MPRI 2.30: Proofs of Security Protocols

2. A Higher-Order Logic for Mechanization

Adrien Koutsos

2022/2023

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$@\tau$, *in*$@\tau$, *etc at ambient level.*
- More generally, large part of the reasoning done in the **ambient logic**. E.g. the logic lacks a **temporal component**.

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

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

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 such values to the adversary)
- **built-in** types interpretations are fixed.
  Example: $[\![\texttt{bool}]\!]^{\eta}_{\mathbb{M}} = \{0, 1\}$ for every η

HO Indistinguishability Logic: Variables

We assume a set x of **variables** $\mathcal{X}$ and

- $\mathcal{N} \subseteq \mathcal{X}$ a set of **names**, for random samplings.
  A name $\mathsf{n} \in \mathcal{N}$ type must be $\tau_0 \to \tau_1$ with τ_0 **finite**.
  (see typing rules next)
- $\mathcal{F}_{\text{built-ins}} \subseteq \mathcal{X}$ a set of **built-ins**, which are variables with a **restricted interpretations** (e.g. $\dot{\neg}, \dot{\wedge}, \mathbf{att}$).
  (see semantics next)

Using variables for everything allows a more unified treatment.

HO Indistinguishability Logic: Terms

Terms are defined by:

$$\mathsf{t} := \ \mathsf{x} \mid (\mathsf{t}\ \mathsf{t}) \mid \lambda(x : \tau).\,\mathsf{t} \mid \dot{\forall}(x : \tau).\,\mathsf{t} \mid \text{if } \mathsf{t} \text{ then } \mathsf{t} \text{ else } \mathsf{t} \qquad (\mathsf{x} \in \mathcal{X})$$

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

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

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

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

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

A Higher-Order Indistinguishability Logic: Term Typing

Term typing judgements

$$\textsc{Ty.Decl}\;\frac{}{\mathcal{E} \vdash \mathsf{x} : \mathcal{E}(\mathsf{x})}$$

$$\textsc{Ty.If}\;\frac{\mathcal{E} \vdash \mathsf{t} : \mathtt{bool} \qquad \mathcal{E} \vdash \mathsf{t}_i : \tau, i \in \{1,2\}}{\mathcal{E} \vdash \mathsf{if\ t\ then\ t_1\ else\ t_2} : \tau}$$

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

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

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

Environment typing

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

$$\textsc{Ty-Env.Decl}\;\frac{\vdash \mathcal{E}}{\vdash \mathcal{E}, (\mathsf{x} : \tau)}$$

$$\textsc{Ty-Env.Def}\;\frac{\vdash \mathcal{E} \qquad \mathcal{E} \vdash \mathsf{t} : \tau \qquad \mathsf{x} \notin (\mathcal{N} \cup \mathcal{F}_{\text{built-ins}})}{\vdash \mathcal{E}, \left(\mathsf{x} : \tau = \mathsf{t}\right)}$$

Names and built-ins symbols can only be declared.

HO Indistinguishability Logic: Probability Space

Terms are **interpreted** as η-indexed families of **random variables**.

- **probability space:** the set $\mathbb{T}_{\mathbb{M},\eta} = \mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta} \times \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$, where $\mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta}$ and $\mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ are **finite** same-length set of bit-strings.
  We equip it with the **uniform** probability measure.
  ($\mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta}$ for the adversary, $\mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ for honest functions)

HO Indistinguishability Logic: Term Semantics

A model $\mathbb{M}$ w.r.t. $\mathcal{E}$ (written $\mathbb{M} : \mathcal{E}$) interprets any **declaration** $(\mathsf{x} : \tau) \in \mathcal{E}$ as a family $(X_\eta)_{\eta\in\mathbb{N}}$ of functions $X_\eta : \mathbb{T}_{\mathbb{M},\eta} \to [\![\tau]\!]^{\eta}_{\mathbb{M}}$, which we write $\big(\mathbb{M}(\mathsf{x})(\eta)\big)_{\eta\in\mathbb{N}}$, with some **restrictions**:

- names are PTIME-computable (in η) **random samplings** using random in $\mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ (details later).
- **built-ins** in $\mathcal{F}_{\text{built-ins}}$ must be PTIME-computable *deterministic* (honest functions) or *adversarial* (random in $\mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta}$) functions.

HO Indistinguishability Logic: Term Semantics

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

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

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

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

$$[\![\text{if } \mathsf{t} \text{ then } \mathsf{t}_0 \text{ else } \mathsf{t}_1]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}} \stackrel{\text{def}}{=} [\![\mathsf{t}_i]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}} \text{ if } [\![\mathsf{t}]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}} = i$$

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

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

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

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

where $[\![\mathsf{n}]\!]_{\mathbb{M}}$ is a PTIME in 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

Remark

- $\mathcal{E}$ 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: Satisfiability and Validity

Notations

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

$$\mathsf{Pr}_\rho([\![\phi]\!]^{\eta;\rho}_{\mathbb{M}:\mathcal{E}} = 1) \in \mathsf{o.w.}(\eta)^1$$

- We write $\mathbb{M} : \mathcal{E} \models \mathbb{S}$ if $\mathbb{M} : \mathcal{E} \models \phi$ for every $\phi \in \mathbb{S}$.
  Remark: $\mathbb{S}$ can be infinite.
- **Validity:** $\mathcal{E} \models \phi$ if $\mathbb{M} : \mathcal{E} \models \phi$ for every $\mathbb{M} : \mathcal{E}$.

[1] $f \in \mathsf{o.w.}(\eta)$ iff. $(1 - f) \in \mathsf{negl}(\eta)$

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 $[\![\cdot]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}$.

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. $\mathsf{in}@\tau$).
  - $\Rightarrow$ support **uncomputable** functions.
  - $\Rightarrow$ support **quantifiers** $\dot\forall, \dot\exists$ over **arbitrary types**.
- the **probability space** is **finite**.
  - $\Rightarrow$ ensures that $(\rho \mapsto [\![t]\!]^{\eta,\rho}_{\mathbb{M},\mathcal{E}})$ 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: Recursive Definitions

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

Any type τ and order $< \in \mathcal{F}_{\text{built-ins}}$ with type $\tau \to \tau \to \texttt{bool}$ can be tagged as $\texttt{wf}(\tau, <)$.
$\Rightarrow$ only consider models s.t. $(\llbracket \tau \rrbracket^{\eta}_{\mathbb{M}}, \llbracket < \rrbracket^{\eta}_{\mathbb{M},\mathcal{E}})$ is **well-founded**.

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

Details

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

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

HO Indistinguishability Logic: Recursive Definitions

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

$$\textsc{Ty-Env.Rec-Def}\quad \frac{\vdash \mathcal{E} \qquad \mathcal{E}, \mathsf{x} : \tau \vdash \mathsf{t} : \tau \qquad \mathsf{wf}^{\mathsf{x},\mathsf{y}}_{\tau,<}(\mathsf{t}) \qquad \mathsf{x} \notin \mathcal{N} \cup \mathcal{F}_{\text{built-ins}}}{\vdash \mathcal{E}, \left(\mathsf{x} : \tau = \lambda \mathsf{y}.\, \mathsf{t}\right)}$$

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

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

$$\mathcal{E} \models (\dot\forall \vec{\alpha}.\, \phi \dot\rightarrow \mathsf{t}_0 < \mathsf{y}) \quad \text{for any } (\vec{\alpha}, \phi, \mathsf{x}\ \mathsf{t}_0) \in \mathcal{ST}(\mathsf{t})$$

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

Example

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

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

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.

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

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

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

Example

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

HO Indistinguishability Logic: Protocols

Example: encoding of Basic Hash

$$
\begin{aligned}
\mathsf{in}@t &= \texttt{match}\ t\ \texttt{with}\ \mathsf{init} \to d \\
&\qquad \mid \_ \to \mathbf{att}(\mathsf{frame}@\mathsf{pred}\ t) \\
\mathsf{out}@t &= \texttt{match}\ t\ \texttt{with}\ \mathsf{init} \to d \\
&\qquad \mid \mathsf{T}(\mathsf{A},\mathsf{i}) \to \langle \mathsf{n}(\mathsf{A},\mathsf{i}), \mathsf{h}(\langle \mathsf{in}@t, \mathsf{n}(\mathsf{A},\mathsf{i})\rangle, \mathsf{k}\ \mathsf{A})\rangle \\
&\qquad \mid \mathsf{R}\ \mathsf{j} \to \dots \\
\mathsf{frame}@t &= \texttt{match}\ t\ \texttt{with}\ \mathsf{init} \to d \\
&\qquad \mid \_ \to \langle \mathsf{frame}@\mathsf{pred}\ t, \mathsf{out}@t\rangle
\end{aligned}
$$

Formulas

HO Indistinguishability Logic: Formulas

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

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

HO Indistinguishability Logic: Formula Semantics

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

$[\![\Phi]\!]_{\mathbb{M}:\mathcal{E}} \in \{0,1\}$ is as expected for **boolean connective** and FO **quantifiers**. E.g.:

$$[\![\top]\!]_{\mathbb{M}:\mathcal{E}} \stackrel{\text{def}}{=} 1 \qquad\qquad [\![\Phi \wedge \Psi]\!]_{\mathbb{M}:\mathcal{E}} \stackrel{\text{def}}{=} [\![\Phi]\!]^{\sigma}_{\mathcal{M}} \text{ and } [\![\Psi]\!]^{\sigma}_{\mathcal{M}}$$

$$[\![\neg\Phi]\!]_{\mathbb{M}:\mathcal{E}} \stackrel{\text{def}}{=} \text{not } [\![\Phi]\!]^{\sigma}_{\mathcal{M}}$$

$$[\![\forall(\mathsf{x} : \tau).\Phi]\!]_{\mathbb{M}:\mathcal{E}} \stackrel{\text{def}}{=} 1 \quad \text{ if } \forall A \in \left([\![\tau]\!]^{\eta}_{\mathbb{M}}\right)_{\eta\in\mathbb{N}}, [\![\Phi]\!]_{\mathbb{M}[\mathsf{x}\mapsto A]:(\mathcal{E},\mathsf{x}:\tau)} = 1$$

HO Indistinguishability Logic: Formula Semantics

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

$[\![\vec{t_1} \sim \vec{t_2}]\!]_{\mathbb{M}:\mathcal{E}} = 1$ iff. $\forall$ PPTM $\mathcal{A}$, $\mathsf{Adv}^{\eta}_{\mathbb{M}:\mathcal{E}}(\mathcal{A} : \vec{t_1} \sim \vec{t_2})$ is negligible.

Execution Model

- Values in $[\![\tau_b]\!]^{\eta}_{\mathbb{M}}$ 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 input it can compute, any number of times.
  Remark: queries can yield more oracles, which $\mathcal{A}$ can in turn query (e.g. for type $\tau_0 \to (\tau_1 \to \tau_2)$).
- We require that terms in $\vec{t_1}$ and $\vec{t_2}$ have types $\tau_b^0 \to \dots \to \tau_b^n$ (i.e. no higher-order arguments).

HO Indistinguishability Logic: Proof System

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

Example: **function application** splits into two rules

$$\textsc{FA-App}\quad \frac{\vec{u}_1, \mathrm{t}_1, \mathrm{t}'_1 \sim \vec{u}_2, \mathrm{t}_2, \mathrm{t}'_2}{\vec{u}_1, \mathrm{t}_1\ \mathrm{t}'_1 \sim \vec{u}_2, \mathrm{t}_2\ \mathrm{t}'_2} \qquad \textsc{FA-Const}\quad \frac{\vec{u}_1 \sim \vec{u}_2}{\vec{u}_1, f \sim \vec{u}_2, f} \qquad (\text{where } f \in \mathcal{F}_{\text{built-ins}})$$

Moreover, FA-App can be extended to apply under a λ:

$$\textsc{FA-App}_\lambda\quad \frac{\begin{array}{c}\vec{u}_1,(\lambda(x:\tau).\,\mathrm{t}_1),(\lambda(x:\tau).\,\mathrm{t}'_1)\\ \sim\ \vec{u}_2,(\lambda(x:\tau).\,\mathrm{t}_2),(\lambda(x:\tau).\,\mathrm{t}'_2)\end{array}}{\vec{u}_1, \lambda(x:\tau).\,(\mathrm{t}_1\ \mathrm{t}'_1) \sim \vec{u}_2, \lambda(x:\tau).\,(\mathrm{t}_2\ \mathrm{t}'_2)}$$

Remark: soundness proof requires to **simulate the oracles**.

HO Indistinguishability Logic: Formula and Term Quantifiers

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

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

Proposition

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

$$\mathbb{M} : \mathcal{E} \models \forall(\mathsf{x} : \tau).\,(\phi \sim \mathsf{true}) \quad \text{iff.} \quad \mathbb{M} : \mathcal{E} \models \left(\dot{\forall}\,(\mathsf{x} : \tau).\,\phi\right) \sim \mathsf{true}$$

Preliminary Remark

A function $f : \mathbb{S} \mapsto [0,1]$ is **overwhelmingly true**, written $f(\eta) \in \mathsf{o.w.}(\eta)$, if $(1 - f(\eta)) \in \mathsf{negl}(\eta)$.

For any term $\mathcal{E} \vdash \phi : \texttt{bool}$ and model $\mathbb{M}$:

$$\mathbb{M} : \mathcal{E} \models \phi \sim \mathsf{true} \quad \text{iff.} \quad \mathsf{Pr}_\rho([\![\phi]\!]^{\eta;\rho}_{\mathbb{M}:\mathcal{E}}) \in \mathsf{o.w.}(\eta)$$

Proof: $\Rightarrow$ take $\mathcal{A}$ to be the identity. $\Leftarrow$ trivial up-to-bad reasoning.

HO Indistinguishability Logic: Formula and Term Quantifiers

Proof of the Proposition

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

$$\mathbb{M} : \mathcal{E} \models (\dot{\forall}(x : \tau).\, \phi \sim \mathsf{true}) \qquad (\star)$$

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

$$\mathsf{Pr}\left([\![\phi]\!]^{\eta,\rho}_{\mathbb{M}[x \mapsto A]:(\mathcal{E}, x:\tau)}\right) \in \mathsf{o.w.}(\eta)$$

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

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

HO Indistinguishability Logic: Formula and Term Quantifiers

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

$$\mathbb{M} : \mathcal{E} \models \forall(x : \tau).\, (\phi \sim \text{true}) \qquad (\dagger)$$

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

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

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

where a_{witness} is an arbitrary value in $\llbracket \tau \rrbracket^{\eta}_{\mathbb{M}}$ (recall that $\llbracket \tau \rrbracket^{\eta}_{\mathbb{M}} \neq \emptyset$), 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

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

Then:

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

HO Indistinguishability Logic: Reachability Proof System

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

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

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

Freshness and Cryptographic Rules

HO Indistinguishability Logic: Name Collision

We allow **names** (i.e. random samplings) over arbitrary types.
$\Rightarrow$ names can have collisions.

- e.g. $\mathsf{Pr}(\llbracket \mathsf{n}_0 \doteq \mathsf{n}_1 \rrbracket)$ is non-negligible if $\mathsf{n}_0, \mathsf{n}_1 : \texttt{bool}$.

Large names are names with around η random bits:

- for any name $\mathsf{n} : \tau_0 \to \tau$ over a **large** type τ (e.g. $\texttt{message}$), we ask that for any $\eta \in \mathbb{N}$, $a \in \llbracket \tau_0 \rrbracket^\eta_{\mathbb{M}}$ and $b \in \llbracket \tau \rrbracket^\eta_{\mathbb{M}}$,

$$\mathsf{Pr}_{\rho_{\mathsf{h}}} \left(\llbracket \mathsf{n} \rrbracket_{\mathbb{M}}(\eta, a)(\rho_{\mathsf{h}}) = b \right) \leq \frac{1}{2^{c_\tau \cdot \eta}}$$

where $c_\tau > 0$ is a positive real number.

HO Indistinguishability Logic: Name Collision

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

Base Logic Rule

$$\frac{}{t \doteq \mathsf{n} \sim \mathsf{false}} \quad \text{when } \mathsf{n} \notin \mathsf{st}(t)$$

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

Rule for Name Collision (first tentative)

$\mathcal{E}$ with only **declarations** of built-ins and names ($\approx$ ground-terms).

t, t_0 well-typed in $\mathcal{E}$ and $(\mathsf{n} : \_ \to \tau) \in \mathcal{E}$ where τ is **large**

$$\frac{}{\mathsf{t} \doteq \mathsf{n}\ \mathsf{t}_0 \sim \mathsf{false}}$$

when n does not appear in t, 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.

$\mathcal{E}$ with only **declarations** of built-ins and names, except for a **single inductive definition**:

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

where $\mathsf{n} : \mathtt{int} \to \mathtt{message}$.

Rule (special case)

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

$$\frac{}{\left(\mathbf{att}(\ell\ \mathsf{t}) \doteq \mathsf{n}\ \mathsf{t}_0\right) \dot{\to} \mathsf{t}_0 \leq \mathsf{t} \sim \text{true}}$$

Indeed, $\mathbf{att}(\ell\ \mathsf{t})$ only depends on the random samplings $\mathsf{n}\ 1, \dots, \mathsf{n}\ \mathsf{t}$, 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: conditions under which this name collision rule is sound

$$\frac{}{\mathsf{t} \doteq \mathsf{n}\ \mathsf{t}_0 \mathrel{\dot{\rightarrow}} \dot{\neg}\phi_{\mathsf{fresh}} \sim \mathsf{true}}$$

- Collect all **occurrences** at which name n is sampled in t, t_0, including in **recursive calls**.
  $\Rightarrow$ use the set of **generalized subterms** $\mathcal{ST}_{\mathcal{E}}^{\mathsf{rec}}(\cdot)$.
  ($\mathcal{ST}_{\mathcal{E}}^{\mathsf{rec}}(\mathsf{t})$ 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 $\mathcal{ST}_{\mathcal{E}}^{\mathsf{rec}}(\mathsf{t}, \mathsf{t}_0)$ are s.t. $s \mathrel{\dot{\neq}} \mathsf{t}_0$.

HO Indistinguishability Logic: Generalized Subterms

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

$$
\begin{array}{rcll}
\mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{x}) & \stackrel{\mathsf{def}}{=} & \{(\epsilon, \mathsf{true}, \mathsf{x})\} & \text{if } (\mathsf{x} : \tau) \in \mathcal{E} \text{ or } \mathsf{x} \notin \mathcal{E} \\
\mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{x}) & \stackrel{\mathsf{def}}{=} & \mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{t}_0) & \text{if } (\mathsf{x} : \tau = \mathsf{t}_0) \in \mathcal{E} \\
\mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{x}\ \mathsf{t}) & \stackrel{\mathsf{def}}{=} & \mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{t}_0\{y \mapsto \mathsf{t}\}) & \text{if } (\mathsf{x} : \tau = \lambda y.\, \mathsf{t}_0) \in \mathcal{E} \\
\mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{t}\ \mathsf{t}_0) & \stackrel{\mathsf{def}}{=} & \begin{array}{l} \{(\epsilon, \mathsf{true}, \mathsf{t}\ \mathsf{t}_0)\} \cup \\ \mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{t}) \cup \mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\mathsf{t}_0) \end{array} & \text{if no other case applies}
\end{array}
$$

where the if-then-else and quantifier cases are as in $\mathcal{ST}(\cdot)$, and y is taken fresh in the λ case.

💡 *$\mathcal{ST}^{\mathsf{rec}}_{\mathcal{E}}(\cdot)$ ignores variable that can be unrolled into their definitions.*

HO Indistinguishability Logic: Freshness Condition

Rule for Name Collision

$\mathcal{E}$ with only **declarations** of built-ins and names ($\approx$ ground-terms).

t, t_0 well-typed in $\mathcal{E}$ and $(\mathsf{n} : \_ \to \tau) \in \mathcal{E}$ where τ is **large**

$$\frac{}{\mathsf{t} \doteq \mathsf{n}\ \mathsf{t}_0 \mathrel{\dot{\to}} \dot{\neg}\phi_{\mathsf{fresh}} \sim \mathsf{true}}$$

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

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

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

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

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.

$$\frac{}{\left(\mathbf{att}(\ell\ \mathsf{t}) \doteq \mathsf{n}\ \mathsf{t}_0\right) \mathrel{\dot{\rightarrow}} \mathsf{t}_0 \leq \mathsf{t} \sim \mathsf{true}}$$

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

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

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

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

$$(\mathsf{t} < \mathsf{t}_0) \mathrel{\dot{\rightarrow}} (\mathsf{pred}^j\ \mathsf{t} \mathrel{\dot{\neq}} \mathsf{t}_0)$$

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

$$\frac{}{\left(\mathbf{att}(\ell\ \mathsf{t}) \doteq \mathsf{n}\ \mathsf{t}_0\right) \mathrel{\dot{\rightarrow}} \dot{\neg}(\mathsf{t} < \mathsf{t}_0) \sim \mathsf{true}}$$

$$\Leftrightarrow \quad \frac{}{\left(\mathbf{att}(\ell\ \mathsf{t}) \doteq \mathsf{n}\ \mathsf{t}_0\right) \mathrel{\dot{\rightarrow}} \mathsf{t}_0 \leq \mathsf{t} \sim \mathsf{true}}$$

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 $[\![t]\!]^{\eta,\rho_1}_{\mathbb{M}:\mathcal{E}} = [\![t]\!]^{\eta,\rho_2}_{\mathbb{M}:\mathcal{E}}$ if

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

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 $(\mathcal{E}, \vec{\alpha})$
- $[\![\phi]\!]^{\eta,\rho_1}_{\mathbb{M}':\mathcal{E},\vec{\alpha}} = 1$

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