttt{bool}}{\mathcal{E} \vdash \forall(\mathsf{x} : \tau).\,\mathsf{t} : \texttt{bool}}$$

Environment typing

$$\textsc{Ty-Env.}\epsilon\quad \frac{}{\vdash \epsilon}$$

$$\textsc{Ty-Env.Decl}\quad \frac{\vdash \mathcal{E}}{\vdash \mathcal{E}, (s : \tau)}$$

$$\textsc{Ty-Env.Def}\quad \frac{\vdash \mathcal{E} \qquad \mathcal{E} \vdash \mathsf{t} : \tau \qquad \mathsf{x} \notin (\mathcal{N} \cup \mathcal{F} \cup \mathcal{G})}{\vdash \mathcal{E}, (\mathsf{x} : \tau = \mathsf{t})}$$

Remark: *names, builtins and adversarial symbols can only be declared.*

Change w.r.t. the FO logic.

Terms are interpreted as arbitrary **random variables**, not necessarily **PPTMs**.

$$[\![t]\!]_{\mathbb{M}} : \eta\text{-indexed families of } \textbf{random variables}$$

using **probability space** $\mathbb{T}_{\mathbb{M},\eta} = \mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta} \times \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$.

($\mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta}, \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ use the uniform prob. measure.)

HO Indistinguishability Logic: Probability Space

Change w.r.t. the FO logic.

Terms are interpreted as arbitrary **random variables**, not necessarily **PPTMs**.

$$[\![t]\!]_{\mathbb{M}} : \eta\text{-indexed families of } \textbf{random variables}$$

using **probability space** $\mathbb{T}_{\mathbb{M},\eta} = \mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta} \times \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$.
($\mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta}, \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ use the uniform prob. measure.)

Examples:

- $\forall x : \texttt{message}.\ \mathrm{len}(\mathbf{att}(x)) \leq 42$
- $\forall e : \texttt{int}.\ \mathrm{dlog}(\mathrm{g}^{e}) = e$

HO Indistinguishability Logic: Probability Space

Change w.r.t. the FO logic.

Terms are interpreted as arbitrary **random variables**, not necessarily **PPTMs**.

$$[\![t]\!]_{\mathbb{M}} : \eta\text{-indexed families of } \textbf{random variables}$$

using **probability space** $\mathbb{T}_{\mathbb{M},\eta} = \mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta} \times \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$.
($\mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta}, \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ use the uniform prob. measure.)

Examples:

- $\forall x : \texttt{message}.\, \mathrm{len}(\mathbf{att}(x)) \leq 42$
- $\forall e : \texttt{int}.\, \mathrm{dlog}(\mathrm{g}^{e}) = e$
- $\forall \phi : \tau \to \texttt{bool}.\, \big(\forall x.\, (\forall y.\, y < x \to \phi\ y\,) \to \phi\ x\,\big) \to (\forall x.\, \phi\ x\,)$

HO Indistinguishability Logic: Term Semantics

Let $\mathbb{RV}_{\mathbb{M}}(\tau)$ be the set $\prod_{n \in \mathbb{N}}(\mathbb{T}_{\mathbb{M},\eta} \rightarrow [\![\tau]\!]^{\eta}_{\mathbb{M}})$.

A model $\mathbb{M}$ w.r.t. $\mathcal{E}$, written $\mathbb{M} : \mathcal{E}$, interprets any **declaration** $(s : \tau) \in \mathcal{E}$ as a random variable:

$$\mathbb{M}(s) \in \mathbb{RV}_{\mathbb{M}}(\tau)$$

HO Indistinguishability Logic: Term Semantics

Let $\mathbb{RV}_{\mathbb{M}}(\tau)$ be the set $\prod_{n \in \mathbb{N}}(\mathbb{T}_{\mathbb{M},\eta} \to [\![\tau]\!]^{\eta}_{\mathbb{M}})$.

A model $\mathbb{M}$ w.r.t. $\mathcal{E}$, written $\mathbb{M} : \mathcal{E}$, interprets any **declaration** $(s : \tau) \in \mathcal{E}$ as a random variable:

$$\mathbb{M}(s) \in \mathbb{RV}_{\mathbb{M}}(\tau)$$

with some **restrictions**:

- names are PTIME-computable (in η) **random samplings** using only randomness in $\mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ (details later);
- **builtins** $\mathcal{F}$ must be PTIME-computable *deterministic* functions;
- **adversarial functions** $\mathcal{G}$ must be PTIME-computable functions using only randomness in $\mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta}$.

Remark: $\mathbb{M}(s)(\eta)(\rho) \in [\![\tau]\!]^{\eta}_{\mathbb{M}}$.

HO Indistinguishability Logic: Term Semantics

The **semantics** $[\![\mathsf{t}]\!]_{\mathbb{M}}^{\eta,\rho}$ of t w.r.t. $\mathbb{M}$ and $\eta \in \mathbb{N}$ is a value in $[\![\tau]\!]_{\mathbb{M}}^{\eta}$:

$$[\![s]\!]_{\mathbb{M}}^{\eta,\rho} \stackrel{\text{def}}{=} \mathbb{M}(s)(\eta)(\rho) \qquad \text{(decl., } (s : \tau) \in \mathcal{E})$$

$$[\![\mathsf{x}]\!]_{\mathbb{M}}^{\eta,\rho} \stackrel{\text{def}}{=} [\![\mathsf{t}]\!]_{\mathbb{M}}^{\eta,\rho} \qquad \text{(def., } (\mathsf{x} : \tau = \mathsf{t}) \in \mathcal{E})$$

$$[\![\mathsf{t}\ \mathsf{t}']\!]_{\mathbb{M}}^{\eta,\rho} \stackrel{\text{def}}{=} [\![\mathsf{t}]\!]_{\mathbb{M}}^{\eta,\rho}([\![\mathsf{t}']\!]_{\mathbb{M}}^{\eta,\rho})$$

HO Indistinguishability Logic: Term Semantics

The **semantics** $[\![\mathsf{t}]\!]^{\eta,\rho}_{\mathbb{M}}$ of t w.r.t. $\mathbb{M}$ and $\eta \in \mathbb{N}$ is a value in $[\![\tau]\!]^{\eta}_{\mathbb{M}}$:

$$[\![s]\!]^{\eta,\rho}_{\mathbb{M}} \overset{\text{def}}{=} \mathbb{M}(s)(\eta)(\rho) \qquad \text{(decl., } (s : \tau) \in \mathcal{E})$$

$$[\![\mathsf{x}]\!]^{\eta,\rho}_{\mathbb{M}} \overset{\text{def}}{=} [\![\mathsf{t}]\!]^{\eta,\rho}_{\mathbb{M}} \qquad \text{(def., } (\mathsf{x} : \tau = \mathsf{t}) \in \mathcal{E})$$

$$[\![\mathsf{t}\ \mathsf{t}']\!]^{\eta,\rho}_{\mathbb{M}} \overset{\text{def}}{=} [\![\mathsf{t}]\!]^{\eta,\rho}_{\mathbb{M}}([\![\mathsf{t}']\!]^{\eta,\rho}_{\mathbb{M}})$$

$$[\![\lambda(\mathsf{x} : \tau).\, \mathsf{t}]\!]^{\eta,\rho}_{\mathbb{M}} \overset{\text{def}}{=} \left(a \in [\![\tau]\!]^{\eta}_{\mathbb{M}} \mapsto [\![\mathsf{t}]\!]^{\eta,\rho}_{\mathbb{M}[\mathsf{x}\mapsto \mathbb{1}^{\eta}_{a}]}\right)$$

$$[\![\forall(\mathsf{x} : \tau).\, \mathsf{t}]\!]^{\eta,\rho}_{\mathbb{M}} \overset{\text{def}}{=} 1 \quad \text{iff. } [\![\mathsf{t}]\!]^{\eta,\rho}_{\mathbb{M}[\mathsf{x}\mapsto \mathbb{1}^{\eta}_{a}]} = 1 \text{ for any } a \in [\![\tau]\!]^{\eta}_{\mathbb{M}}$$

where $\mathbb{1}^{\eta}_{a}$ is the indexed family of functions such that:

- $\mathbb{1}^{\eta}_{a}(\eta)(\rho) = a$ for all $\rho \in \mathbb{T}_{\mathbb{M},\eta}$;
- $\mathbb{1}^{\eta}_{a}(\eta')(\rho')$ is some arbitrary value in $[\![\tau]\!]^{\eta'}_{\mathbb{M}}$ for any $\eta' \neq \eta$.

HO Indistinguishability Logic: Name Semantics

A name $\mathsf{n} \in \mathcal{N}$ interpretation must be such that

$$[\![\mathsf{n}\ \mathsf{t}]\!]_{\mathbb{M}}^{\eta,(\rho_{\mathsf{a}},\rho_{\mathsf{h}})} = (\!|\mathsf{n}|\!)_{\mathbb{M}}(\eta, [\![\mathsf{t}]\!]_{\mathbb{M}}^{\eta,\rho})(\rho_{\mathsf{h}})$$

where $(\!|\mathsf{n}|\!)_{\mathbb{M}}$ is a PTIME computation w.r.t. η.

HO Indistinguishability Logic: Name Semantics

A name $\mathsf{n} \in \mathcal{N}$ interpretation must be such that

$$[\![\mathsf{n}\ \mathsf{t}]\!]_{\mathbb{M}}^{\eta,(\rho_{\mathsf{a}},\rho_{\mathsf{h}})} = (\!|\mathsf{n}|\!)_{\mathbb{M}}(\eta, [\![\mathsf{t}]\!]_{\mathbb{M}}^{\eta,\rho})(\rho_{\mathsf{h}})$$

where $(\!|\mathsf{n}|\!)_{\mathbb{M}}$ is a PTIME computation w.r.t. η.

Moreover, $\rho_{\mathsf{h}} \mapsto (\!|\mathsf{n}_0|\!)_{\mathbb{M}}(\eta, a)(\rho_{\mathsf{h}})$ and $\rho_{\mathsf{h}} \mapsto (\!|\mathsf{n}_1|\!)_{\mathbb{M}}(\eta, a')(\rho_{\mathsf{h}})$

- are **independent random samplings** when $(\mathsf{n}_0, a) \neq (\mathsf{n}_1, a')$. They must extract $\neq$ random bits from ρ_{h}.
- have the same **distribution** when n_0 and n_1 have the same output type (i.e. $\mathcal{E}(\mathsf{n}_0) = \_ \to \tau$ and $\mathcal{E}(\mathsf{n}_1) = \_ \to \tau$).

HO Indistinguishability Logic: Name Semantics

Remarks

- $\mathcal{E}$ contains a **finite** number of names.
- names have type $\tau_0 \to \tau_1$ where τ_0 is **finite**.
- $(\!|\mathsf{n}|\!)_{\mathbb{M}}$ uses a **finite** number of bits from ρ_{h} (since PTIME in η).

$\Rightarrow$ compatible with requirement that $\mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ is a set of **finite** tapes.

HO Indistinguishability Logic: Local Satisfiability and Validity

Definitions

- **Satisfiability:** when $\mathcal{E} \vdash \phi : \texttt{bool}$, we write $\mathbb{M} : \mathcal{E} \models \phi$ if

$$\mathsf{Pr}_\rho(\llbracket \phi \rrbracket_{\mathbb{M}}^{\eta,\rho} = 1) \in \mathsf{o.w.}(\eta).$$

- **Validity:** $\mathcal{E} \models \phi$ if $\mathbb{M} : \mathcal{E} \models \phi$ for every $\mathbb{M} : \mathcal{E}$.

HO Indistinguishability Logic: Local Satisfiability and Validity

Definitions

- **Satisfiability:** when $\mathcal{E} \vdash \phi : \texttt{bool}$, we write $\mathbb{M} : \mathcal{E} \models \phi$ if

$$\mathsf{Pr}_\rho(\llbracket \phi \rrbracket_{\mathbb{M}}^{\eta,\rho} = 1) \in \text{o.w.}(\eta).$$

- **Validity:** $\mathcal{E} \models \phi$ if $\mathbb{M} : \mathcal{E} \models \phi$ for every $\mathbb{M} : \mathcal{E}$.

Local Sequents

- **Syntax:** $\mathcal{E}; \Gamma \vdash \phi$
- **Semantics:** $\mathcal{E} \models (\wedge \Gamma) \rightarrow \phi$

HO Indistinguishability Logic: Term Semantics

Summary:

A model $\mathbb{M}$ for $\mathcal{E}$ comprises:

- The **interpretation domains** of base types $\mathbb{B}$.
  $\Rightarrow$ yields a type semantics $[\![\cdot]\!]^{\eta}_{\mathbb{M}}$.
- The **probability space** $\mathbb{T}_{\mathbb{M},\eta} = \mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta} \times \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$.
- The **interpretations** of **declared** variables of $\mathcal{E}$.
  Defined variables are interpreted by their **definitions**.
  $\Rightarrow$ yields a term semantics $[\![\cdot]\!]^{\eta,\rho}_{\mathbb{M}}$.

Remarks

We restrict possible models in several ways (more to come):

- **finiteness** required of some types (e.g. to index names).
- **constraints** on name and **built-ins** interpretations.
- ...

HO Indistinguishability Logic: Term Semantics

Key ingredients:

- terms are interpreted as arbitrary **random variables**, not necessarily PPTMs.
  - $\Rightarrow$ support **probabilistic user-defined** functions (e.g. in$@\tau$).
  - $\Rightarrow$ support **uncomputable** functions.
  - $\Rightarrow$ support **quantifiers** $\forall, \exists$ over **arbitrary types**.
- the **probability space** is **finite**.
  - $\Rightarrow$ ensures that $(\rho \mapsto [\![t]\!]_{\mathbb{M}}^{\eta,\rho})$ is a **random variable**.

  *indeed, any function $X : \mathbb{S}_1 \mapsto \mathbb{S}_2$ (where $\mathbb{S}_1$ is a **finite** probability space and $\mathbb{S}_2$ is a measurable space) is a measurable function.*

Encoding Protocols

HO Indistinguishability Logic: Protocols

Encode protocol executions as (mutually) **recursive computations**.

Example: encoding of Hash-Lock

$$
\begin{aligned}
\mathsf{in}@t =\ & \texttt{match}\ t\ \texttt{with}\ \mathsf{init} \rightarrow d \\
& \mid \_ \rightarrow \mathbf{att}(\mathsf{frame}@\mathsf{pred}\ t) \\
\mathsf{frame}@t =\ & \texttt{match}\ t\ \texttt{with}\ \mathsf{init} \rightarrow d \\
& \mid \_ \rightarrow \langle \mathsf{frame}@\mathsf{pred}\ t, \mathsf{out}@t \rangle \\
\mathsf{out}@t =\ & \texttt{match}\ t\ \texttt{with}\ \mathsf{init} \rightarrow d \\
& \mid \mathsf{T}(\mathsf{A},\mathsf{i}) \rightarrow \langle \mathsf{n_T}(\mathsf{A},\mathsf{i}), \mathsf{h}(\langle \mathsf{in}@t, \mathsf{n_T}(\mathsf{A},\mathsf{i})\rangle, \mathsf{k}\ \mathsf{A})\rangle \\
& \mid \mathsf{R_1}(\mathsf{j}) \rightarrow \mathsf{n_R}\ \mathsf{j} \\
& \mid \mathsf{R_2}(\mathsf{j}) \rightarrow \ldots
\end{aligned}
$$

$\Rightarrow$ need **support** for **recursive definitions** $f : \tau = t$ where $f \in \mathsf{st}(t)$.

HO Indistinguishability Logic: Recursive Definitions

We first extend the HO logic to allow **recursive definitions**.

Any type τ and order $< \in \mathcal{F}$ with type $\tau \to \tau \to \texttt{bool}$ can be tagged as $\texttt{wf}(\tau, <)$.

$\Rightarrow$ only consider models s.t. $(\llbracket \tau \rrbracket^{\eta}_{\mathbb{M}}, \llbracket < \rrbracket^{\eta}_{\mathbb{M}})$ is **well-founded**.

We allow well-founded **recursion** over such types.

Details

- we assume a *fixed* set of **type tags** $\mathbb{S}_{\mathsf{wf}}$.
- we assume a *fixed* set $\mathbb{S}_{\mathsf{ax}}$ of terms of type $\texttt{bool}$ (**axioms**).
- we require that any model $\mathbb{M}$ is such that $\mathbb{M} \models \mathbb{S}_{\mathsf{ax}}$ and

$$(\llbracket \tau \rrbracket^{\eta}_{\mathbb{M}}, \llbracket < \rrbracket^{\eta}_{\mathbb{M}}) \text{ is } \textbf{well-founded} \qquad (\text{for any } \texttt{wf}(\tau, <) \in \mathbb{S}_{\mathsf{wf}})$$

HO Indistinguishability Logic: Recursive Definitions

We add a **typing rule** for **recursive** definitions:

$$\textsc{Ty-Env.Rec-Def}\quad \frac{\vdash \mathcal{E} \qquad \mathcal{E}, f : \tau \vdash \lambda \mathsf{x}.\, \mathsf{t} : \tau \qquad \mathsf{wf}^{f,\mathsf{x}}_{\tau,<}(\mathsf{t}) \qquad f \in \mathcal{X}}{\vdash \mathcal{E}, \left(f : \tau = \lambda \mathsf{x}.\, \mathsf{t}\right)}$$

where $\mathsf{wf}^{f,\mathsf{x}}_{\tau,<}(\mathsf{t})$ is any **syntactic condition** which checks that

- f is used in η-**long form** in t.
- recursive calls to f are **well-founded**, i.e. on arguments t_0 smaller than x:

$$\mathcal{E} \models [\forall \vec{\alpha}.\, \phi \rightarrow \mathsf{t}_0 < \mathsf{x}] \qquad \text{(for any } (\vec{\alpha}, \phi, f\ \mathsf{t}_0) \in \mathcal{ST}(\mathsf{t}))$$

where $\mathcal{ST}(\mathsf{t})$ are the **conditioned subterms** of t (see next slide).

Example

$$\ell = \lambda(i : \mathtt{int}).\, \text{if } i = 0 \text{ then empty else } \langle \mathsf{n}\ i, \ell\ (\mathsf{pred}\ i)\rangle$$

with $\mathtt{wf}(\mathtt{int}, <)$ and the axiom $\forall (i : \mathtt{int}).\, i \neq 0 \rightarrow \mathsf{pred}\ i < i$.

HO Indistinguishability Logic: Conditioned Subterms

We let $\mathcal{ST}(\mathsf{t})$ be the subterms of t, decorated the (typed) **bound variables** and the **conditions** holding at each position.

$$\mathcal{ST}(\mathsf{t}) \stackrel{\text{def}}{=} \{(\epsilon, \mathsf{true}, \mathsf{t})\} \cup \begin{cases} \emptyset & \text{if } \mathsf{t} = \mathsf{x} \in \mathcal{X} \\ (\mathsf{x} : \tau).\mathcal{ST}(\mathsf{t}_0) & \text{if } \mathsf{t} = \mathcal{Q}(\mathsf{x} : \tau).\mathsf{t}_0,\ \mathcal{Q} \in \{\lambda, \forall\} \\ \mathcal{ST}(\phi) \cup [\phi]\mathcal{ST}(t_1) \cup [\neg\phi]\mathcal{ST}(t_0) & \text{if } \mathsf{t} = \text{if } \phi \text{ then } \mathsf{t}_1 \text{ else } \mathsf{t}_0 \\ \mathcal{ST}(\mathsf{t}_0) \cup \mathcal{ST}(\mathsf{t}_1) & \text{if } \mathsf{t} = (\mathsf{t}_0\ \mathsf{t}_1) \end{cases}$$

where x is taken fresh in the λ and $\forall$ cases, and where

$$[\phi]S \stackrel{\text{def}}{=} \{(\vec{\alpha}, \psi \wedge \phi, \mathsf{t}) \mid (\vec{\alpha}, \psi, \mathsf{t}) \in S\}$$
$$(\mathsf{x} : \tau).S \stackrel{\text{def}}{=} \{((\vec{\alpha}, \mathsf{x} : \tau), \psi, \mathsf{t}) \mid (\vec{\alpha}, \psi, \mathsf{t}) \in S\}$$

HO Indistinguishability Logic: Conditioned Subterms

Example

$$
\begin{aligned}
\mathcal{ST}(\langle \mathsf{x}\,,\ \lambda(\mathsf{x}_0,\mathsf{x}_1 : \tau).\,\mathsf{if}\ \mathsf{x}_0 < \mathsf{x}_1\ \mathsf{then}\ \mathsf{x}_0\ \mathsf{else}\ \mathsf{x}_1\rangle) \ =\ & \\
& \{(\epsilon, \mathsf{true}, \langle \mathsf{x}\,,\ \lambda(\mathsf{x}_0,\mathsf{x}_1 : \tau).\,\mathsf{if}\ \mathsf{x}_0 < \mathsf{x}_1\ \mathsf{then}\ \mathsf{x}_0\ \mathsf{else}\ \mathsf{x}_1\rangle)\} \\
& \cup \{(\epsilon, \mathsf{true}, \mathsf{x}), (\epsilon, \mathsf{true}, \lambda(\mathsf{x}_0,\mathsf{x}_1 : \tau).\,\mathsf{if}\ \mathsf{x}_0 < \mathsf{x}_1\ \mathsf{then}\ \mathsf{x}_0\ \mathsf{else}\ \mathsf{x}_1)\} \\
& \cup \{(\mathsf{x}_0, \mathsf{true}, \lambda(\mathsf{x}_1 : \tau).\,\mathsf{if}\ \mathsf{x}_0 < \mathsf{x}_1\ \mathsf{then}\ \mathsf{x}_0\ \mathsf{else}\ \mathsf{x}_1)\} \\
& \cup \{((\mathsf{x}_0,\mathsf{x}_1), \mathsf{true}, \mathsf{if}\ \mathsf{x}_0 < \mathsf{x}_1\ \mathsf{then}\ \mathsf{x}_0\ \mathsf{else}\ \mathsf{x}_1)\} \\
& \cup \{((\mathsf{x}_0,\mathsf{x}_1), \mathsf{true}, \mathsf{x}_0 < \mathsf{x}_1)\} \\
& \cup \{((\mathsf{x}_0,\mathsf{x}_1), \mathsf{true} \wedge \mathsf{x}_0 < \mathsf{x}_1, \mathsf{x}_0)\} \\
& \cup \{((\mathsf{x}_0,\mathsf{x}_1), \mathsf{true} \wedge \neg(\mathsf{x}_0 < \mathsf{x}_1), \mathsf{x}_1)\}
\end{aligned}
$$

Formulas

HO Indistinguishability Logic: Formulas

Formulas do not change, except that we use **higher-order terms**.

$$
\begin{aligned}
\Phi := {} & \tilde{\top} \mid \tilde{\bot} \\
& \mid \Phi \mathbin{\tilde{\wedge}} \Phi \mid \Phi \mathbin{\tilde{\vee}} \Phi \mid \Phi \mathbin{\tilde{\rightarrow}} \Phi \mid \tilde{\neg}\, \Phi \\
& \mid \tilde{\forall}(\mathsf{x} : \tau).\Phi \mid \tilde{\exists}(\mathsf{x} : \tau).\Phi && (\mathsf{x} \in \mathcal{X}) \\
& \mid \mathsf{t}_1, \ldots, \mathsf{t}_n \sim_n \mathsf{t}_{n+1}, \ldots, \mathsf{t}_{2n} && (\mathsf{t}_1, \ldots, \mathsf{t}_{2n} \text{ higher-order terms})
\end{aligned}
$$

HO Indistinguishability Logic: Formula Semantics

Standard FO semantics with η-**indexed sequences of random variables** interpretation domains.

The satisfaction $\mathbb{M} : \mathcal{E} \models \Phi$ of Φ in $\mathbb{M}$ is as expected for **boolean connective** and FO **quantifiers**. E.g.:

$$\mathbb{M} : \mathcal{E} \models \tilde{\top} \qquad \mathbb{M} : \mathcal{E} \models \Phi \mathbin{\tilde{\wedge}} \Psi \quad \text{if } \mathbb{M} : \mathcal{E} \models \Phi \text{ and } \mathbb{M} : \mathcal{E} \models \Psi$$

$$\mathbb{M} : \mathcal{E} \models \tilde{\neg}\, \Phi \quad \text{if not } \mathbb{M} : \mathcal{E} \models \Phi$$

$$\mathbb{M} : \mathcal{E} \models \tilde{\forall} \mathrm{x} : \tau. \Phi \qquad \text{if } \forall A \in \mathbb{RV}_{\mathbb{M}}(\tau), \mathbb{M}[\mathrm{x} \mapsto A] : (\mathcal{E}, x : \tau) \models \Phi$$

HO Indistinguishability Logic: Formula Semantics

$\sim$ is still interpreted as **computational indistinguishability**.

$$\mathbb{M} \models \vec{t}_1 \sim \vec{t}_2 \text{ iff. } \forall \text{ PPTM } \mathcal{A}, \mathsf{Adv}^{\eta}_{\mathbb{M}:\mathcal{E}}(\mathcal{A} : \vec{t}_1 \sim \vec{t}_2) \text{ is negligible.}$$

Execution Model

- Values in $[\![\tau_{\mathsf{b}}]\!]^{\eta}_{\mathbb{M}}$ are **encoded as bitstrings** and sent to $\mathcal{A}$.
- **Higher-order terms** given to $\mathcal{A}$ are **oracles**, which $\mathcal{A}$ can **query** on any inputs it can compute, any number of times.
- We require that terms in $\vec{t}_1$ and $\vec{t}_2$ have types $\tau^0_{\mathsf{b}} \to \ldots \to \tau^n_{\mathsf{b}}$ (i.e. no higher-order arguments).

HO Indistinguishability Logic: Proof System

Our **rules** still apply, though with **minor adaptations**.

Example: **function application** requires an additional check:

$$\text{FA}\quad \frac{\vec{u}_1, t_1 \sim \vec{u}_2, t_2 \qquad [\mathsf{len}(t_1) \leq P(\eta) \wedge \mathsf{len}(t_2) \leq P(\eta)]}{\vec{u}_1, f\ t_1 \sim \vec{u}_2, f\ t_2}$$

where $f \in \mathcal{F} \cup \mathcal{G}$, and P is a polynomial.

HO Indistinguishability Logic: Proof System

New rule for **induction**:

$$\frac{\vec{u}(0) \sim \vec{v}(0) \qquad \tilde{\forall}(N : \texttt{int}).\ \vec{u}(N) \sim \vec{v}(N) \mathrel{\tilde{\rightarrow}} \vec{u}(N+1) \sim \vec{v}(N+1)}{\tilde{\forall}(N : \texttt{int}).\ \vec{u}(N) \sim \vec{v}(N)}$$

HO Indistinguishability Logic: Proof System

New rule for **induction**:

$$\frac{\vec{u}(0) \sim \vec{v}(0) \qquad \tilde{\forall}(N : \mathtt{int}).\ \vec{u}(N) \sim \vec{v}(N) \mathrel{\tilde{\to}} \vec{u}(N+1) \sim \vec{v}(N+1)}{\tilde{\forall}(N : \mathtt{int}).\ \vec{u}(N) \sim \vec{v}(N)}$$

Only for a **constant** number of steps N.

Same reason as for **hybrid arguments**:

$$\vec{u}(0) \sim \ldots \sim \vec{u}(N) \implies \vec{u}(0) \sim_{f_1(\eta)} \ldots \sim_{f_N(\eta)} \vec{u}(N) \quad ((f_i)_i \text{ negligible})$$
$$\implies \vec{u}(0) \sim_{\sum_{i \leq N} f_i(\eta)} \vec{u}(N)$$

$\sum_{i \leq N} f_i(\eta)$ may not be negligible if N polynomial in η.

HO Indistinguishability Logic: Proof System

New rule for **induction**:

$$\frac{\vec{u}(0) \sim \vec{v}(0) \qquad \tilde{\forall}(N : \texttt{int}).\ \big(\mathsf{const}(N)\ \tilde{\wedge}\ \vec{u}(N) \sim \vec{v}(N)\big) \mathrel{\tilde{\rightarrow}} \vec{u}(N+1) \sim \vec{v}(N+1)}{\tilde{\forall}(N : \texttt{int}).\ \mathsf{const}(N) \mathrel{\tilde{\rightarrow}} \vec{u}(N) \sim \vec{v}(N)}$$

Only for a **constant** number of steps N.

Same reason as for **hybrid arguments**:

$$\begin{aligned} \vec{u}(0) \sim \ldots \sim \vec{u}(N) &\implies \vec{u}(0) \sim_{f_1(\eta)} \ldots \sim_{f_N(\eta)} \vec{u}(N) \quad ((f_i)_i \text{ negligible}) \\ &\implies \vec{u}(0) \sim_{\sum_{i \leq N} f_i(\eta)} \vec{u}(N) \end{aligned}$$

$\sum_{i \leq N} f_i(\eta)$ may not be negligible if N polynomial in η.

HO Indistinguishability Logic: Formula and Term Quantifiers

We have two kind of **quantifiers**: **term** $\forall$ and **formula** $\tilde{\forall}$.

But we have only **one kind of variable**! Why?

Proposition

For every model $\mathbb{M}$ of $\mathcal{E}$, we have:

$$\mathbb{M} : \mathcal{E} \models \tilde{\forall}(\mathsf{x} : \tau).\, [\phi] \quad \text{iff.} \quad \mathbb{M} : \mathcal{E} \models [\, \forall\, (\mathsf{x} : \tau).\, \phi]$$

HO Indistinguishability Logic: Formula and Term Quantifiers

Proof of the Proposition

$\Rightarrow$ **case.** Assume the following:

$$\mathbb{M} : \mathcal{E} \models [\,\forall\,(x : \tau).\,\phi] \qquad (\star)$$

Let $A \in \left(\llbracket\tau\rrbracket_{\mathbb{M}}^{\eta}\right)_{\eta\in\mathbb{N}}$ be a sequence of random variables. We must show

$$\Pr\left(\llbracket\phi\rrbracket_{\mathbb{M}[x\mapsto A]}^{\eta,\rho}\right) \in \text{o.w.}(\eta)$$

where the probability is over $\rho \in \mathbb{T}_{\mathbb{M},\eta}$.

$$\begin{aligned}
&\Pr\left(\llbracket\phi\rrbracket_{\mathbb{M}[x\mapsto A]}^{\eta,\rho}\right) \\
&\qquad = \Pr\left(\llbracket\phi\rrbracket_{\mathbb{M}[x\mapsto \mathbb{1}^{\eta}_{A(\eta)(\rho)}]}^{\eta,\rho}\right) \\
&\qquad \geq \Pr\left(\bigcap_{a\in\llbracket\tau\rrbracket_{\mathbb{M}}^{\eta}} \llbracket\phi\rrbracket_{\mathbb{M}[x\mapsto \mathbb{1}^{\eta}_{a}]}^{\eta,\rho}\right) \\
&\qquad = \Pr\left(\llbracket\forall(x : \tau).\,\phi\rrbracket_{\mathbb{M}}^{\eta,\rho}\right) \\
&\qquad \in \text{o.w.}(\eta) \qquad\qquad (\text{using } (\star))
\end{aligned}$$

HO Indistinguishability Logic: Formula and Term Quantifiers

$\Leftarrow$ **case.** Assume that

$$\mathbb{M} : \mathcal{E} \models \tilde{\forall}(x : \tau).\, [\phi] \qquad (\dagger)$$

We need to show that $\Pr\left(\llbracket \forall(x : \tau).\, \phi \rrbracket_{\mathbb{M}}^{\eta,\rho}\right) \in \text{o.w.}(\eta)$.

Let A be the family of functions choosing, for any η and ρ, a value $a \in \llbracket \tau \rrbracket_{\mathbb{M}}^{\eta}$ making ϕ false when evaluated on tape ρ

$$A(\eta)(\rho) \stackrel{\text{def}}{=} \begin{cases} \text{choose}\left\{a \in \llbracket \tau \rrbracket_{\mathbb{M}}^{\eta} \mid \llbracket \neg\phi \rrbracket_{\mathbb{M}[x \mapsto 1_a^{\eta}]}^{\eta,\rho}\right\} & \text{if non-empty} \\ a_{\text{witness}} & \text{otherwise} \end{cases}$$

where a_{witness} is an arbitrary value in $\llbracket \tau \rrbracket_{\mathbb{M}}^{\eta}$ (recall that $\llbracket \tau \rrbracket_{\mathbb{M}}^{\eta} \neq \emptyset$), and choose($\mathbb{S}$) is an arbitrary choice function for set $\mathbb{S}$.

Since all functions from $\mathbb{T}_{\mathbb{M},\eta}$ to $\{0, 1\}$ are random variables (thanks to $\mathbb{T}_{\mathbb{M},\eta}$'s finitness), we get that, by applying ($\dagger$) to A

$$\Pr\left(\llbracket \phi \rrbracket_{\mathbb{M}[x \mapsto A]}^{\eta,\rho}\right) \in \text{o.w.}(\eta) \qquad (\ddagger)$$

HO Indistinguishability Logic: Formula and Term Quantifiers

Then:

$$
\begin{aligned}
&\mathsf{Pr}\left(\llbracket\phi\rrbracket^{\eta,\rho}_{\mathbb{M}[x\mapsto A]}\right)\\
&\quad= \mathsf{Pr}\left(\llbracket\phi\rrbracket^{\eta,\rho}_{\mathbb{M}[x\mapsto \mathbb{1}^{\eta}_{A(\eta)(\rho)}]}\right)\\
&\quad= \mathsf{Pr}\left(\textstyle\bigcap_{a\in\llbracket\tau\rrbracket^{\eta}_{\mathbb{M}}}\llbracket\phi\rrbracket^{\eta,\rho}_{\mathbb{M}[x\mapsto \mathbb{1}^{\eta}_{a}]}\right)\\
&\quad= \mathsf{Pr}\left(\llbracket\forall(x:\tau).\,\phi\rrbracket^{\eta,\rho}_{\mathbb{M}}\right)\\
&\quad\in \text{o.w.}(\eta) && \text{(using } (\ddagger))
\end{aligned}
$$

Our local proof system hence supports the usual rules for **arbitrary term quantifiers**, e.g.

$$\frac{\mathcal{E}, \mathsf{x} : \tau ; \Gamma \vdash \phi}{\mathcal{E}; \Gamma \vdash \forall(\mathsf{x} : \tau).\, \phi}$$

$\Rightarrow$ Allow for **generic higher-order reasoning** in terms.

Freshness and Cryptographic Rules

HO Indistinguishability Logic: Name Collision

How to adapt the rule exploiting **probabilistic independence**?

Base Logic Rule

$$\frac{}{[t \neq \mathsf{n}]} \quad \text{when } \mathsf{n} \not\in \mathsf{st}(t)$$

where t is a **ground** **low-order** term.

HO Indistinguishability Logic: Name Collision

How to adapt the rule exploiting **probabilistic independence**?

Base Logic Rule

$$\frac{}{[t \neq \mathsf{n}]} \quad \text{when } \mathsf{n} \notin \mathsf{st}(t)$$

where t is a **ground** **low-order** term.

Rule for Name Collision (first tentative)

t, t_0 well-typed in $\mathcal{E}$ where $\mathcal{E}$ has **no variable declarations**.
(I.e. $\mathsf{t}_0, \mathsf{t}_1$ ground-terms.)

$$\frac{}{[\mathsf{t} \neq \mathsf{n}\ \mathsf{t}_0]}$$

when $\mathsf{n} \notin \mathsf{st}(\mathsf{t}, \mathsf{t}_0)$ **and all definitions in** $\mathcal{E}$.
$\Rightarrow$ not very useful!

HO Indistinguishability Logic: Name Collision

How to do better? Lets see on an example.

$\mathcal{E}$ a **ground environment** with a **single inductive definition**:

$$\ell = \lambda(i : \texttt{bint}).\,\text{if } i = 0 \text{ then empty else } \langle \mathsf{n}\ i, \ell\ (\text{pred } i)\rangle$$

where $\mathsf{n} : \texttt{bint} \to \texttt{message}$ and $[\![\texttt{bint}]\!]^{\eta}_{\mathbb{M}} = \{0, \ldots, \eta\}$ for any η.

Rule (special case)

Terms t, t_0 well-typed in $\mathcal{E}$ that **do not use** ℓ **and** n:

$$\frac{}{[(\mathbf{att}(\ell\ \mathsf{t}) = \mathsf{n}\ \mathsf{t}_0) \to \mathsf{t}_0 \le \mathsf{t}]}$$

Indeed, $\mathbf{att}(\ell\ \mathsf{t})$ only depends on the random samplings $\mathsf{n}\ 1, \ldots, \mathsf{n}\ \mathsf{t}$, which are independent from $\mathsf{n}\ \mathsf{t}_0$ when $\mathsf{t} < \mathsf{t}_0$.

$\Rightarrow$ requires **in-depth** analysis of **recursive definitions**.

HO Indistinguishability Logic: Name Collision

Key ideas to find a condition under which the rule below is sound

$$\frac{}{[\mathsf{t} = \mathsf{n}\ \mathsf{t}_0 \rightarrow \neg\phi_{\mathsf{fresh}}]}$$

- Collect all **occurrences** at which name n is sampled in t, t_0, including in **recursive calls**.
  ⇒ use the set of **generalized subterms** $\mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\cdot)$.
  ($\mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{t})$ can be infinite)
- ϕ_{fresh} must ensure **independence** w.r.t. $(\mathsf{n}\ \mathsf{t}_0)$, i.e. that all generalized occurrences $(\mathsf{n}\ s)$ in $\mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{t}, \mathsf{t}_0)$ are s.t. $s \neq \mathsf{t}_0$.

HO Indistinguishability Logic: Generalized Subterms

$\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{t})$ are the **generalized subterms** of t.

$$
\begin{aligned}
\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(s) &\stackrel{\text{def}}{=} \{(\epsilon, \mathsf{true}, s)\} && \text{if } (s : \tau) \in \mathcal{E} \text{ or } s \notin \mathcal{E} \\
\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{x}) &\stackrel{\text{def}}{=} \mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{t}_0) && \text{if } (\mathsf{x} : \tau = \mathsf{t}_0) \in \mathcal{E} \\
\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{x}\ \mathsf{t}) &\stackrel{\text{def}}{=} \mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{t}_0\{y \mapsto \mathsf{t}\}) && \text{if } (\mathsf{x} : \tau = \lambda y.\, \mathsf{t}_0) \in \mathcal{E} \\
\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathcal{Q}(\mathsf{x} : \tau).\mathsf{t}_0) &\stackrel{\text{def}}{=} (\mathsf{x} : \tau).\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{t}_0) && \mathcal{Q} \in \{\lambda, \forall\} \\
\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{if}\ \phi\ \mathsf{then}\ \mathsf{t}_1\ \mathsf{else}\ \mathsf{t}_0) &\stackrel{\text{def}}{=} \mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\phi) \cup [\phi]\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(t_1) \cup [\neg\phi]\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(t_0) \\
\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{t}\ \mathsf{t}_0) &\stackrel{\text{def}}{=} \{(\epsilon, \mathsf{true}, \mathsf{t}\ \mathsf{t}_0)\} \cup && \text{if no other case applies} \\
&\qquad \mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{t}) \cup \mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\mathsf{t}_0)
\end{aligned}
$$

where y is taken fresh in the λ case and

$$
\begin{aligned}
[\phi]S &\stackrel{\text{def}}{=} \{(\vec{\alpha}, \psi \wedge \phi, \mathsf{t}) \mid (\vec{\alpha}, \psi, \mathsf{t}) \in S\} \\
(\mathsf{x} : \tau).S &\stackrel{\text{def}}{=} \{((\vec{\alpha}, \mathsf{x} : \tau), \psi, \mathsf{t}) \mid (\vec{\alpha}, \psi, \mathsf{t}) \in S\}
\end{aligned}
$$

$\mathcal{ST}^{\text{rec}}_{\mathcal{E}}(\cdot)$ ignores variable that can be unfolded into their definitions.

HO Indistinguishability Logic: Freshness Condition

Rule for Name Collision

$\mathcal{E}$ a **ground**, t, t_0 well-typed in $\mathcal{E}$.

$$\frac{}{[\mathsf{t} = \mathsf{n}\ \mathsf{t}_0 \rightarrow \neg\phi_{\mathsf{fresh}}]}$$

if t, t_0 are in eta-long form and if for $\mathbb{M} : \mathcal{E}$, $\eta \in \mathbb{N}$ and ρ:

$$[\![\phi_{\mathsf{fresh}}]\!]_{\mathbb{M}}^{\eta,\rho} = 1 \text{ implies } [\![\phi]\!]_{\mathbb{M}}^{\eta,\rho} = 1 \text{ for every } \phi \in \mathbb{S}$$

where $\mathbb{S}$ is a (possibly infinite) set formulas stating that $\mathsf{n}\ \mathsf{t}_0$ is **not sampled** in t, t_0.

$$\mathbb{S} \stackrel{\mathsf{def}}{=} \left\{(\forall\vec{\alpha}.\psi \Rightarrow \mathsf{s} \neq \mathsf{t}_0) \mid (\vec{\alpha}, \psi, \mathsf{n}\ \mathsf{s}) \in \mathcal{ST}_{\mathcal{E}}^{\mathsf{rec}}(\mathsf{t}, \mathsf{t}_0)\right\}$$

Proof: On the blackboard, using the Proposition shown later.

HO Indistinguishability Logic: Name Collision

Example

Assume t, t_0 do not use n nor ℓ.

$$\overline{[(\mathbf{att}(\ell\ \mathsf{t}) = \mathsf{n}\ \mathsf{t}_0) \to \mathsf{t}_0 \leq \mathsf{t}]}$$

All occurrences of name n in $\mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathbf{att}(\ell\ \mathsf{t}))$ are of the form

$$(\epsilon, \mathsf{t} \neq 0 \wedge \mathsf{pred}\ \mathsf{t} \neq 0 \wedge \cdots \wedge \mathsf{pred}^j\ \mathsf{t} \neq 0, \mathsf{n}\ (\mathsf{pred}^j\ \mathsf{t}))$$

for $j \in \mathbb{N}$ (there are infinitely many occurrences).

All of these are **guaranteed fresh** by the formula $\mathsf{t} < \mathsf{t}_0$:

$$(\mathsf{t} < \mathsf{t}_0) \to (\mathsf{pred}^j\ \mathsf{t} \neq \mathsf{t}_0)$$

Hence $\mathsf{t} < \mathsf{t}_0$ is a **suitable candidate** for ϕ_{fresh}, yielding the rule

$$\overline{[(\mathbf{att}(\ell\ \mathsf{t}) = \mathsf{n}\ \mathsf{t}_0) \to \neg(\mathsf{t} < \mathsf{t}_0)]}$$

$$\Leftrightarrow \quad \overline{[(\mathbf{att}(\ell\ \mathsf{t}) = \mathsf{n}\ \mathsf{t}_0) \to \mathsf{t}_0 \leq \mathsf{t}]}$$

HO Indistinguishability Logic: Name Collision

The semantics of a term t w.r.t. a model $\mathbb{M} : \mathcal{E}$ and **two different tapes** ρ_1 and ρ_2 is **identical**, if the interpretation of **declared variables** by $\mathbb{M}$ **coincides** on ρ_1 and ρ_2.

Proposition

Let t well-typed in $\mathcal{E}$ in eta-long form. Then $[\![t]\!]^{\eta,\rho_1}_{\mathbb{M}} = [\![t]\!]^{\eta,\rho_2}_{\mathbb{M}}$ if

$$\mathbb{M}(x)(\eta)(\rho_1)(a) = \mathbb{M}(x)(\eta)(\rho_2)(a) \quad \text{with } a \stackrel{\text{def}}{=} [\![\vec{u}]\!]^{\eta,\rho_1}_{\mathbb{M}'}$$

for all $(\vec{\alpha}, \phi, (x\ \vec{u})) \in \mathcal{ST}^{\text{rec}}_{\mathcal{E}}(t)$ such that:

- x is a variable declaration bound in $\mathcal{E}$ (not in $\vec{\alpha}$)
- $\mathbb{M}'$ extends $\mathbb{M}$ into a model of $(\mathcal{E}, \vec{\alpha})$
- $[\![\phi]\!]^{\eta,\rho_1}_{\mathbb{M}'} = 1$

Proof Sketch: induction over the generalized subterms of t involved in $[\![t]\!]^{\eta,\rho_1}_{\mathbb{M}}$.