Proofs for "a uniform type structure for secure information flow"

Kohei Honda Nobuko Yoshida

	$\tau, \uparrow_{\rm L}$	$\oplus\uparrow_{\rm L}, \uparrow_{\rm A}$	$\downarrow_{\rm L}$	$\downarrow_{\rm A}$
affecting:	no	yes	no	no
enabled:	yes	yes	yes	no
	$?_{\rm L}, ?_{\rm A}$	$!_{\rm L}, !_{\rm A}$	$?_{{\rm L}\mu}$	$!_{{\rm L}\mu}$
affecting:	no	no	yes	no
enabled:	yes	no	yes	no

Figure 14: Classification of Actions

E Proofs for Section 2

E.1 Proposition 2.4

(i) and (ii) follow [6, 49]. The proof of (iii) uses the observation that we can shrink all affine types and associated (prime) terms without altering the actions involved in the stated linear action, reducing the problem to that of linearly typed processes. Then we use the corresponding result (Lemma 6.2) in [49].

F Proofs for Section 3

F.1 Proposition 3.2

(i) and (iii) are by the same reasoning as given in [6, 49, 23]. For (ii), the case for $\tau \leq \tau'$ is by observing that, in $\leq$, the occurring types are ordered covariantly, and that each prefix rule allows a type of the subject which is smaller than specified. The case for $\tau \doteq \tau'$ is by noting the prefix rules for non-receiving, non-tampering prefixes do not care their outermost secrecy levels.

F.2 Proposition 3.4: (a) Preliminaries

For reference we restate the proposition.

(non-interference) *Let* $\Gamma \vdash_{\rm sec} P_i \triangleright A$ *(*$i = 1, 2$*) such that* $\mathsf{tamp}_\Gamma(A) = s$*. Then* $s \not\sqsubseteq s'$ *implies* $\Gamma \vdash_{\rm sec} P_1 \cong^{\pi}_{s'} P_2$.

The proof uses a (proper) subcongruence of $\cong^{\pi}_{s}$, which is defined as a non-standard weak bisimilarity. The bisimilarity differs from the known constructions in that it abstracts away not only τ-actions but also certain visible actions, which makes its definition more complex than that of the standard ones. We use the typed transition following [7, 49]. Transition labels are:

$$l \ ::= \ \boldsymbol{\tau} \mid x(\vec{y}) \mid \overline{x}(\vec{y}) \mid x\,\mathtt{in}_i(\vec{y}) \mid \overline{x}\mathtt{in}_i(\vec{y})$$

$\mathsf{sbj}(l)$ is the initial name of l when $l \neq \tau$. $\mathsf{fn}(l)$ and $\mathsf{bn}(l)$ are free and bound names in l, respectively. $t, t', \ldots$ often range over a sequence of actions. First, the untyped transition $P \xrightarrow{l} Q$ is defined as in the standard manner (see Appendix F.4 in [49]). We say A *prohibits* l when $\perp x \in |A|$ and $x = \mathsf{sbj}(l)$ or $!_{\rm L}x \in |A|$, l is output and $\mathsf{sbj}(l) = x$. We then write $\Gamma \vdash P \xrightarrow{l} \Gamma' \cdot \Delta \vdash Q$ iff, for $\Gamma \vdash P \triangleright A$, we have (1) $P \xrightarrow{l} Q$ such that $\mathsf{bn}(l) \cap \mathsf{fn}(\Gamma) = \emptyset$ and (2) A does not prohibit l, with

(a) $\Gamma' = \Gamma/x$ if $\mathsf{md}(\Gamma(x)) \in \mathcal{M}_{\downarrow,\uparrow}$, $\Gamma' = \Gamma$ if else, and

(b) $\Delta = \{y_i : \tau_i \mid \Gamma \vdash x : (\vec{\tau})^p, l$ has mode p under $\Gamma\}$, similarly when l is branching.

We use the classification of typed actions in Figure 14 (except for $?_{{\rm L}\mu}$ and $!_{{\rm L}\mu}$). In the table, unary linear output (denoted by $\uparrow_{\rm L}$) does not affect since it is inevitable and are fixed in shape, while linear selection (denoted by $\oplus\uparrow_{\rm L}$) does so; $?_{\rm L}, ?_{\rm A}$ have no effect since they only touch stateless replications. We say:

- l under Γ is *affecting, non-affecting and enabled* following the mode $\Gamma(\mathsf{sbj}(l))$.
- l under Γ is *s-affecting* if it is affecting and, moreover, the type of its subject in Γ has a secrecy level s' such that $s' \sqsubseteq s$. If not, we say l is *non-s-affecting*.

We define relativised invisibility as follows. We write $\Gamma \asymp \Delta$ when $\Gamma(x) = \Delta(x)$ for each $x \in \mathsf{fn}(\Gamma) \cap \mathsf{fn}(\Delta)$. $\Gamma \vdash l$ indicates either $l = \boldsymbol{\tau}$ or, if not, its shape follows Γ. Let $\Gamma \asymp \Delta$ and $\Gamma \vdash l$ below.

- (invisible actions) l is Δ-*invisible* when either $\mathsf{fn}(l) \cap \mathsf{fn}(\Delta) = \emptyset$ or, if not, l is an output which is both non-affecting and enabled under Γ. If l is Δ-invisible and enabled under Γ, then l is *strongly* Δ-*invisible*.
- (s-invisible actions) Δ-*s-invisible actions* and *strongly* Δ-*s- invisible actions* are defined by literally replacing "non-affecting" with "non-s-affecting" above.
- (abstracted actions) We also write: $\Gamma \vdash P \xrightarrow{\hat{l}}_{\Delta,s} \Gamma' \vdash P'$ when either (1) $\Gamma \vdash P \xrightarrow{l} \Gamma' \vdash P'$ or (2) $\Gamma' \stackrel{\rm def}{=} \Gamma$, $P \stackrel{\rm def}{=} P'$ and l is s-Δ-invisible under Γ. We also write $\Gamma \vdash P \Longrightarrow_{\Delta,s} \Gamma' \vdash P'$ when $\Gamma \vdash P \stackrel{l_1 \ldots l_n}{\longrightarrow} \Gamma' \vdash P'$ with each l_i strongly s-Δ-invisible. Following these notations we define $\Gamma \vdash P \stackrel{l}{\Longrightarrow}_{\Delta,s} \Gamma' \vdash P'$ (resp. $\Gamma \vdash P \stackrel{\hat{l}}{\Longrightarrow}_{\Delta,s} \Gamma' \vdash P'$).

The abstraction of non-τ-actions necessitate two further notions. Below (1) is to relate typed terms with different bases when an abstracted non-τ-action changes a base. (2) is to abstract away a linear branching input. In (2) a *branching variant of* l is a (well-typed) branching input with the same subject as l and a different index. Actions are always considered up to α-equality.

(1) (semi-typed relation) A relation, say $\mathcal{R}$, over typed terms is *semi-typed* when $(\Gamma \vdash P \triangleright A)\,\mathcal{R}\,(\Delta \vdash Q \triangleright B)$ implies the projections of Γ and Δ (resp. A and B) on $\mathsf{fn}(\Gamma) \cap \mathsf{fn}(\Delta)$ coincide. We write $\Gamma \vdash P\,\mathcal{R}_{\Theta,C}\,\Delta \vdash Q$ or $\Gamma \vdash P\,\mathcal{R}_{\Theta}\,\Delta \vdash Q$ to indicate $\mathcal{R}$ is semi-typed as well as the intersecting part is Θ and C.

(2) (branching closure) A set Ψ of typed transitions $\{\Gamma \vdash P \xrightarrow{t_i} \Delta_i \vdash P_i\}_{i\in I}$ is Δ-*branching-closed*, or often simply *closed*, when the following conditions hold: Whenever $t_i = sls'$ with l being a linear branching input s.t. $\mathsf{fn}(l) \cap \mathsf{fn}(\Delta) = \emptyset$, there is $t_j = sl's''$ $(j \in I)$ for each branching variant l' of l.

We can now introduce the bisimilarity.

Definition F.1 (s-bisimulation) *A semi-typed relation $\mathcal{R}$ is a s-bisimulation when $\Gamma_1 \vdash P_1 \,\mathcal{R}\, \Gamma_2 \vdash P_2$ with $\Delta = \Gamma_1 \cap \Gamma_2$ implies the following and its symmetric case: Whenever $\Gamma_1 \vdash P_1 \xrightarrow{l} \Gamma_1' \vdash P_1'$, there is a Δ-closed $\{\Gamma_2 \vdash P_2 \stackrel{\hat{l}}{\Longrightarrow}_{\Delta,s} \Gamma_{2i}' \vdash P_{2i}'\}$ such that $\Gamma_1' \vdash P_1' \,\mathcal{R}\, \Gamma_{2i}' \vdash P_{2i}'$. We write $\Gamma_1 \vdash P_1 \approx_s^{\iota} \Gamma_2 \vdash P_2$ when there is a s-bisimulation between $\Gamma_1 \vdash P_1$ and $\Gamma_2 \vdash P_2$. The typed sub-relation of the maximum s-bisimulation is denoted $\approx_s^{\iota}$.*

Using the partial confluence (cf. [31]) of strongly invisible actions vis-a-vis other actions modulo additional strongly invisible actions, we can show $\approx_s^{\iota}$ is a congruence, hence $\approx_s^{\iota} \subset \cong_s^{\pi}$. It is notable that the partial confluence relies on the linear action lemma. We also observe that, in practice, branching closure can often be ignored. However the notion is necessary for consistency of the bisimilarity (indeed the construction does not give a congruence without branching closure).

F.3 Proposition 3.4: (b) Proof

The proof is by showing the following relation is a s-bisimulation:

$$(\Gamma_1 \vdash_{\mathsf{sec}} P_1 \triangleright A_1)\, \mathcal{R}_{\Delta,B}\, (\Gamma_2 \vdash_{\mathsf{sec}} P_2 \triangleright A_2) \quad \stackrel{\text{def}}{\Leftrightarrow} \quad \mathsf{tamp}_{\Delta}(B) \not\sqsubseteq s.$$

Let $\Gamma_1 \vdash P_1 \xrightarrow{l} \Gamma_1' \vdash P_1'$. First assume l is not an input. Then by $\mathsf{tamp}_{\Delta}(B) \not\sqsubseteq s$, we know l is s-Δ-invisible. We let $\Gamma_2 \vdash P_2$ simulate this by the inaction, resulting in the same closure (note the singleton consisting of the inaction is always branching-closed). Second if l is an input and its subject is outside of Δ, then this is again simulated by the inaction. Thirdly, assume l is an input with its subject, say x, occurring in Δ, with mode p. Then, by $A_1 \restriction \mathsf{fn}(\Delta) = A_2 \restriction \mathsf{fn}(\Delta)$ and because input is always available, P_2 can do the same action:

$$\Gamma_2 \vdash P_2 \xrightarrow{l} \Gamma_2' \vdash P_2'$$

Let $\vec{y} : \vec{\tau}$ be a newly introduced base by this transition, with $\mathsf{md}(\vec{\tau}) = \vec{q}$. Note y_i should be an output. By $\mathsf{tamp}_{\Delta}(px) \not\sqsubseteq s$, we know $\mathsf{tamp}_{\Delta}(q_i y_i) \not\sqsubseteq s$, hence the resulting pair is again in the closure. This establishes the bisimilarity of $\mathcal{R}$.

F.4 Proposition 3.5

Remark. The presentation of DCC in our initial version considers lifted types modulo the equation $\llcorner T_1 \Rightarrow T_2 \lrcorner = T_1 \Rightarrow \llcorner T_2 \lrcorner$. This is non-standard but induces a sound notion of pointedness, hence a consistent variant of DCC. In particular, its embedding in $\pi^{\mathsf{LA}}_{\mathsf{sec}}$, as given in the initial version, satisfies Proposition 3.5, hence Theorem 3.6 (noninterference) holds. The updated version eliminates this equation and changes the encoding of $\mathtt{lift}(M)$ and $\mathtt{seq}$ accordingly. The following proof is for this updated version.

(i) (syntactic soundness) *$E \vdash M : T$ implies $E^\circ \cdot u : T^\circ \vdash_{\mathsf{sec}} [\![M]\!]_u \triangleright \langle T \rangle_{u,E}$.*

By induction of M. The only interesting cases are:

(a) $M \equiv \mathtt{bind}\ x = N_1\ \mathtt{in}\ N_2$

(b) $M \equiv \mathtt{lift}(N)$

(c) $M \equiv \mathtt{seq}\ x = N_1\ \mathtt{in}\ N_2$

Other cases are the same as [7, 49].

Case (a). We must show if $E^\circ \cdot x : [T_1 ... T_n (\gamma)_s]^\circ \vdash_{\mathsf{sec}} [\![N_1]\!]_x \triangleright A_1$ and $E^\circ \cdot x : \overline{[T_1 ... T_n \gamma]^\circ} \cdot u : [T_1' ... T_n' \gamma']^\circ \vdash_{\mathsf{sec}} [\![N_2]\!]_u \triangleright A_2$ with $s \sqsubseteq \mathsf{sec}(\gamma')$, then $E^\circ \cdot u : [T_1' ... T_n' \gamma']^\circ \vdash_{\mathsf{sec}} [\![M]\!]_u \triangleright A$ where $A_1 = \langle [T_1 ... T_n (\gamma)_s] \rangle_{x, E \cdot x:[T_1 ... T_n (\gamma)_s]}$, $A_2 = \langle [T_1' ... T_n' \gamma'] \rangle_{u, E \cdot x:[T_1 ... T_n \gamma]}$, and $A = \langle [T_1' ... T_n' \gamma'] \rangle_{u,E}$.

First $(A_1 \odot A_2)/x = A$ is mechanical. We also note the tampering levels of $[\![N_1]\!]_x$, $[\![N_2]\!]_u$ and $[\![M]\!]_u$ coincide with $\mathsf{sec}(\gamma) \sqcup s$, $\mathsf{sec}(\gamma')$, and $\mathsf{sec}(\gamma')$, respectively because $\mathsf{protect}(\gamma) = \mathsf{sec}(\gamma)$ and $\mathsf{protect}(\gamma') = \mathsf{sec}(\gamma')$ (hence we omit action types). Here we only have to prove:

$$\begin{array}{l} E^\circ \cdot x : \overline{[T_1 ... T_n \gamma]^\circ} \cdot u : [T_1' ... T_n' \gamma']^\circ \vdash_{\mathsf{sec}} [\![N_2]\!]_u \text{ implies} \\ E^\circ \cdot x : \overline{[T_1 ... T_n (\gamma)_s]^\circ} \cdot u : [T_1' ... T_n' \gamma']^\circ \vdash_{\mathsf{sec}} [\![N_2]\!]_u \end{array}$$

Note that we cannot directly use the former of Lemma 3.2 (ii) when $\mathsf{sec}(\gamma) \sqsubseteq s$ since $\overline{[T_1 ... T_n (\gamma)_s]^\circ} \leq \overline{[T_1 ... T_n \gamma]^\circ}$ by definition of $\leq$ in Figure 3.

We prove this by induction on N_2. If $x \notin \mathsf{fn}(N_2)$, then it is proved by the standard weakening. Hence we only have to consider the case $x \in \mathsf{fn}(N_2)$. Moreover, if N_2 is not variable x, then it is straightforward by the inductive hypothesis. Thus we will prove:

$$\begin{array}{l} \Gamma \vdash_{\mathsf{sec}} !u(\vec{x}z).\overline{x}(\vec{x}'z')(\Pi_i [x_i' \to x_i]^{T^\circ} \mid [z' \to z]^{\overline{\gamma^\bullet}}) \\ \text{implies} \\ \Gamma' \vdash_{\mathsf{sec}} !u(\vec{x}z).\overline{x}(\vec{x}'z')(\Pi_i [x_i' \to x_i]^{T^\circ} \mid [z' \to z]^{\overline{\gamma^\bullet}}) \\ \text{where} \\ \Gamma = x : \overline{[T_1 ... T_n \gamma]^\circ} \cdot u : [T_1' ... T_n' \gamma']^\circ \text{ and} \\ \Gamma' = x : \overline{[T_1 ... T_n (\gamma)_s]^\circ} \cdot u : [T_1' ... T_n' \gamma']^\circ. \end{array}$$

Similarly for the branching copy cat. Note that this relates only to the typability of $[z' \to z]^{\overline{\gamma^\bullet}}$. This is because u and x_i's mode is $!$, and x's mode is output, so they are not receiving at any level (cf. Definition 3.1). Hence w.o.l.g. we only have to prove the following lemma:

- **(copy-cat)** $z' : \tau \cdot z : \overline{\tau}' \vdash_{\mathsf{sec}} [z' \to z]$ implies $z' : \tau' \cdot z : \overline{\tau}' \vdash_{\mathsf{sec}} [z' \to z]$ with $\mathsf{sec}(\tau) = \mathsf{tamp}(\tau) \sqsubseteq \mathsf{tamp}(\tau') = \mathsf{sec}(\tau')$ where z is immediate tampering (note $\tau \doteq \tau'$).

The proof is easy by structure induction of τ. For example, as a base case, suppose $\Gamma \vdash_{\mathsf{sec}} z'.\overline{z}$ with $s \sqsubseteq s'$ and $\Gamma = z' : ()_s^{\downarrow_{\mathsf{A}}} \cdot z : ()_{s'}^{\uparrow_{\mathsf{A}}}$. Then $\downarrow_{\mathsf{A}} z'$ receives at s under Γ. Hence we can exchange s by any s' in Γ because this still satisfies $s' \sqsubseteq \mathsf{tamp}_{\Gamma'}(\uparrow_{\mathsf{A}}) = s'$ with $\Gamma' = z' : ()_{s'}^{\downarrow_{\mathsf{A}}} \cdot z : ()_{s'}^{\uparrow_{\mathsf{A}}}$, so $\downarrow_{\mathsf{A}} z' \succ^{\Gamma} \uparrow_{\mathsf{A}} z$. Thus we have $z' : ()_{s'}^{\downarrow_{\mathsf{A}}} \cdot z : ()_{s'}^{\uparrow_{\mathsf{A}}} \vdash_{\mathsf{sec}} z'.\overline{z}$, as required. We also use Lemma 3.2 (ii) here for a copycat with non-tampering types.

Case (b). Suppose $E^\circ \cdot m : T^\circ \vdash_{\mathsf{sec}} [\![M]\!]_m \triangleright \langle T \rangle_{m,E}$. Then for all T and M, we have

$$E^\circ \cdot c : (T^\circ)_s^{\uparrow_{\mathsf{A}}} \vdash_{\mathsf{sec}} \overline{c}(m)[\![M]\!]_m \triangleright \uparrow_{\mathsf{A}} c \otimes ?_{\mathsf{L}} ?_{\mathsf{A}} \vec{y}$$

because m is active in $\langle T \rangle_{m,E}$ (hence $\uparrow_{\mathsf{A}} c(m) \succ^{\Gamma} \langle T \rangle_{m,E}$), and c is an output (hence we do not have to consider the security level). Then we can get:

$$E^\circ \cdot u : ((T^\circ)_s^{\uparrow_{\mathsf{A}}})^{!_{\mathsf{A}}} \vdash_{\mathsf{sec}} !\, u(c).\overline{c}(m)[\![M]\!]_m \triangleright\, !_{\mathsf{A}} u \otimes ?_{\mathsf{L}} ?_{\mathsf{A}} \vec{y}$$

because c is active (hence $\mathbf{!}_{\mathrm{A}}u(c) \succ (\uparrow_{\mathrm{A}}c \otimes \mathbf{?}_{\mathrm{L}}\mathbf{?}_{\mathrm{A}}\vec{y})$), and u is not receiving at any level (hence we do not have to consider the security level again).

Case (c). We only have to prove $\mathsf{Lift}\langle xn\rangle^{[T_1\ldots T_n\gamma]}$ is typable when n's mode is $\mathbf{?}_{\mathrm{A}}$, c's mode is $\downarrow_{\mathrm{A}}$ and c's security level is $\perp$.

$$x:\overline{T^\circ}\cdot n:((T^\circ)^{\downarrow_{\mathrm{A}}}_{\perp})^{\mathbf{?}_{\mathrm{A}}} \vdash_{\mathrm{sec}} \mathsf{Lift}\langle xn\rangle^{[T_1\ldots T_n\gamma]}$$

with $\mathsf{Lift}\langle xn\rangle^{[T_1\ldots T_n\gamma]} \stackrel{\mathrm{def}}{=} \mathbf{!}x(\vec{z}w).\overline{n}(c)c(m).\overline{m}(\vec{z}'w')(\Pi[z_i' \to z_i] \mid [w' \to w]^{\overline{\gamma}^\bullet})$. We have two cases: (1) γ is pointed or (2) γ is not pointed. For the case (1), since all x, c, m, w and w' are affine channels, we only have to ensure that n's level is less than the tamper level of w, which is obvious by assumption. For the case (2), we need to assign the mode $\downarrow_{\mathrm{L}}$ to w' and $\mathbf{?}_{\mathrm{L}}$ to m. Again, we can mechanically check the typability by (C1-3) in S.2.3 and by definition of $\succ$ in 2.2. Hence $(\boldsymbol{\nu}\, x)([\![M]\!]_u \mid \mathsf{Lift}\langle xn\rangle)$ is always typable, which implies the required result.

(ii) (adequacy) The proof is by following the proof of a similar result for the affine calculus, given in Appendix J.1 of [7], which uses the extended reduction [49]. This proves $M \Downarrow$ iff $[\![M]\!]_u \not\cong^{\pi}_{\top} \Omega_u$. Since the inhabitants of $\mathbb{O}_s$ do not differ between (considering processes modulo) $\cong^{\pi}_{s}$ and $\cong^{\pi}_{\top}$, we know $[\![M]\!]_u \not\cong^{\pi}_{s} \Omega_u$ implies $[\![M]\!]_u \not\cong^{\pi}_{\top} \Omega_u$. This proves adequacy.

(iii) (soundness) The proof is standard, using (ii).

G Proofs for Section 4

G.1 Proposition 4.1

We first prove, in $\pi^{\mathsf{LA}\mu}$:

(i) (subject reduction) *Let* $\Gamma \vdash P \triangleright A$. *Then* $P \twoheadrightarrow P'$ *implies* $\Gamma \vdash P' \triangleright A$.

We note the conditions for action types in the original version (§4.1 "Action Types" and App. C) are not strong enough for (iii) of the same proposition (liveness at linear channels) so that we use strengthened conditions, listed in the updated version (dated July 30).

For the proof, we follow the same routine as given in Appendix A.1 in the long version of [49]. What corresponds to Lemma A.1 of [49] (well-definedness of operators) is easy. A basic lemma follows, which corresponds to Lemma A.2 in [49].

Lemma G.1 *Fix* Γ. *Let* A_1, A_2, A_3, A *and* B *be action types. Then we have:*

- (i) (commutativity) *Assume* $A_1 \asymp A_2$. *Then we have* $A_2 \asymp A_1$ *and* $A_1 \odot A_2 = A_2 \odot A_1$.
- (ii) (associativity) *Assume* $A_1 \asymp A_2$ *and* $(A_1 \odot A_2) \asymp A_3$. *Then we have:* (1) $A_1 \asymp A_3$ *and* $A_2 \asymp A_3$, (2) $A_1 \asymp (A_2 \odot A_3)$ *and* (3) $(A_1 \odot A_2) \odot A_3 = A_1 \odot (A_2 \odot A_3)$.
- (iii) *If* $px \in |A|$ *and* $p \in \mathcal{M}_{\mathbf{!}_{\mathrm{L}},\downarrow_{\mathrm{L}}}$ *then there is no* $qy \in |A|$ *such that* $qy \to px$.
- (iv) *If* $A \asymp B$ *with* $A/\vec{x} = A_0$, $p_ix_i \in |A|$, $p_i \in \mathcal{M}_{\mathbf{!},\downarrow,\perp}$, *and* $\mathsf{fn}(B) \cap \{\vec{x}\} = \emptyset$, *then* $A_0 \asymp B$ *and* $(A \odot B)/\vec{x} = A_0 \odot B$.
- (v) *If* $A \asymp B$ *with* $A/\vec{x} = A_0$, $px_i \in |A|$, $p \in \mathcal{M}_{\mathbf{!},\downarrow}$, *and* $B/\vec{x} = B_0$, *then* $A_0 \asymp B$, $A \asymp B_0$, $A_0 \asymp B_0$, *and* $(A \odot B)/\vec{x} = A_0 \odot B_0$.
- (vi) $?B \asymp ?B$ *and* $B \odot B = B$.

PROOF: (i,ii) are immediate by the definition of permissibility. (iii) is obvious since there is no edge to inputs and $\perp$. Note that, for (iv), we require the side condition $\mathsf{md}(x_i) \in \mathcal{M}_{\mathbf{!},\downarrow,\perp}$, since if we delete an active output at x_i, then $(A \odot B)/\vec{x}$ may be undefined: for example, suppose $A = \mathbf{?}_{\mathrm{L}\mu}y \to \mathbf{?}_{\mathrm{L}\mu}x$ and $B = \mathbf{!}_{\mathrm{L}}z \to \mathbf{?}_{\mathrm{L}\mu}y$. then $A \asymp B$, and A/x and B/x are defined, but $(A \odot B)/x$ is not defined since $A \odot B = \mathbf{!}_{\mathrm{L}}z \to \mathbf{?}_{\mathrm{L}\mu}y \to \mathbf{?}_{\mathrm{L}\mu}x$ where x is not active at all. Similarly for (iv). However if p_ix_i is either input or $\perp$ in $A \odot B$, then by (iii), we can easily prove (iv) and (v). (vi) is obvious by $\mathbf{?}_{\mathrm{L}} \odot \mathbf{?}_{\mathrm{L}} = \mathbf{?}_{\mathrm{L}}$, etc. ■

Since we have to consider the height preservation between immutable channels, we need the following lemma.

Lemma G.2 *Fix* Γ. *Let us assume* A *and* B *are action types. Suppose*

- $A/\vec{x} = A_0$, $B/\vec{x} = B_0$ *and* $A_0 \asymp B_0$.
- $p_ix_i \in |A|$, $p_i'x_i \in |B|$ *with* $p_i \asymp p_i'$, *and* $p_i \in \mathcal{M}_{\mathbf{!},\downarrow}$.

Then $A \asymp B$ *and* $(A \odot B)/\vec{x} = A_0 \odot B_0$.

PROOF: The only difficult case is $p \in \{\mathbf{!}_{\mathrm{L}}, \mathbf{!}_{\mathrm{L}\mu}\}$; other cases were already proved in [7, 49]. W.o.l.g. we only have to prove either case, $A = \mathbf{!}_{\mathrm{L}}x \to \mathbf{?}_{\mathrm{L}\mu}\mathbf{?}_{\mathrm{L}}A_0$ or $A = \mathbf{!}_{\mathrm{L}\mu}x \to \mathbf{?}_{\mathrm{L}\mu}\mathbf{?}_{\mathrm{L}}A_0$. Note that if there is no $\mathbf{?}_{\mathrm{L}\mu}w \to^+ px$ in B, it is just proved as in [49].

Suppose $A = \mathbf{!}_{\mathrm{L}\mu}x \to A_0$ and there exists w such that $\mathbf{?}_{\mathrm{L}\mu}w \to^+ px$ in B. We have to prove $w \notin \mathsf{fn}(A_0)$ (since if $w \in \mathsf{fn}(A_0)$, then there is a vicious circle between x and w). Assume, by a contradiction, there is w such that $w \in \mathsf{fn}(A_0)$ and $\mathbf{?}_{\mathrm{L}\mu}w \to^+ px$ in B. By $\mathbf{?}_{\mathrm{L}\mu}w \to^+ px$, we know $\mathsf{ht}(\Gamma(w)) \gneq \mathsf{ht}(\Gamma(x))$. However, since w is mutable under Γ and $A = \mathbf{!}_{\mathrm{L}\mu}x \to A_0$, if $w \in \mathsf{fn}(A_0)$, then we have $\mathsf{ht}(\Gamma(x)) \geq \mathsf{ht}(\Gamma(w))$. This contradicts to $\mathsf{ht}(\Gamma(w)) \gneq \mathsf{ht}(\Gamma(x))$. ■

Lemma G.3 (i) $\Gamma \vdash P \triangleright A$ *and* $P \equiv Q$ *then* $\Gamma \vdash Q \triangleright A$.

- (ii) $\Gamma \vdash x(\vec{y}).P \mid \overline{x}(\vec{y})Q \triangleright A$ *implies* $\Gamma \vdash (\boldsymbol{\nu}\,\vec{y})(P \mid Q) \triangleright A$. *Similarly for selection.*
- (iii) $\Gamma \vdash !x(\vec{y}).P \mid \overline{x}(\vec{y})Q \triangleright A$ *implies* $\Gamma \vdash !x(\vec{y}).P \mid (\boldsymbol{\nu}\,\vec{y})(P \mid Q) \triangleright A$. *Similarly for selection.*
- (iv) $\Gamma \vdash \mathsf{ref}\langle xy\rangle \mid \overline{x}\mathtt{inl}(c)P \triangleright A$ *implies* $\Gamma \vdash \mathsf{ref}\langle xy\rangle \mid (\boldsymbol{\nu}\, c)(P \mid \overline{c}\langle y\rangle^{\tau}) \triangleright A$
- (v) $\Gamma \vdash \mathsf{ref}\langle xy\rangle \mid \overline{x}\mathtt{inr}(wc)P \triangleright A$ *implies* $\Gamma \vdash (\boldsymbol{\nu}\, wc)(\mathsf{ref}\langle xw\rangle \mid P \mid \overline{c}) \triangleright A$.

PROOF: For (i), we can use the same reasoning as the proof of (i) in Lemma A.3 in [49]; For example, in the structural rule

$$(\overline{x}(\vec{y})P) \mid Q \;\equiv\; \overline{x}(\vec{y})(P|Q) \quad \text{with } y_i \notin \mathsf{fn}(Q)$$

y_i's mode should be $\mathcal{M}_{\mathbf{!}}$ because of **(C1)** in § 2.3. Also in the structure rule

$$(\boldsymbol{\nu}\,\vec{y})P \mid Q \;\equiv\; (\boldsymbol{\nu}\,\vec{y})(P \mid Q) \quad \text{with } y_i \notin \mathsf{fn}(Q)$$

y_i's mode should be $\mathcal{M}_{\mathbf{!},\perp}$ because of the definition of (Res). Hence we can use (iv) and (v) of the above lemma as in [49]. Similarly we can directly use (v,vi,vii) of the above lemma to prove (ii) and (iii) as in [49]. Hence we only prove (iv) and (v). (v) is non-trivial because the side effect to the action type occurs when $\mathsf{ref}\langle xv\rangle$ changes to $\mathsf{ref}\langle xw\rangle$.

(iv): We have two cases.

Immutable read: Assume $\Gamma \vdash \mathsf{ref}\langle xy\rangle \mid \overline{x}\mathtt{inl}(c)P \triangleright A$. Suppose $\mathsf{ref}\langle xy\rangle^\tau$ is inferred by $(\mathsf{Ref}^{!_\mathrm{L}})$, i.e.

$$\Gamma \vdash \mathsf{ref}\langle xy\rangle^\tau \triangleright\ !_{\mathrm{L}\mu}x \to ?_{\mathrm{L}}y \tag{1}$$

with

a. $\Gamma \vdash x : [(\tau)^{\uparrow_\mathrm{L}} \& \overline{\tau}()^{\uparrow_\mathrm{L}}]^{!_\mathrm{L}, !_{\mathrm{L}\mu}}$ and

b. $\Gamma \vdash y : \overline{\tau}$ with $\mathsf{md}(\tau) = !_\mathrm{L}$.

By (i) of this lemma, we can assume $\overline{x}\mathtt{inl}(c)P$ is prime, cf. Appendix B.3 in [49]. Hence we can write $P \equiv c(y').Q$ or $P \equiv c[\&y_i'.Q_i]$. Both are proved by the same reasoning, so we set $P \equiv c(y').Q$. By assumption, we have:

$$\Gamma \vdash \overline{x}\mathtt{inl}(c)P \triangleright (?_{\mathrm{L}\mu}x \to ?_\mathrm{L}?_{\mathrm{L}\mu}B^{-x}) \otimes \uparrow_\mathrm{L}C \otimes ?_\mathrm{A}\uparrow_\mathrm{A}D \tag{2}$$

with

a. $\Gamma \cdot c : (\overline{\tau})^{\downarrow_\mathrm{L}} \vdash c(y').Q \triangleright B \otimes (\downarrow_\mathrm{L}c \to \uparrow_\mathrm{L}C) \otimes D$

b. $(?_{\mathrm{L}\mu}x \otimes B) \asymp (!_{\mathrm{L}\mu}x \to ?_\mathrm{L}y)$ and $(?_{\mathrm{L}\mu}x \otimes B) \odot (!_{\mathrm{L}\mu}x \to ?_\mathrm{L}y) = B' \otimes (!_{\mathrm{L}\mu}x \to ?_\mathrm{L}y)$ with $B = B' \otimes ?_\mathrm{L}y$ or $B = B'^{-y}$ with $A = B' \otimes (!_{\mathrm{L}\mu}x \to ?_\mathrm{L}y) \otimes C \otimes D$. (note that y is not mutable, hence there is no z such that $?_\mathrm{L}y \to^+ pz$).

We also have, by (1-b),

$$\Gamma \cdot c : (\tau)^{\uparrow_\mathrm{L}} \vdash \overline{c}\langle y\rangle^\tau \triangleright \uparrow_\mathrm{L}c \otimes ?_\mathrm{L}y \tag{3}$$

By $(\downarrow_\mathrm{L}c \to \uparrow_\mathrm{L}C) \asymp \uparrow_\mathrm{L}c$ and $B \asymp ?_\mathrm{L}y$, we have

$$(B \otimes (\downarrow_\mathrm{L}c \to \uparrow_\mathrm{L}C) \otimes D) \asymp (\uparrow_\mathrm{L}c \otimes ?_\mathrm{L}y)$$

hence we get

$$\begin{aligned}&(B \otimes (\downarrow_\mathrm{L}c \to \uparrow_\mathrm{L}C) \otimes D) \odot (\uparrow_\mathrm{L}c \otimes ?_\mathrm{L}y)\\ &= (B \odot ?_\mathrm{L}y) \otimes C \otimes D \otimes \bot c\end{aligned}$$

Hence by weakening, together with (Res), we have

$$\Gamma \vdash (\boldsymbol{\nu}\, c)(c(w).Q \mid \overline{c}\langle y\rangle^\tau) \triangleright (B \odot ?_\mathrm{L}y) \otimes C \otimes D \tag{4}$$

Now we know $(B \odot ?_\mathrm{L}y) \odot (!_{\mathrm{L}\mu}x \to ?_\mathrm{L}y) = B' \otimes (!_{\mathrm{L}\mu}x \to ?_\mathrm{L}y)$ by (2-b). Hence by (1) and (4), we are done.

Mutable read: Since y is mutable, we need to modify (2-b). The case $y \notin \mathsf{fn}(B)$ is as the same as the above. Suppose B includes $?_{\mathrm{L}\mu}y \to B_i$ as its sub-graph. Then we have:

$$\begin{aligned}&(?_{\mathrm{L}\mu}x \otimes B) \odot (!_{\mathrm{L}\mu}x \to ?_{\mathrm{L}\mu}y)\\ &= (B \odot (?_{\mathrm{L}\mu}x \odot (!_{\mathrm{L}\mu}x \to ?_{\mathrm{L}\mu}y))\\ &= (B \odot (!_{\mathrm{L}\mu}x \to ?_{\mathrm{L}\mu}y))\end{aligned}$$

On the other hand, we always have $B \asymp (!_{\mathrm{L}\mu}x \to ?_{\mathrm{L}\mu}y)$ since for all $z \in \mathsf{fn}(B_i)$, we have $\mathsf{ht}(\Gamma(y)) \gneq \mathsf{ht}(\Gamma(z))$, and by $!_{\mathrm{L}\mu}x \to ?_{\mathrm{L}\mu}y$, we have $\mathsf{ht}(\Gamma(x)) \geq \mathsf{ht}(\Gamma(y))$. Hence $\mathsf{ht}(\Gamma(x)) \gneq \mathsf{ht}(\Gamma(z))$ by transitivity. Thus:

$$\begin{aligned}&(B \odot ?_{\mathrm{L}\mu}y) \odot (!_{\mathrm{L}\mu}x \to ?_{\mathrm{L}\mu}y)\\ &= (B \odot (?_{\mathrm{L}\mu}y \odot (!_{\mathrm{L}\mu}x \to ?_{\mathrm{L}\mu}y))\\ &= B \odot (!_{\mathrm{L}\mu}x \to ?_{\mathrm{L}\mu}y)\end{aligned}$$

The rest of reasoning is just the same as the above.

(v): Suppose $\mathsf{ref}\langle xy\rangle^\tau$ is inferred by $(\mathsf{Ref}^{!_\mathrm{L}})$. The case $(\mathsf{Ref}^{!_{\mathrm{L}\mu}})$ is just the same because the right branch is the same in the both rules. As in Example 2.1 [49], in the following, we often write down action types syntactically by duplicating shared $?_\mathrm{L}/?_{\mathrm{L}\mu}$-nodes. Suppose (1) and $\Gamma \vdash \mathsf{ref}\langle xy\rangle \mid \overline{x}\mathtt{inr}(wc)P \triangleright A$. W.o.l.g. we assume $P \equiv (!w(y').Q \mid c.R)$ and

$$\Gamma \vdash \overline{x}\mathtt{inr}(wc)P \triangleright (?_{\mathrm{L}\mu}x \to B) \otimes \uparrow_\mathrm{L}C \otimes D \tag{5}$$

with

a. $\Gamma \cdot w : \tau \cdot c : ()^{\downarrow_\mathrm{L}} \vdash !w(y').Q \mid c.R \triangleright (!_\mathrm{L}w \to B) \otimes (\downarrow_\mathrm{L}c \to C) \otimes D$ and

b. $(?_{\mathrm{L}\mu}x \to B) \otimes \uparrow_\mathrm{L}C \otimes D \asymp (!_{\mathrm{L}\mu}x \to ?_{\mathrm{L}\mu}y)$.

Note that $x, w \notin \mathsf{fn}(B)$. First, we have

$$\Gamma \cdot c : ()^{\uparrow_\mathrm{L}} \vdash \overline{c} \triangleright \uparrow_\mathrm{L}c \tag{6}$$

Hence we have

$$\Gamma \cdot w : \tau \vdash (\boldsymbol{\nu}\, c)(!w(y').Q \mid c.R \wp \overline{c}) \triangleright (!_\mathrm{L}w \to B) \otimes C \otimes D \tag{7}$$

Now we compose the above with $\mathsf{ref}\langle xw\rangle$ which has a type $!_{\mathrm{L}\mu}x \to ?_\mathrm{L}w$. We have to show $(!_\mathrm{L}w \to B) \asymp (!_{\mathrm{L}\mu}x \to ?_\mathrm{L}w)$ with preserving the height condition. This is easy by transitivity of $\geq$ just as the above case (note by $x \notin \mathsf{fn}(B)$, there is no vicious circle between x and w). Then $(!_\mathrm{L}w \to B) \odot (!_{\mathrm{L}\mu}x \to ?_\mathrm{L}w) = (!_\mathrm{L}w \to B) \otimes (!_{\mathrm{L}\mu}x \to B) = B'$ and $B'/w = B \odot (!_{\mathrm{L}\mu}x \to B) = (!_{\mathrm{L}\mu}x \to B)$. Hence we have $\Gamma \vdash (\boldsymbol{\nu}\, wc)(\mathsf{ref}\langle xw\rangle \mid P \mid \overline{c}) \triangleright (!_{\mathrm{L}\mu}x \to B) \otimes C \otimes D$.

Now we have two cases.

- If $y \in \mathsf{fn}(B)$, then $A = (!_{\mathrm{L}\mu}x \to B) \otimes C \otimes D$.
- If $y \notin \mathsf{fn}(B)$, we can apply (Weak) when we infer Q above, i.e. just before the inference of (5-a). Hence we have $A = (!_{\mathrm{L}\mu}x \to (B \otimes ?_\mathrm{L}y)) \otimes C \otimes D$, as required. ■

(ii) of Proposition 4.1 is easy syntactic analysis. **(iii)** is as in (iii) of § 2.4, where the linear action lemma for stateful linear processes is proved using the partial order on names at replicated channels as given in [49] for the standard reduction instead of the extended reduction.

G.2 Proposition 4.4

(non-interference in $\pi_{\mathrm{sec}}^{\mathsf{LA}\mu}$) *Let* $\Gamma \vdash_{\mathrm{sec}} P_{1,2} \triangleright A$ *such that* $\mathsf{tamp}_\Gamma(A) = s$. *Then* $s \not\sqsubseteq s'$ *implies* $\Gamma \vdash_{\mathrm{sec}} P_1 \cong_{s'}^{\pi} P_2$.

The proof uses the extension of $\approx_s$ in $\pi_{\mathrm{sec}}^{\mathsf{LA}}$ to $\pi_{\mathrm{sec}}^{\mathsf{LA}\mu}$, which is defined by the same definition using the entries on $!_{\mathrm{L}\mu}$ and $?_{\mathrm{L}\mu}$ in Figure 14 in addition. The congruence of $\approx_s$ relies on both the linear action lemma and the structural secrecy. The relation for noninterference is given precisely as for $\pi_{\mathrm{sec}}^{\mathsf{LA}}$. The reasoning for its bisimilarity is again identical.

H Proofs for Section 5

H.1 Proposition 5.2

The proof is by mechanical induction, proving a slightly stronger statement:

> $E \vdash c : \rho$ *implies* $E^\circ \cdot u : \rho^\circ \vdash_{\mathrm{sec}} [\![c]\!]_u^E \triangleright A$ *such that* (1) *edges in* A *are always of form* $?_{\mathrm{L}\mu}x \to py$ *where* $E(x) \gneq E(y)$, *and* (2) $|A| = \langle\rho\rangle_u$.

Some cases are of interest which we list below. We note a side condition on heights of types is lacking from the original version of *[Lam]*, which is added in the updated version (dated July 30). The new version also slightly relaxed the side condition, again on heights of types, of *[Lam-∗]*.

[Seq]. By assumption, we know $E^\circ \cdot u : ()^p \vdash_{\mathrm{sec}} [\![c_i]\!]_u \triangleright pu \otimes A_i$ such that $|A_i| = X_i^\star$ with $p \in \{\uparrow_{\mathrm{L}}, \uparrow_{\mathrm{A}}\}$. First assume $\tau = \Downarrow$, so that $p = \uparrow_{\mathrm{L}}$. We observe: (1) we can prefix $[\![c_2]\!]_u$ by a unary linear input regardless of its secrecy level, since it does not receive; and (2) $A_1 \asymp A_2$ since, by (IH), edges follow the height of types. Thus by (In) and (Par) we infer:

$$E^\circ \cdot u : ()^{\uparrow_{\mathrm{L}}} \vdash_{\mathrm{sec}} (\boldsymbol{\nu}\, e)([\![c_1]\!]_e | e.[\![c_2]\!]_u) \triangleright \uparrow_{\mathrm{L}} u \otimes (A_1 \odot A_2)$$

as required. If on the other hand $\tau = \Uparrow$, then $p = \uparrow_{\mathrm{A}}$. By the side condition and by noting $\mathsf{tamp}_E(X_2) = \mathsf{tamp}_{E^\circ}(A_2)$, we have $\mathsf{tamp}_{E^\circ \cdot u:()^{\uparrow_{\mathrm{A}}}_{s_2}}(\uparrow_{\mathrm{A}} u \otimes A_2) \geq s_1$. Thus the following is well-typed:

$$E^\circ \cdot u : ()^{\uparrow_{\mathrm{A}}}_{s_2} \cdot e : ()^{\downarrow_{\mathrm{A}}}_{s_1} \vdash_{\mathrm{sec}} e.[\![c_2]\!]_u \triangleright \uparrow_{\mathrm{A}} u \otimes \downarrow_{\mathrm{A}} e \otimes A_2$$

Hence by (Par) we are done.

[Sub]. The only non-trivial case is when we replace $\Downarrow_s$ with $\Uparrow_s$, which we show by induction. The base cases ($c \stackrel{\mathrm{def}}{=} \mathtt{skip}$ and $c \stackrel{\mathrm{def}}{=} x := v$) are trivial. For induction, for $[\![c_1; c_2]\!]_u$ we note $[\![c_1]\!]_e$ outputs at e linearly, similarly for $[\![\mathtt{if}\ x\ \mathtt{then}\ c_1\ \mathtt{else}\ c_2]\!]_u$. Other cases are direct from the induction hypothesis.

[Deref]. We show the case when T is mutable (the reasoning when T is immutable is easier). Assume $E \vdash z : \mathtt{ref}_s(T), X$ and $E \cdot x : T \vdash c : \mathrm{cmd}\, \tau_{s_0}\, Y$ with T mutable. By induction hypothesis, we have, with $p \in \{\uparrow_{\mathrm{L}}, \uparrow_{\mathrm{A}}\}$,

$$E^\circ \cdot x : \overline{T^\circ} \cdot u : ()^p_{s_0} \vdash_{\mathrm{sec}} [\![c]\!]_u \triangleright pu \otimes A$$

such that $|A| = Y^\circ$. Note $\mathtt{ref}_s(T)^\circ = [(T^\circ)^{\uparrow_{\mathrm{L}}} \& \overline{T^\circ}()^{\uparrow_{\mathrm{L}}}]^{!_{\mathrm{L}\mu}, !_{\mathrm{L}\mu}}$ since T is mutable. Hence we have, by setting the above type as τ,

$$E^\circ \cdot z : \tau \cdot u : ()^p_{s_0} \vdash_{\mathrm{sec}} \overline{z}\mathtt{inl}(c)c(x).[\![c]\!]_u \triangleright pu \otimes ?_{\mathrm{L}\mu} z \otimes A.$$

Note we need neither a prefixing nor the constraint on the height of types since the prefixing at c is linear, not replicated. Finally noting $|pu \otimes (?_{\mathrm{L}\mu} z \to A)| = pu \otimes ?_{\mathrm{L}\mu} z \otimes |A| = \mathtt{w}z \cdot X$ we are done.

[Id]. Let $T \leq T'$. First assume T is not mutable. Then $\mathsf{md}(T^\circ) = !_{\mathrm{L}}$. Thus we have:

$$E^\circ \cdot x : \overline{T^\circ} \cdot c : T^\circ \vdash_{\mathrm{sec}} [c \to x] \triangleright !_{\mathrm{L}} c \to ?_{\mathrm{L}} x$$

We can now use $u : T'^\bullet \vdash_{\geq} u : T^\bullet$ to infer:

$$E^\circ \cdot x : \overline{T^\circ} \cdot u : T'^\bullet \vdash_{\mathrm{sec}} \overline{u}(c)[c \to x] \triangleright \uparrow_{\mathrm{L}} u \otimes ?_{\mathrm{L}} x$$

By using (Weak) as needed, we reach the required form. Similarly for the case when T is mutable, except for, by $\mathsf{md}(T^\circ) = !_{\mathrm{L}\mu}$, changing $?_{\mathrm{L}} x$ to $?_{\mathrm{L}\mu} x$.

[Lam-∗]. Let $E \cdot x : T \vdash e : T', X$. By (IH), we have $E^\circ \cdot x : T^\circ \cdot u : T'^\bullet \vdash_{\mathrm{sec}} [\![e]\!]_u \triangleright \uparrow_{\mathrm{L}} u \otimes A$ such that $|A| = X^\circ$. By the condition $s \sqsubseteq \mathsf{tamp}_E(X/x)$ we know $s \sqsubseteq \mathsf{tamp}_{E^\circ}(A/x)$ hence we have, noting the condition on the height of types is satisfied by the side condition when prefixing at c:

$$E^\circ \cdot u : (T \stackrel{*}{\Rightarrow}_s T')^\bullet \vdash_{\mathrm{sec}} \overline{u}(c) !c(xm).\langle e \rangle_m \triangleright \uparrow_{\mathrm{L}} u \otimes A/x,$$

as required.