# Type-based information flow analysis for $\pi$-calculus with a dynamically extensible security lattice

Yukihiro Oda
*Graduate School of Information Sciences*
*Tohoku University*
*Tohoku, Japan*
*yukihiro.oda.e5 [at] tohoku.ac.jp*
*ORCID:0000-0002-6216-3193*

Eijiro Sumii
*Graduate School of Information Sciences*
*Tohoku University*
*Tohoku, Japan*
*sumii [at] tohoku.ac.jp*

***Abstract*—We develop a type system for secure information flow where new security levels can be created and inserted into the security lattice *dynamically*, i.e., even in the middle of an execution of a system. Our system is formalized by extending Kobayashi's type-based secure information flow analysis for Milner's pi-calculus, which is one of the most expressive models (or "languages") supporting both sequential and concurrent computations, with concise syntax, reduction-based semantics, and bisimulation equivalence as a robust formalization of secrecy as non-interference. The development required careful treatment of extensions of lattices themselves as well as deliberate generalization from the simple 2-element lattice (consisting of only High and Low) in the original system.**

***Index Terms*—language-based security, pi-calculus, barbed bisimulation, non-interference, dynamic extension of security lattice, runtime creation and insertion of new security levels**

## 1. Introduction

Lattice-based secure information flow [1] classifies data into security levels—such as H(igh) and L(ow)—that are elements of the security lattice, and aims to prevent leakage of higher-level information into lower-level actors. Unlike mere access control, secure information flow also addresses indirect information leakage—like $\texttt{if}\ b^{\mathtt{H}}\ \texttt{then}\ 1^{\mathtt{L}}\ \texttt{else}\ 0^{\mathtt{L}}$ where $b^{\mathtt{H}}$ is a high-level Boolean value and $1^{\mathtt{L}}$, $0^{\mathtt{L}}$ are low-level integers—and even $\texttt{if}\ b^{\mathtt{H}}\ \texttt{then}\ 1^{\mathtt{L}}\ \texttt{else}\ \mathit{diverge}()$ when termination-sensitive. Absence of information leakage is formalized as non-interference [2], which asserts the equivalence of two systems with different high-level information when observed from a low level.

To account for such indirect information flows, language-based—and, more specifically, type-based—information flow analysis [3], [4] models systems as programs and adopts a static type system that imposes the classification by annotating types with security levels. Though called "language-based" with "programs," this approach is not limited to programs or programming languages in the narrow sense (such as C and Java), but is applicable to various models of systems as well. Traditionally, the "languages" (or models) have been imperative [3] or functional [5], and sequential. They have also been extended with (mainly thread-based) concurrency, where determinism has often been essential and non-interference has been proved in probabilistic settings or under a strong restriction on the concurrent computations—for instance, no low-level communication is allowed after high-level synchronization, or observable non-determinism is forbidden at all; see [4, Section IV-B] for a survey.

Kobayashi [6] removed such strong restrictions by adopting a type system for lock-freedom [7] in $\pi$-calculus [8]–[10], a rather general and expressive model of both sequential and concurrent computations. In short, even high-level synchronization is allowed before low-level communications as long as the former is lock-free. Non-interference is proved as (barbed [11]) bisimulation-based congruence, which is also a general and robust notion of equivalence (and can be extended with probability; see, for instance, [12]–[15], among many others).[1] However, Kobayashi [6] only considered the security lattice with 2 elements (high and low).

In the present work, we extend Kobayashi [6] with general security lattices. Furthermore, we allow *dynamic* extension of the lattice, that is, new security levels can be added *while* the system is running, which is a mandatory functionality for many modern systems that allow registration/creation of new users/accounts.

1. Equivalence (and therefore non-interference) of concurrent processes with general interactions (as opposed to "threads" with limited concurrency primitives) has by itself been a significant research challenge, e.g. classically [16], [17] and more recently [18], just to name a few. While no single definition of equivalence may be considered satisfactory in every respect, barbed bisimulation is "fine" (as opposed to coarse) and *sufficient* as a proof of *soundness* of a security type system.

Even the former generaliztion by itself is non-trivial—all the definitions, statements, and proofs need to be carefully parameterized with the level $l$ of the attacker (namely, observer for the equivalence) being considered (Definition 3.13, Definition 3.14, Definition 4.11, and so forth). The latter extension is, to the best of our knowledge, new, even for sequential languages. It also requires careful treatment of the "current" security lattice of the system, throughout our technical developments such as reduction (Definition 2.6) and typing rules (Figure 1), as well as the definition of a "safe" extension of a lattice itself (Definition 2.5) and all the proofs (in the Appendices).

The rest of this paper is as follows: Section 2 introduces the syntax and reduction semantics of our language along with definitions concerning the security lattices. Section 3 defines our type system for information flow analysis. Section 4 proves the non-interference theorem and Section 5 concludes. Further details of our technical developments and proofs are given in the Appendices.

## 2. $\pi^L$-calculus

This section introduces our process calculus $\pi^L$ for type-based information flow analysis, which extends the $\pi$-calculus [8]–[10] with a lattice of secrecy levels.

### 2.1. Syntax

Our language is $\pi$-calculus [6], [8]–[10] augmented with a $\nu$ operation for extending the lattice of secrecy levels, as in the definition below. Intuitively, the new process form $(l_1, \ldots, l_m < \nu l < l'_1, \ldots, l'_n)P$ creates a new level $l$ above (resp. below) existing levels $l_1, \ldots, l_m$ (resp. $l'_1, \ldots, l'_n$), and then execute $P$. (Its formal semantics will be defined in the next sections.)

In the rest of this paper, we often write $\tilde{l}$, $\tilde{x}$, etc. to abbreviate sequences like $l_1, \ldots, l_m$ and $x_1, \ldots, x_n$ when their lengths $m, n \geq 0$ are arbitrary or clear from the context. For a sequence $\tilde{t}$ where $t$ is a meta-variable of any kind, we write $a \in \tilde{t}$ if $a$ is an element of $\tilde{t}$.

We write $\mathsf{Chan}$ and $\mathsf{SecLev}$ for the distinct sets of *channel names* and *secrecy level names*, respectively. Also, we assume at least two distinct secrecy level names $\top, \bot \in \mathsf{SecLev}$.

**Definition 2.1** (Syntax of $\pi^L$-calculus)**.** We define *processes* as follows

$$
\begin{array}{rll}
x, y, \ldots \in \mathsf{Chan} & & \text{(channel name)} \\
k, l, m \in \mathsf{SecLev} & & \text{(secrecy level name)} \\
c & ::= \mathrm{true}^l \mid \mathrm{false}^l \mid \mathrm{unit} & \text{(constant value)} \\
v & ::= c \mid x & \text{(value)} \\
P & ::= 0 \mid (P \mid P) \mid *P \mid (\nu x : \xi)P \mid & \text{(process)} \\
 & \quad x!\tilde{v}.P \mid x?\tilde{x}.P \mid \left(\tilde{l} < \nu l < \tilde{l}\right)P \mid & \\
 & \quad \mathtt{if}\ v\ \mathtt{then}\ P\ \mathtt{else}\ P &
\end{array}
$$

where $\xi$ ranges over the core channel types (defined later in Definition 3.1).

By convention, we give a lower precedence to $\mid$ than to other operators, so $(\nu x : \xi)P_1 \mid P_2$ means $((\nu x : \xi)P_1) \mid P_2$ for example. We also assume $\mid$ is left-associative.

As usual, every $y_i \in \tilde{y}$ in $x?\tilde{y}.P$, $x$ in $(\nu x : \xi)P$, and, in particular, $l$ in $\left(\tilde{l_1} < \nu l < \tilde{l_2}\right)P$ are *bound* in $P$ and subject to implicit $\alpha$-conversion such that each of them is different from other (bound or unbound) names. We write $\mathrm{FN}(P)$, $\mathrm{FCN}(P)$, and $\mathrm{FSN}(P)$, respectively, for the set of free (i.e., unbound) names, free channel names, and free secrecy level names of process $P$. A *sub-process* of a process $P$ is defined as a subexpression of $P$ that is also a process. We write $\mathscr{P}$ for the set of processes.

We write $P[y_0 \mapsto v_0, \ldots, y_n \mapsto v_n]$ for the process obtained by respectively replacing all the free occurrences of $y_0, \ldots, y_n$ in $P$ with $v_0, \ldots, v_n$. We often abbreviate $P[y_0 \mapsto v_0, \ldots, y_n \mapsto v_n]$ as $P[\tilde{y} \mapsto \tilde{v}]$ and $(\nu x_0 : \xi_0) \ldots (\nu x_n : \xi_n)P$ as $\left(\nu \tilde{x} : \tilde{\xi}\right)P$.

### 2.2. Lattice of secrecy levels

In this section, we give definitions and prove lemmas for the lattice of secrecy levels.

**Definition 2.2** (Lattice)**.** We define a lattice as a poset $(L, \leq_L)$ where, for any finite $S \subseteq L$, there exist the supremum and infimum of $S$.

Note that the supremum of $\emptyset$ is the minimum of $(L, \leq_L)$, and the infimum of $\emptyset$ is the maximum of $(L, \leq_L)$. Thus, for each lattice, its maximum and minimum exist.[2] We sometimes write $1_L$ and $0_L$ for the maximum and minimum of $(L, \leq_L)$, respectively. For simplicity, we often write just $L$ for a lattice $(L, \leq_L)$. For $(L, \leq_L)$ and $a, b \in L$, we write $a <_L b$ if $a \leq_L b$ and $a \neq b$. We also write $a \not\leq_L b$ (resp. $a \not<_L b$) when $a \leq_L b$ (resp. $a <_L b$) does not hold. For $S \subseteq L$, we write $\sup_L(S)$ and $\inf_L(S)$ for the supremum and infimum of $S$ in $L$, respectively. Note also $a \leq_L b \iff \sup_L(\{a, b\}) = b \iff \inf_L(\{a, b\}) = a$.

The following definition is crucial for "safe" extension of a lattice, as we will adopt in the rest of this paper. In short, an extension $L$ of a lattice $L'$ must be a "superlattice" of $L'$, that is, $L'$ must be a sublattice of $L$.

**Definition 2.3** (Sublattice)**.** For a lattice $(L, \leq_L)$, we define a sublattice of $(L, \leq_L)$ as a lattice $(L', \leq_{L'})$ satisfying the following conditions:

(1) $L' \subseteq L$
(2) $1_L, 0_L \in L'$

2. We adopt the present definition as in [19] and [20, p. 3, Remark]; the latter explains why it is more "natural." An alternative term for this definition is a *bounded lattice* [19, Section 2], which we avoid for brevity in this paper.

(3) $\sup_{L'}(S) = \sup_L(S)$ and $\inf_{L'}(S) = \inf_L(S)$ for every finite $S \subseteq L'$.

We write $L' \sqsubseteq L$ if $L'$ is a sublattice of $L$.

**Lemma 2.4.** *Let $L$ be a lattice and $L' \sqsubseteq L$. For any $a, b \in L'$,*
*(1) $a \leq_{L'} b$ if and only if $a \leq_L b$, and*
*(2) $a <_{L'} b$ if and only if $a <_L b$.*

We omit proofs when they are straightforward.

A *lattice of secrecy levels* is a lattice such that its underlying set is a finite subset of $\mathsf{SecLev}$, with $\top$ and $\bot$ being the maximum and minimum, respectively. We write $\mathscr{L}$ for the set of lattices of secrecy levels. We also write $\tilde{l} \subseteq L$ if every $l_i \in \tilde{l}$ belongs to $L$.

We then give a notation $\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$ for extension of lattices:[3]

**Definition 2.5.** Let $(L, \leq_L)$ be a lattice of secrecy levels with $\tilde{l_0}, \tilde{l_1} \subseteq L$, and $l \notin L$ for an $l \in \mathsf{SecLev}$. Let furthermore $L' = L \cup \{l\}$ and $\leq_{L'}$ be the reflexive and transitive closure of $\leq_L \cup \left\{(l', l) \;\middle|\; l' \in \tilde{l_0}\right\} \cup \left\{(l, l') \;\middle|\; l' \in \tilde{l_1}\right\}$. If $(L', \leq_{L'})$ is a lattice, then we write $\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$ for $L'$.

Note that $L'$ may not always be a lattice, e.g., if $L = \{\bot, \top\}$, $\tilde{l_0} = \top$, and $\tilde{l_1} = \bot$. We reject such extensions by definition. Note also that $L'$ may not always be a superlattice of $L$, that is, $L$ may not be a sublattice of $L'$, even if $L'$ is a lattice. Later, we impose $L \sqsubseteq L'$ by typing.

### 2.3. Reduction

This section defines reduction in $\pi^L$-calculus via structural preorder, which is a variant of standard structural congruence in $\pi$-calculus but is asymmetric for the sake of specifying canonical forms.

**Definition 2.6** (Structural preorder)**.** The binary relation $\preceq$ on processes, called *structural preorder*, is defined as the least reflexive and transitive relation satisfying the following rules, where $P_0 \simeq P_1$ denotes that both $P_0 \preceq P_1$ and $P_1 \preceq P_0$ hold.

(SP-Zero1) $P \simeq P \mid \mathsf{0}$
(SP-Zero2) $\mathsf{0} \simeq (\nu x : \xi)\mathsf{0}$
(SP-Commut) $P_0 \mid P_1 \preceq P_1 \mid P_0$
(SP-Assoc) $(P_0 \mid P_1) \mid P_2 \preceq P_0 \mid (P_1 \mid P_2)$ [4]
(SP-New) $(\nu x : \xi)P_0 \mid P_1 \simeq (\nu x : \xi)(P_0 \mid P_1)$ if $x \notin \mathrm{FCN}(P_1)$
(SP-IfT) $\mathtt{if}\ \mathrm{true}^l\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1 \preceq P_0$
(SP-IfF) $\mathtt{if}\ \mathrm{false}^l\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1 \preceq P_1$

3. In fact, *any* extension of a lattice would do for the rest of our development as long as it yields a superlattice and parallel extensions are commutative. We adopt the present definition only for the sake of concreteness.

4. The other direction can be derived from (SP-Commut) and (SP-Par).

(SP-Rep) $*P \preceq *P \mid P$
(SP-Par) If $P_0 \preceq P_1$, then $P_0 \mid Q \preceq P_1 \mid Q$.
(SP-CNew) If $P_0 \preceq P_1$, then $(\nu x : \xi)P_0 \preceq (\nu x : \xi)P_1$.

**Definition 2.7** (Reduction)**.** The binary relation $\longrightarrow$ on $\mathscr{P} \times \mathscr{L}$, called *reduction*, is defined as the least relation satisfying the following rules:

(R-Com) $(x!\tilde{v}.P_0 \mid x?\tilde{y}.P_1, L) \longrightarrow (P_0 \mid P_1[\tilde{y} \mapsto \tilde{v}], L)$
(R-NewLev) If $\tilde{l_0}, \tilde{l_1} \subseteq L$ and $\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$ is defined, then $\left(\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)P, L\right) \longrightarrow \left(P, \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L\right)$.
(R-Par) If $(P_0, L) \longrightarrow (P_0', L')$, then $(P_0 \mid P_1, L) \longrightarrow (P_0' \mid P_1, L')$.
(R-New) If $(P, L) \longrightarrow (P', L')$, then $((\nu x : \xi)P, L) \longrightarrow ((\nu x : \xi)P', L')$.
(R-SP) If $P_0 \preceq P_0'$, $(P_0', L_0) \longrightarrow (P_1', L_1)$, and $P_1' \preceq P_1$, then $(P_0, L_0) \longrightarrow (P_1, L_1)$.

We write $\longrightarrow\!\!\!\!\!\rightarrow$ for the reflexive and transitive closure of $\longrightarrow$. We also write $\longrightarrow\!\!\!\!\!\!\rightarrow$ for the transitive closure of $\longrightarrow$.

## 3. Type System

Our type system is an extension of Kobayashi [6]'s, with a general lattice of secrecy levels and dynamic creation of new levels.

### 3.1. Types and Usages

Before our extension, we basically repeat Kobayashi [6]'s definition of *usages*—originally proposed in [21]—albeit omitting recursion for the sake of technical simplicity (while keeping usage variables for substitutions as in Definition 3.7 (a)). Informally, a usage is part of a channel type and expresses how (when and in what order) the channel is used for input and output, so as to ensure lock-freedom by checking the correctness—called *reliability*—of the usage. The intuitive meanings of usage expressions are briefly summarized in Table 1.

**Definition 3.1.** We define *types* and *usages* as follows:

$$\begin{aligned}
\tau &::= \mathtt{Bool}^l \mid \mathtt{Unit} \mid \xi/U && \text{(type)}\\
\xi &::= \langle\tilde{\tau}\rangle^l && \text{(core channel type)}\\
\rho &\in \mathsf{UVar} && \text{(usage variable)}\\
t_o, t_c &\in \mathbb{N} \cup \{\infty\} && \text{(obligation and capability levels)}\\
U &::= \mathsf{0} \mid \rho \mid \alpha^{t_o}_{t_c}.U \mid (U \mid U) \mid && \text{(usage)}\\
&\quad\ *U \mid \uparrow^{(t_o,t_c)} U \mid U \,\&\, U\\
\alpha &::= I \mid O && \text{(input and output)}
\end{aligned}$$

We write $\mathrm{FV}(U)$ for the set of usage variables occurring in a usage $U$. A usage $U$ is *closed* if no usage variable occurs in $U$. Also, we write $\overline{\alpha}$ for the *co-action* of $\alpha$, defined as $\overline{I} = O$ and $\overline{O} = I$. We define *the type of* $\mathrm{true}^l$ *and* $\mathrm{false}^l$ as $\mathtt{Bool}^l$ and *the type of* unit as $\mathtt{Unit}$.

| Usages | Intuitive meaning (how the channel should be used) |
|---|---|
| $\mathtt{0}$ | cannot be used at all |
| $\alpha^{t_o}_{t_c}.U$ | used once for input ($\alpha = I$) or output ($\alpha = O$), and then used according to $U$, where $t_o$ and $t_c$ are natural numbers (or $\infty$) respectively called *obligation* and *capability* levels (not to be confused with secrecy levels) and represent when (i.e., in what order) the input or output *must* and *can* be performed, so as to prevent deadlocks and livelocks caused by self or cyclic dependencies |
| $U_0 \mid U_1$ | used according to $U_0$ and $U_1$, possibly in parallel (the symbol $\mid$ here represents parallel composition as in $\pi$-calculus) |
| $*U$ | used according to $U$ infinitely many times in parallel |
| $\uparrow^{(t_I,t_O)} U$ | used according to $U$, but input and output obligation levels are raised (at least) to $t_I$ and $t_O$, respectively |
| $U_0 \,\&\, U_1$ | used according to either $U_0$ or $U_1$, as chosen by the "user" (the symbol & here represents additive conjunction as in linear logic [22]) |

TABLE 1. Intuitive meaning of usage expressions (similar to [6, Table 1])

We assume $\mid$ for usages is left-associative as well. We call $\mathtt{Bool}^l$ and $\mathtt{Unit}$ *base types*. A type $\tau$ is called a *channel type* if it is not a base type. *The secrecy level of a type* $\tau$ is defined as $l$ if $\tau$ is either $\mathtt{Bool}^l$ or of the form $\langle \tilde{\tau} \rangle^l / U$.

For each occurrence of $\alpha^{t_o}_{t_c}$ in a usage, $t_o$ and $t_c$ are respectively called the *obligation* and *capability level annotation* of the occurrence. Intuitively, they mean that the input or output $\alpha$ must be performed—though may not succeed—by the "time" (relative ordering in terms of natural numbers and $\infty$) specified by $t_o$, and will succeed by time $t_c$ if—though need not be—performed.

**Definition 3.2** (Capability)**.** For $\alpha \in \{I, O\}$, $\mathrm{cap}_\alpha(U)$ is defined by:

$$\mathrm{cap}_\alpha(\mathtt{0}) = \mathrm{cap}_\alpha(\rho) = \mathrm{cap}_\alpha\left(\overline{\alpha}^{t_o}_{t_c}.U\right) = \infty$$
$$\mathrm{cap}_\alpha\left(\alpha^{t_o}_{t_c}.U\right) = t_c$$
$$\mathrm{cap}_\alpha(U_0 \mid U_1) = \mathrm{cap}_\alpha(U_0 \,\&\, U_1) = \min(\mathrm{cap}_\alpha(U_0), \mathrm{cap}_\alpha(U_1))$$
$$\mathrm{cap}_\alpha(*U) = \mathrm{cap}_\alpha\left(\uparrow^{(t_I,t_O)} U\right) = \mathrm{cap}_\alpha(U)$$

We call $\mathrm{cap}_I(U)$ and $\mathrm{cap}_O(U)$, respectively, the *input* and *output capability level* of a usage $U$.

**Definition 3.3** (Obligation)**.** For $\alpha \in \{I, O\}$, $\mathrm{ob}_\alpha(U)$ is defined as:

$$\mathrm{ob}_\alpha(\mathtt{0}) = \mathrm{ob}_\alpha(\rho) = \mathrm{ob}_\alpha\left(\overline{\alpha}^{t_o}_{t_c}.U\right) = \infty,$$
$$\mathrm{ob}_\alpha\left(\alpha^{t_o}_{t_c}.U\right) = t_o,$$
$$\mathrm{ob}_\alpha(U_0 \mid U_1) = \min(\mathrm{ob}_\alpha(U_0), \mathrm{ob}_\alpha(U_1)),$$
$$\mathrm{ob}_\alpha(*U) = \mathrm{ob}_\alpha(U),$$
$$\mathrm{ob}_\alpha\left(\uparrow^{(t_I,t_O)} U\right) = \max(t_\alpha, \mathrm{ob}_\alpha(U)), \text{ and}$$
$$\mathrm{ob}_\alpha(U_0 \,\&\, U_1) = \max(\mathrm{ob}_\alpha(U_0), \mathrm{ob}_\alpha(U_1)).$$

We call, respectively, $\mathrm{ob}_I(U)$ and $\mathrm{ob}_O(U)$ the *input* and *output obligation level of a usage* $U$. We define $\mathrm{ob}(U) = \min(\mathrm{ob}_I(U), \mathrm{ob}_O(U))$, which is used as $\mathrm{ob}(U) = \infty$ to mean $U$ has no obligation, and write $\uparrow U$ for $\uparrow^{(t_I+1,t_O+1)} U$ where $t_I = \mathrm{ob}_I(U)$ and $t_O = \mathrm{ob}_O(U)$.

We then define reduction of usages (with structural preorder, like we did for processes), which is required for defining their reliability and for the statement of type preservation (subject reduction), as is usual for behavioral type systems, where static types capture dynamic behavior of processes.

**Definition 3.4** (Structural preorder for usages)**.** The binary relation $\preceq$ on usages is the least reflexive and transitive relation satisfying the following rules:

(UP-Zero) $\mathtt{0} \mid U \preceq U$
(UP-Commut) $U_0 \mid U_1 \preceq U_1 \mid U_0$
(UP-Assoc) $(U_0 \mid U_1) \mid U_2 \preceq U_0 \mid (U_1 \mid U_2)$
(UP-CongP) If $U_0 \preceq U_0'$, then $U_0 \mid U_1 \preceq U_0' \mid U_1$.
(UP-Rep) $*U \preceq *U \mid U$
(UP-↑) $\uparrow^{(t_I,t_O)} \alpha^{t_o}_{t_c}.U \preceq \alpha^{\max(t_o,t_\alpha)}_{t_c}.U$
(UP-Dist) $\uparrow^{(t_I,t_O)} (U_0 \mid U_1) \preceq \uparrow^{(t_I,t_O)} U_0 \mid \uparrow^{(t_I,t_O)} U_1$
(UP-Or) $U_0 \,\&\, U_1 \preceq U_i$ for $i \in \{0, 1\}$
(UP-Cong↑) If $U \preceq U'$, then $\uparrow^{(t_I,t_O)} U \preceq \uparrow^{(t_I,t_O)} U'$.
(UP-Commut↑) $\uparrow^{(t_I,t_O)} \uparrow^{(t_I',t_O')} U \preceq \uparrow^{(t_I',t_O')} \uparrow^{(t_I,t_O)} U$ [5]

**Definition 3.5** (Usage reduction)**.** The binary relation $\longrightarrow$ on usages, called *usage reduction*, is defined as the least relation satisfying the following rules:

(1) $O^{t_o}_{t_c}.U_0 \mid I^{t_o'}_{t_c'}.U_1 \longrightarrow U_0 \mid U_1$
(2) If $U_0 \longrightarrow U_0'$, then $U_0 \mid U_1 \longrightarrow U_0' \mid U_1$.
(3) If $U_0 \preceq U_0'$, $U_0' \longrightarrow U_1'$ and $U_1' \preceq U_1$, then $U_0 \longrightarrow U_1$.

We write $\longrightarrow\!\!\!\!\!\rightarrow$ for the reflexive and transitive closure of $\longrightarrow$ for usages as well.

**Definition 3.6** (Reliability)**.** We write $\mathrm{con}_\alpha(U)$ if $\mathrm{ob}_{\overline{\alpha}}(U) \leq \mathrm{cap}_\alpha(U)$, and $\mathrm{con}(U)$ if both $\mathrm{con}_I(U)$ and $\mathrm{con}_O(U)$. Then we say that a usage $U$ is *reliable*, written $\mathrm{rel}(U)$, if $\mathrm{con}(U')$ for any $U'$ such that $U \longrightarrow\!\!\!\!\!\rightarrow U'$.

Next, we define the following *subusage* and subtyping relations.

**Definition 3.7** (Subusage)**.** The *subusage relation* $<:$ on closed usages is the largest binary relation such that, whenever $U_0 <: U_1$, the following conditions hold:

(a) $U[\rho \mapsto U_0] <: U[\rho \mapsto U_1]$ for any usage $U$ with $\mathrm{FV}(U) = \{\rho\}$.
(b) If $U_1 \longrightarrow U_1'$, then there exists $U_0'$ such that $U_0 \longrightarrow U_0'$ and $U_0' <: U_1'$.
(c) $\mathrm{cap}_\alpha(U_0) \leq \mathrm{cap}_\alpha(U_1)$ for each $\alpha \in \{I, O\}$.
(d) For each $\alpha \in \{I, O\}$, if $\mathrm{con}_{\overline{\alpha}}(U_0)$, then $\mathrm{ob}_\alpha(U_0) \geq \mathrm{ob}_\alpha(U_1)$.

5. This rule was not present in [6] but is added for a part of our soundness proof.

**Proposition 3.8.** *(1) If* $U_0 <: U_1$ *and* $\mathrm{con}_\alpha(U_0)$*, then* $\mathrm{con}_\alpha(U_1)$*.*
*(2) If* $U_0 <: U_1$ *and* $\mathrm{rel}(U_0)$*, then* $\mathrm{rel}(U_1)$*.*
*(3) The subusage relation is reflexive and transitive.*

**Definition 3.9** (Subtyping)**.** The *subtyping relation* $<:$ on types is the least reflexive relation such that $\xi/U <: \xi/U'$ if $U <: U'$.

Note that if $\tau$ is a base type, then $\tau <: \tau'$ implies $\tau' = \tau$. Note also that the subtyping relation is transitive, i.e., $\tau <: \tau'$ and $\tau' <: \tau''$ imply $\tau <: \tau''$.

**Definition 3.10.** The *obligation level of a type* $\tau$, written $\mathrm{ob}_\alpha(\tau)$, is defined by

$$\mathrm{ob}_\alpha(\tau) = \begin{cases} \infty & \text{if } \tau \text{ is a base type} \\ \mathrm{ob}_\alpha(U) & \text{if } \tau = \xi/U \end{cases}$$

along with $\mathrm{ob}(\tau) = \min(\mathrm{ob}_I(\tau), \mathrm{ob}_O(\tau))$. We also define $\uparrow^{(t_I,t_O)}\tau$, $\uparrow\tau$, $*\tau$, and $\tau_0 \mid \tau_1$ as:

$$\uparrow^{(t_I,t_O)}\tau = \begin{cases} \tau & \text{if } \tau \text{ is a base type} \\ \xi/\uparrow^{(t_I,t_O)}U & \text{if } \tau = \xi/U \end{cases}$$

$$\uparrow\tau = \begin{cases} \tau & \text{if } \tau \text{ is a base type} \\ \xi/\uparrow U & \text{if } \tau = \xi/U \end{cases}$$

$$*\tau = \begin{cases} \tau & \text{if } \tau \text{ is a base type} \\ \xi/*U & \text{if } \tau = \xi/U \end{cases}$$

$$\tau_0 \mid \tau_1 = \begin{cases} \tau_0 & \text{if } \tau_0 = \tau_1 \text{ and is a base type} \\ \xi/(U_0 \mid U_1) & \text{if } \tau_0 = \xi/U_0 \text{ and } \tau_1 = \xi/U_1 \\ \text{undefined} & \text{otherwise} \end{cases}$$

We assume $\mid$ for types is also left-associative, that is, $\tau_0 \mid \tau_1 \mid \tau_2$ stands for $(\tau_0 \mid \tau_1) \mid \tau_2$.

**Definition 3.11** (Equivalence except usages)**.** The relation $\tau \sim \tau'$ on types is the least equivalence relation satisfying $\langle\tilde{\tau}\rangle^l/U \sim \langle\tilde{\tau}\rangle^l/U'$ for $l \in \mathsf{SecLev}$.

Then $\tau_0 \mid \tau_1$ is defined if and only if $\tau_0 \sim \tau_1$. Note also that $\tau_0 <: \tau_1$ implies $\tau_0 \sim \tau_1$.

## 3.2. Type Environments

Our *type environments* $\Gamma$ and $\Delta$ are defined as functions from a finite set of values $v$ (consisting of channel names $x$ and constants $c$) to types $\tau$, with constant values mapped to their respective types. We write $\emptyset$ for the empty type environment. For a value $v \notin \mathrm{Dom}(\Gamma)$, we write $\Gamma, v : \tau$ for type environment $\Gamma'$ such that $\mathrm{Dom}(\Gamma') = \mathrm{Dom}(\Gamma) \cup \{v\}$, $\Gamma'(v) = \tau$, and $\Gamma'(y) = \Gamma(y)$ for $y \in \mathrm{Dom}(\Gamma)$. We write $v : \tau$ for the type environment $\Gamma$ with $\Gamma(v) = \tau$ and $\mathrm{Dom}(\Gamma) = \{v\}$.

We extend the subtyping relation to a relation on type environments.

**Definition 3.12** (Subtyping relation on type environments)**.** For type environments $\Gamma$ and $\Delta$, we write $\Gamma <: \Delta$ if

(a) $\mathrm{Dom}(\Gamma) \supseteq \mathrm{Dom}(\Delta)$,
(b) $\Gamma(x) <: \Delta(x)$ for each $x \in \mathrm{Dom}(\Delta)$, and
(c) $\mathrm{ob}(\Gamma(x)) = \infty$ for each $x \in \mathrm{Dom}(\Gamma) \setminus \mathrm{Dom}(\Delta)$.

We say that a type environment $\Gamma$ is *closed* [6, p. 316] [23, p. 238, Definition 6.1.2] if $\Gamma(x)$ is a channel type for each channel name $x \in \mathrm{Dom}(\Gamma)$. We also say that $\Gamma$ is *reliable*, written $\mathrm{rel}(\Gamma)$, if, for any $x \in \mathrm{Dom}(\Gamma)$, $\Gamma(x)$ is a channel type $\xi/U$ with $\mathrm{rel}(U)$. Note that the subtyping relation on type environments is also transitive, i.e., if $\Gamma <: \Gamma'$ and $\Gamma' <: \Gamma''$, then $\Gamma <: \Gamma''$.

For type environments $\Gamma$ and $\Delta$, we define :

$$(\Gamma \mid \Delta)(x) = \begin{cases} \Gamma(x) \mid \Delta(x) & \text{if } x \in \mathrm{Dom}(\Gamma) \cap \mathrm{Dom}(\Delta) \\ \Gamma(x) & \text{if } x \in \mathrm{Dom}(\Gamma) \setminus \mathrm{Dom}(\Delta) \\ \Delta(x) & \text{if } x \in \mathrm{Dom}(\Delta) \setminus \mathrm{Dom}(\Gamma) \end{cases}$$

For a type environment $\Gamma$, we write $*\Gamma$, $\uparrow^{(t_I,t_O)}\Gamma$, and $\uparrow\Gamma$ for the type environments satisfying $(*\Gamma)(x) = *(\Gamma(x))$, $(\uparrow^{(t_I,t_O)}\Gamma)(x) = \uparrow^{(t_I,t_O)}(\Gamma(x))$, and $(\uparrow\Gamma)(x) = \uparrow(\Gamma(x))$, respectively. Note $\mathrm{Dom}(\Gamma \mid \Delta) = \mathrm{Dom}(\Gamma) \cup \mathrm{Dom}(\Delta)$ and $\mathrm{Dom}(*\Gamma) = \mathrm{Dom}\left(\uparrow^{(t_I,t_O)}\Gamma\right) = \mathrm{Dom}(\uparrow\Gamma) = \mathrm{Dom}(\Gamma)$. Again, we assume $\mid$ is left-associative, and abbreviate $v_1 : \tau_1 \mid \cdots \mid v_n : \tau_n$ as $\tilde{v} : \tilde{\tau}$. Furthermore, we write $\Gamma \sim \Gamma'$ if $\mathrm{Dom}(\Gamma) = \mathrm{Dom}(\Gamma')$ and $\Gamma(x) \sim \Gamma'(x)$ for every $x \in \mathrm{Dom}(\Gamma)$.

We now start to extend the type system with general lattices. The first definition below generalizes well-formed channel types [6, Definition 14]. Informally, it means the channel type is well-formed when the level of the "attacker" is $l$ (which was just $\bot$, written $\mathbf{L}$ in [6], in the 2-element lattice).

**Definition 3.13** ($l$-secure channel type)**.** We say that a channel type $\langle\tilde{\tau}\rangle^{l'}/U$ is *$l$-secure in $L$* when

(1) if $l' \leq_L l$, then all the capability level annotations in $U$ are $\infty$, and
(2) $l' \leq_L l''$ for any secrecy level $l''$ occurring in $\tilde{\tau}$.

We write $\Gamma \parallel L$ for the pair $(\Gamma, L)$ and call it an *environment*.

**Definition 3.14** ($l$-secure environment)**.** For a type environment $\Gamma$ and a lattice of secrecy levels $L$, we say that $\Gamma \parallel L$ is *$l$-secure* if every channel type in the range of $\Gamma$ is $l$-secure in $L$.

## 3.3. Typing Rules

Our *type judgement* $\Gamma \parallel L \ \rhd_m \ P$ is a tuple $(\Gamma \parallel L, m, P)$ of an environment $\Gamma \parallel L$, a secrecy level $m \in L$, and a process $P$, where every secrecy level occurring in $P$ and $\Gamma$ is in $L$. Intuitively, it means that the process $P$ is secure (i.e., does not leak information about high-secrecy values to low-level "attackers" or contexts) under the type environment $\Gamma$ and secrecy lattice $L$, where $m$ is a lower bound of the levels that $P$ may interact with (as in [6]).

$$\frac{m \in L}{\emptyset \parallel L \rhd_m \mathtt{0}}\ (\text{T-Zero}) \qquad \frac{\Gamma, x : \xi/U \parallel L \rhd_m P \qquad \mathrm{rel}(U)}{\Gamma \parallel L \rhd_m (\nu x : \xi)P}\ (\text{T-New})$$

$$\frac{\Gamma \parallel L \rhd_m P}{*\Gamma \parallel L \rhd_m *P}\ (\text{T-Rep}) \qquad \frac{\Gamma_0 \parallel L \rhd_m P_0 \qquad \Gamma_1 \parallel L \rhd_m P_1}{\Gamma_0 \mid \Gamma_1 \parallel L \rhd_m P_0 \mid P_1}\ (\text{T-Par})$$

$$\frac{\Gamma \parallel L \rhd_m P \qquad \Gamma \parallel L \rhd_m Q}{\Gamma \mid v : \mathtt{Bool}^m \parallel L \rhd_m \mathtt{if}\, v\, \mathtt{then}\, P\, \mathtt{else}\, Q}\ (\text{T-If})$$

$$\frac{\Gamma, x : \langle \tilde{\tau} \rangle^{l_0}/U \parallel L \rhd_{l_1} P \qquad m \leq_L l_0 \qquad m \leq_L l_1 \qquad t_c = \infty \Longrightarrow l_0 \leq_L l_1}{\uparrow^{(t_c+1,t_c+1)} (\Gamma \mid \tilde{v} : \uparrow \tilde{\tau}) \mid x : \langle \tilde{\tau} \rangle^{l_0}/O^0_{t_c}.U \parallel L \rhd_m x!\tilde{v}.P}\ (\text{T-Out})$$

$$\frac{\Gamma, x : \langle \tilde{\tau} \rangle^{l_0}/U, \tilde{y} : \tilde{\tau} \parallel L \rhd_{l_1} P \qquad m \leq_L l_0 \qquad m \leq_L l_1 \qquad t_c = \infty \Longrightarrow l_0 \leq_L l_1}{\uparrow^{(t_c+1,t_c+1)} (\Gamma), x : \langle \tilde{\tau} \rangle^{l_0}/I^0_{t_c}.U \parallel L \rhd_m x?\tilde{y}.P}\ (\text{T-In})$$

$$\frac{\Gamma \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right) L \rhd_m P \qquad L \sqsubseteq \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right) L \qquad m \leq_L \tilde{l_1}, \tilde{l_2}}{\Gamma \parallel L \rhd_m \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right) P}\ (\text{T-NewSec})$$

$$\frac{\Gamma' \parallel L \rhd_{m'} P \qquad \Gamma <: \Gamma' \qquad m \leq_L m'}{\Gamma \parallel L \rhd_m P}\ (\text{T-Weak})$$

Figure 1. Typing rules

The typing rules other than (T-NewSec) are similar to previous ones [6] except that they are all parameterized by the general lattice of secrecy levels $L$. The second premise $L \sqsubseteq \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right) L$ in (T-NewSec) ensures safe extension thanks to our previous definitions on lattices (Definition 2.3 and Definition 2.5). The "side" condition $m \leq_L \tilde{l_1}, \tilde{l_2}$, which is more subtle, guarantees that high-secrecy operations can be erased in the proof of non-interference (the third last case in Definition F.9).

We say a type judgement $\Gamma \parallel L \rhd_m P$ is *$l$-secure* if $\Gamma \parallel L$ is $l$-secure. An *$l$-secure derivation tree* is defined as a tree of $l$-secure type judgements constructed by instances of the rules in Figure 1. An $l$-secure derivation tree with root $\Gamma \parallel L \rhd_m P$ is called an *$l$-secure derivation tree of* $\Gamma \parallel L \rhd_m P$. We say that $\Gamma \parallel L \rhd_m P$ is *$l$-securely derivable from* $\Delta \parallel L' \rhd_{m'} P'$ if there exists an $l$-secure derivation tree of $\Gamma \parallel L \rhd_m P$ whose leaves are either $\Delta \parallel L' \rhd_{m'} P'$ or constructed by (T-Zero). We also say that $\Gamma \parallel L \rhd_m P$ is *$l$-securely derivable* if there exists a derivation tree of $\Gamma \parallel L \rhd_m P$ whose leaves are constructed by (T-Zero), and that $\Gamma \parallel L \rhd_m P$ is *derivable* (from $\Delta \parallel L' \rhd_{m'} P'$) if it is $l$-securely derivable (from $\Delta \parallel L' \rhd_{m'} P'$) for some $l$.

All the careful definitions above are needed for soundness and related proofs of our type system with a generalized (let alone extensible) security lattice (that is, lattice of secrecy levels).

**Example 3.15.** Figure 2 shows a $\top$-secure derivation tree for $\Gamma \parallel L \rhd_\bot P$ where the process $P$ is

$$(\top < \nu l < \bot)\left(\nu x : \left\langle v : \mathtt{Bool}^l \right\rangle^l\right)(x!\mathrm{true}^l.y?.\mathtt{0} \mid x?b.\mathtt{0}),$$

$\Gamma = y : \langle\rangle^\bot/\uparrow^{(1,1)} (I^0_\infty.\mathtt{0}) \mid \mathtt{0}$, and $L = \{\bot, \top\}$. Intuitively, $P$ creates a new secrecy level $l$ and internally communicates a Boolean value $\mathrm{true}^l$ of that level. Non-interferece means that replacing it with $\mathrm{false}^l$ makes no difference to low-level observers.

The following proposition allows a weakening, namely, extension of the lattice $L$ in an environment $\Gamma \parallel L$.

**Proposition 3.16.** *If $\Gamma \parallel L \rhd_m P$ is $l$-securely derivable (resp. from $\Delta \parallel L' \rhd_{m'} P'$), then $\Gamma \parallel \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right) L \rhd_m P$ is also $l$-securely derivable (resp. from $\Delta \parallel \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right) L' \rhd_{m'} P'$), where $l'$ is fresh.*

## 4. Soundness

In this section, we will prove our main theorem: non-interference. To that goal, we first show two important properties of well-typed processes: subject reduction (type preservation) and lock-freedom.

### 4.1. Subject reduction

We define $\Gamma \longrightarrow \Gamma'$ as $\Gamma = (\Gamma_0, x : \xi/U)$ for some $x$ with $U \longrightarrow U'$ and $\Gamma' = (\Gamma_0, x : \xi/U')$. Again, we write $\longrightarrow\!\!\!\!\!\rightarrow$ for the reflexive and transitive closure of $\longrightarrow$.

**Lemma 4.1.** *If $\Gamma \parallel L$ is $l$-secure and $\Gamma \longrightarrow \Gamma'$, then $\Gamma' \parallel L$ is $l$-secure.*

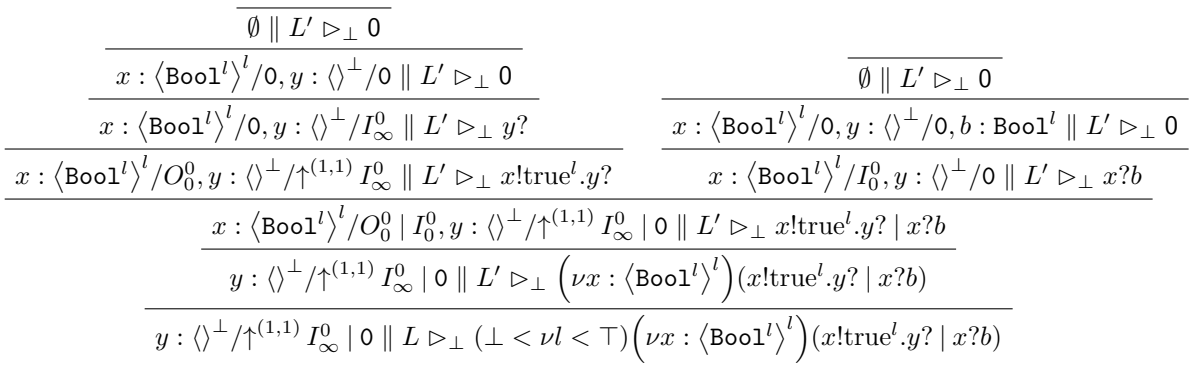

Figure 2. An example of typing (rule names and trailing $\mathtt{0}$ are omitted), where $L' = ((\bot) < \nu l < (\top))L$

**Lemma 4.2** (Structural preorder preserves typing)**.** *If* $\Gamma \parallel L \rhd_m P$ *is* $l$*-securely derivable and* $P \preceq P'$*, then* $\Gamma \parallel L \rhd_m P'$ *is also* $l$*-securely derivable.*

*Proof.* See Appendix D.2. □

**Definition 4.3** (Substitution on type environment)**.** For a type environment $\Gamma$, variables $\tilde{x}$, and values $\tilde{v}$ with $\{\tilde{x}\} \cap \{\tilde{v}\} = \emptyset$, we define a type environment $\Gamma[\tilde{x} \mapsto \tilde{v}]$ as in Figure 3. Furthermore, we say that $\Gamma[\tilde{x} \mapsto \tilde{v}]$ *is well-defined* if $\mathrm{Dom}(\Gamma[\tilde{x} \mapsto \tilde{v}]) = (\mathrm{Dom}(\Gamma) \setminus \{\tilde{x}\}) \cup \{v_i \mid x_i \in \mathrm{Dom}(\Gamma)\}$.

**Lemma 4.4** (Substitution lemma)**.** *If* $\Gamma \parallel L \rhd_m P$ *is* $l$*-securely derivable and* $\Gamma[\tilde{x} \mapsto \tilde{v}]$ *is well-defined, then* $\Gamma[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P[\tilde{x} \mapsto \tilde{v}]$ *is also* $l$*-securely derivable.*

*Proof.* See Appendix D.3. □

**Proposition 4.5** (Subject reduction)**.** *If* $\Gamma \parallel L \rhd_m P$ *is* $l$*-securely derivable and* $(P, L) \longrightarrow (P', L')$*, then there exists* $\Gamma'$ *such that either* $\Gamma = \Gamma'$ *or* $\Gamma \longrightarrow \Gamma'$*, and that* $\Gamma' \parallel L' \rhd_m P'$ *is* $l$*-securely derivable.*

*Proof.* By induction on the derivation of $(P, L) \longrightarrow (P', L')$. See Appendix D.4 for details. □

Note that the $L'$ above is always a superlattice of $L$—that is, $L$ is a sublattice of $L'$—as can be proved by simple induction according to Definition 2.7.

## 4.2. Lock-freedom

Next, we prove the lock-freedom property, which, in short, guarantees that every input or output with finite (namely, not $\infty$) capability will eventually succeed and, as a result, such high-level synchronization can securely be performed even before low-level communication.[6]

**Definition 4.6** (Strong barbs)**.** Let $P$ be a process. We define $\mathrm{SBarbs}_O(P)$, $\mathrm{SBarbs}_I(P)$, and $\mathrm{SBarbs}(P)$ as:

$$\mathrm{SBarbs}_O(P) = \left\{ x \;\middle|\; \begin{array}{c} P \preceq (\nu\tilde{y})(x!\tilde{v}.P_0 \mid P_1) \text{ with} \\ x \notin \tilde{y} \text{ for some } P_0, P_1 \end{array} \right\}$$

6. Although we do not consider timing in the present paper, it can also be incorporated [24].

$$\mathrm{SBarbs}_I(P) = \left\{ x \;\middle|\; \begin{array}{c} P \preceq (\nu\tilde{y})(x?\tilde{z}.P_0 \mid P_1) \text{ with} \\ x \notin \tilde{y} \text{ for some } P_0, P_1 \end{array} \right\}$$
$$\mathrm{SBarbs}(P) = \mathrm{SBarbs}_O(P) \cup \mathrm{SBarbs}_I(P)$$

The following definition specifies reduction by internal communication on a secret channel (of level $l'$) that the attacker (of level $l$) cannot access ($l' \not\leq_L l$).

**Definition 4.7** (Secret reduction)**.** For a type environment $\Gamma$, the binary relation $\longrightarrow_l^\Gamma$ is defined as the least relation satisfying the following rules:

(1) $(x!(v_0, \ldots, v_n).P_0 \mid x?(y_0, \ldots, y_n).P_1, L) \longrightarrow_l^\Gamma (P_0 \mid P_1[y_0 \mapsto v_0, \ldots, y_n \mapsto v_n], L)$, where the secrecy level of $\Gamma(x)$ is $l'$ with $l' \not\leq_L l$

(2) If $\tilde{l_0}, \tilde{l_1} \subseteq L$ and $\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$ is defined, then $\left(\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)P, L\right) \longrightarrow_l^\Gamma \left(P, \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L\right)$.

(3) If $(P_0, L) \longrightarrow_l^\Gamma (P_0', L')$, then $(P_0 \mid P_1, L) \longrightarrow_l^\Gamma (P_0' \mid P_1, L')$,

(4) If $(P, L) \longrightarrow_l^{\Gamma, x:\xi/U} (P', L')$, then $((\nu x : \xi)P, L) \longrightarrow_l^\Gamma ((\nu x : \xi)P', L')$,

(5) If $P_0 \preceq P_0'$, $(P_0', L_0) \longrightarrow_l^\Gamma (P_1', L_1)$, and $P_1' \preceq P_1$, then $(P_0, L_0) \longrightarrow_l^\Gamma (P_1, L_1)$.

We write $\longrightarrow\!\!\!\!\rightarrow_l^\Gamma$ for the reflexive and transitive closure of $\longrightarrow_l^\Gamma$.

Note that the secret reduction $(P_0, L_0) \longrightarrow_l^\Gamma (P_1, L_1)$ implies usual reduction $(P_0, L_0) \longrightarrow (P_1, L_1)$.

**Lemma 4.8.** *Suppose that* $\Gamma \parallel L \rhd_m P$ *and* $\Delta \parallel L \rhd_m Q$ *are* $k$*-securely derivable,* $\Gamma | \Delta$ *is reliable,* $\Gamma \mid \Delta \parallel L$ *is* $k$*-secure, and* $\mathrm{ob}_\alpha(\Gamma(x))$ *is finite, where* $\alpha = I$ *or* $\alpha = O$*. Then, there exist a process* $R$ *and a lattice for secrecy levels* $\hat{L}$ *such that* $(P \mid Q, L) \longrightarrow\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R, \hat{L}\right)$ *and* $x \in \mathrm{SBarbs}_\alpha(R)$.

*Proof.* See Section E.2. □

**Definition 4.9** (Context)**.** A *context* is defined as an expression obtained from a process by replacing a subprocess with $[\,]$. We write $C[P]$ for the process obtained by replacing $[\,]$ in $C$ with $P$.

$$\Gamma[\tilde{x} \mapsto \tilde{v}](w) = \begin{cases} \Gamma(w) & \text{if } w \notin \tilde{v} \text{ and } w \notin \tilde{x} \\ \Gamma(x_{j_0}) \mid \cdots \mid \Gamma(x_{j_k}) & \text{if } w \in \tilde{v} \text{ and } w \notin \mathrm{Dom}(\Gamma) \text{ with } \{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma)\} = \{x_{j_0}, \ldots, x_{j_k}\} \text{ for } 0 \le j_0 < \cdots < j_k \le n \\ \Gamma(x_{j_0}) \mid \cdots \mid \Gamma(x_{j_k}) \mid \Gamma(w) & \text{if } w \in \tilde{v} \text{ and } w \in \mathrm{Dom}(\Gamma) \text{ with } \{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma)\} = \{x_{j_0}, \ldots, x_{j_k}\} \text{ for } 0 \le j_0 < \cdots < j_k \le n \end{cases}$$

Figure 3. Substitution on type environment

$$\begin{aligned} \mathrm{depth}\left(\left[\,\right]^{(1)}\right) = \mathrm{depth}\left(\left[\,\right]^{(2)}\right) &= 0 \\ \mathrm{depth}(P) &= 0 \quad \text{if } \left[\,\right]^{(1)} \text{ and } \left[\,\right]^{(2)} \text{ do not occur in } P \\ \mathrm{depth}(C_0 \mid C_1) &= \mathrm{depth}(C_0) + \mathrm{depth}(C_1) \\ \mathrm{depth}(x!\tilde{v}.C_0) &= \mathrm{depth}(C_0) + 1 \\ \mathrm{depth}(x?\tilde{y}.C_0) &= \mathrm{depth}(C_0) + 1 \\ \mathrm{depth}(*C_0) &= \mathrm{depth}(C_0) \\ \mathrm{depth}((\nu x : \xi)C_0) &= \mathrm{depth}(C_0) \\ \mathrm{depth}\left(\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)C_0\right) &= \mathrm{depth}(C_0) + 1 \\ \mathrm{depth}(\texttt{if } v \texttt{ then } C_0 \texttt{ else } C_1) &= \mathrm{depth}(C_0) + \mathrm{depth}(C_1) \end{aligned}$$

Figure 4. Depth of context

A *context with two holes* is defined as an expression obtained from a process by replacing just two subprocesses with $[\,]^{(1)}$ and $[\,]^{(2)}$. We write $C\,[P_0]^{(1)}[P_1]^{(2)}$ for the process obtained by replacing $[\,]^{(1)}$ and $[\,]^{(2)}$ in $C$ with $P_0$ and $P_1$, respectively.

**Definition 4.10** (Depth of context)**.** For a context with two holes $C$, we inductively define the depth of $C$, written $\mathrm{depth}(C)$, as in Figure 4. We also define the depth of a context with one hole in the same manner.

**Definition 4.11** ($k$-constrained derivation tree, $k$-finite level context, $k$-evaluation context)**.** For a context $C$ (resp. with two holes), we define a *$k$-constrained derivation tree* of $\Gamma \parallel L \rhd_l C$ as a $k$-secure derivation tree of $\Gamma \parallel L \rhd_l C$ from $\Delta \parallel L' \rhd_{l'} [\,]$ (resp. $\Delta_1 \parallel L'_1 \rhd_{l'_1} [\,]^{(1)}$ and $\Delta_2 \parallel L'_2 \rhd_{l'_2} [\,]^{(2)}$) where $l_0 \le_L k$ or $t_c$ is finite in every instance of (T-Out) or (T-In) if $[\,]$ (resp. $[\,]^{(1)}$ or $[\,]^{(2)}$) occurs in $P$.

We then define an *$k$-finite level context in $L$* as a context $F$ satisfying the following conditions:

(1) $F$ is of the following forms:

$$F ::= [\,] \mid (P \mid F) \mid (F \mid P) \mid x!\tilde{v}.F \mid x?\tilde{y}.F \mid (\nu x : \xi)F \mid \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)F$$

(2) There exists a $k$-constrained derivation tree of $\Gamma \parallel L \rhd_l F$.

We also define an *$k$-finite level context in $L$ with two holes* as a context with two holes $F$ satisfying the following conditions:

(1) $F$ is of the following forms:

$$\begin{aligned} F ::= {} & (F^{(1)} \mid F^{(2)}) \mid (F^{(2)} \mid F^{(1)}) \mid (P \mid F) \mid (F \mid P) \mid \\ & x!\tilde{v}.F \mid x?\tilde{y}.F \mid (\nu x : \xi)F \mid \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)F \\ F^{(1)} ::= {} & [\,]^{(1)} \mid (P \mid F^{(1)}) \mid (F^{(1)} \mid P) \mid x!\tilde{v}.F^{(1)} \mid \\ & x?\tilde{y}.F^{(1)} \mid (\nu x : \xi)F^{(1)} \mid \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)F^{(1)} \\ F^{(2)} ::= {} & [\,]^{(2)} \mid (P \mid F^{(2)}) \mid (F^{(2)} \mid P) \mid x!\tilde{v}.F^{(2)} \mid \\ & x?\tilde{y}.F^{(2)} \mid (\nu x : \xi)F^{(2)} \mid \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)F^{(2)} \end{aligned}$$

(2) There exists a $k$-constrained derivation tree of $\Gamma \parallel L \rhd_l F$.

Finally, we define an *$k$-evaluation context* (resp. *with two holes*) as a $k$-finite level context (resp. with two holes) of depth 0.

**Lemma 4.12.** *Let $D_0 \mid D_1$ be a context with two holes (hence, $D_i$ is a process, a context, or a context with two holes for $i = 0, 1$). Suppose that $\Gamma \parallel L \rhd_l D_0$ and $\Delta \parallel L \rhd_l D_1$ are $k$-securely derivable from $\Gamma_0 \parallel L_0 \rhd_{l_0} [\,]^{(1)}$ and $\Gamma_1 \parallel L_1 \rhd_{l_1} [\,]^{(2)}$, $\Gamma \mid \Delta$ is reliable, $\Gamma \mid \Delta \parallel L$ is $k$-secure, and $\mathrm{ob}_\alpha(\Gamma(x))$ is finite, where $\alpha = I$ or $\alpha = O$. Then, there exist a context with two holes $C$ and a lattice for secrecy levels $\hat{L}$ such that $(D_0 \mid D_1, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma \mid \Delta} \left(C, \hat{L}\right)$ and $x \in \mathrm{SBarbs}_\alpha(C)$.*

*Proof.* Similar to Lemma 4.8. □

**Lemma 4.13.** *Let $F$ be a $k$-finite level context with two holes, and $\Gamma \parallel L \rhd_l F$ be the root of a $k$-constrained derivation tree. If $\Gamma$ is reliable, then there exist an evaluation context $E$ and a lattice for secrecy levels $\hat{L}$ such that $(F, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma} \left(E, \hat{L}\right)$.*

*Proof.* By induction on the depth of $F$.

In case the depth of $F$ is 0, we have the claimed result immediately.

Assume that $F$ is of the form $E_0[x!\tilde{v}.C_0]$ for an evaluation context $E_0$. Since $\Gamma$ is reliable, $\mathrm{ob}_I(\Gamma(x)) \leq \mathrm{cap}_O(\Gamma(x))$.

Assume $x$ is free. Since $\Gamma \parallel L \rhd_l F$ is the root of the $k$-constrained derivation tree of $F$, $\mathrm{cap}_O(\Gamma(x))$ is finite. Hence, $\mathrm{ob}_I(\Gamma(x))$ is finite. By Lemma 4.12, there exist $R$ and $\hat{L}$ such that $(E_0[x!\tilde{v}.C_0], L) \longrightarrow\!\!\!\!\rightarrow_k^\Gamma \left(R, \hat{L}\right)$ and $x \in \mathrm{SBarbs}_I(R)$. Then $(E_0[x!\tilde{v}.F_0], L) \longrightarrow\!\!\!\!\rightarrow_k^\Gamma \left(E_0'[F_0], \hat{L}_0\right)$ for an evaluation context $E_0'$. By the induction hypothesis, there exists an evaluation context $E$ and a lattice for secrecy levels $\hat{L}$ such that $\left(E_0'[C_0], \hat{L}_0\right) \longrightarrow\!\!\!\!\rightarrow_k^\Gamma \left(E, \hat{L}\right)$. Thus, $(F, L) \longrightarrow\!\!\!\!\rightarrow_k^\Gamma \left(E, \hat{L}\right)$

In the case that $x$ is not free, $E_0[x!\tilde{v}.F_0] \preceq (\nu x)E_0'[x!\tilde{v}.F_0]$ for a evaluation context $E_0'$. Since there is a $k$-constrained derivation tree of $\Gamma \parallel L \rhd_l E_0[x!\tilde{v}.F_0]$, there is a $k$-constrained derivation tree of $\Gamma \parallel L \rhd_l (\nu x)E_0'[x!\tilde{v}.F_0]$. Hence, there is a $k$-constrained derivation tree of $\Gamma, x : \xi/U \parallel L \rhd_l E_0'[x!\tilde{v}.F_0]$ with $\mathrm{rel}(U)$. Therefore, we can show the claim in the same way to the case that $x$ is free.

In case $F$ is of the form $E[x?\tilde{y}.F_0]$, we can show the claim in the similar way to the case $F \equiv E[x!\tilde{v}.F_0]$.

In case $F$ is of the form $E\left[\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)F_0\right]$, we can show the claim easily. □

### 4.3. Non-interference

We will now show our main theorem: the non-interference property of well-typed processes.

**Definition 4.14** (Barbs)**.** Let $P$ be a process, and $L$ be a lattice of secrecy levels. We define the *barbs of* $(P, L)$, written $\mathrm{Barbs}(P, L)$, as:

$$\left\{ x \;\middle|\; \begin{array}{c} (P, L) \longrightarrow\!\!\!\!\rightarrow (P', L') \text{ and} \\ P' = (\nu\tilde{y})x!\tilde{v}.P_0 \mid P_1 \text{ or } P' = (\nu\tilde{y})x?\tilde{z}.P_0 \mid P_1 \\ \text{with } x \notin \tilde{y} \text{ for some } P_0, P_1 \end{array} \right\}$$

**Definition 4.15** (Barbed bisimulation)**.** A *barbed bisimulation* is defined as a binary relation $\mathcal{R}$ on $\mathscr{P} \times \mathscr{L}$ satisfying the following conditions for every $((P_0, L_0), (P_1, L_1)) \in \mathcal{R}$.

(1) If $(P_0, L_0) \longrightarrow (P_0', L_0')$, then there exists $(P_1', L_1')$ such that $(P_1, L_1) \longrightarrow\!\!\!\!\rightarrow (P_1', L_1')$ with $((P_0', L_0'), (P_1', L_1')) \in \mathcal{R}$.
(2) If $(P_1, L_1) \longrightarrow (P_1', L_1')$, then there exists $(P_0', L_0')$ such that $(P_0, L_0) \longrightarrow\!\!\!\!\rightarrow (P_0', L_0')$ with $((P_0', L_0'), (P_1', L_1')) \in \mathcal{R}$.
(3) $\mathrm{Barbs}(P_0, L_0) = \mathrm{Barbs}(P_1, L_1)$

We say that $(P_0, L_0)$ and $(P_1, L_1)$ are *barbed bisimilar*, written $(P_0, L_0) \overset{\bullet}{\approx} (P_1, L_1)$, if there exists a barbed bisimulation $\mathcal{R}$ such that $((P_0, L_0), (P_1, L_1)) \in \mathcal{R}$.

**Definition 4.16.** A context $C$ is called an $(\Gamma \parallel L, m)$-$(\Delta \parallel L', m')$-*context* if $\Delta \parallel L' \rhd_{m'} C$ is derivable from $\Gamma \parallel L \rhd_m [\,]$.

Note that $L' \sqsubseteq L$ if $\Delta \parallel L' \rhd_{m'} C$ is derivable from $\Gamma \parallel L \rhd_m [\,]$.

**Definition 4.17** (Barbed congruence)**.** For processes $P_0$ and $P_1$, we say that $P_0$ and $P_1$ are barbed $(\Gamma \parallel L, m)$-congruent, written $P_0 \underset{(\Gamma\parallel L,m)}{\approx} P_1$, if

(1) $\Gamma \parallel L \rhd_m P_i$ is derivable for $i = 0, 1$, and
(2) for any closed $\Delta$, lattice of secrecy levels $L'$, secrecy level $m'$, and any $(\Gamma \parallel L, m)$-$(\Delta \parallel L', m')$-context $C$, $(C[P_0], L') \overset{\bullet}{\approx} (C[P_1], L')$.

We say that *the secrecy level of* $\Gamma \parallel L$ *is* $l$ if $l$ is the supremum in $L$ of all the secrecy levels that appear in $\Gamma(x)$ for every channel name $x \in \mathrm{Dom}(\Gamma)$.

Now, we state the non-interference theorems. Intuitively, they guarantee secrets—values of level $l'$, or behavior of processes of level $m'$—do not leak to attackers of level $l$ or $k$.

**Theorem 4.18** (Non-interference (1))**.** *For any type environment* $\Gamma$*, lattice of secrecy levels* $L$*, process* $P$*, and secrecy levels* $l$*,* $l'$*, we have*

$$P\left[x \mapsto \mathrm{true}^{l'}\right] \underset{(\Gamma\parallel L,m)}{\approx} P\left[x \mapsto \mathrm{false}^{l'}\right]$$

*if* $\Gamma \parallel L \rhd_m P\left[x \mapsto \mathrm{true}^{l'}\right]$ *is* $k$*-securely derivable, the secrecy level of* $\Gamma \parallel L$ *is* $l$*,* $l' \not\leq_L l$*, and* $l' \not\leq_L k$*.*

*Proof.* It suffices to show that, for any closed $\Delta$, a lattice for secrecy levels $L'$, and a secrecy level $m'$, $\left(C\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right], L'\right) \overset{\bullet}{\approx} \left(C\left[P\left[x \mapsto \mathrm{false}^{l'}\right], L'\right]\right)$ with any $(\Gamma \parallel L, m)$-$(\Delta \parallel L', m')$-context $C$. We can construct a process $Q$, where

$$\left(C\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right], L'\right) \overset{\bullet}{\approx} (Q, L') \overset{\bullet}{\approx} \left(C\left[P\left[x \mapsto \mathrm{false}^{l'}\right], L'\right]\right).$$

Hence, we have the claimed result. $Q$ is obtained by eliminating channels with secrecy level higher than $k$ from $C\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right]$. See Section F.6 for details. □

**Theorem 4.19** (Non-interference (2))**.** *For any type environments* $\Gamma$*,* $\Delta$*, lattices for secrecy levels* $L$*,* $L'$*, processes* $P_0$*,* $P_1$*, and any* $(\Delta \parallel L', m')$-$(\Gamma \parallel L, m)$*-context* $C$*, we have*

$$C[P_0] \underset{(\Gamma\parallel L,m)}{\approx} C[P_1]$$

*if* $\Delta \parallel L' \rhd_{m'} P_i$ *is* $k$*-securely derivable for* $i = 0, 1$*, the secrecy level of* $\Gamma \parallel L$ *is* $l$*,* $m' \not\leq_L l$*, and* $m' \not\leq_L k$*.*

*Proof.* Let $\Pi$ be a closed type environment, and $C$ be $(\Gamma \parallel L, m)$-$(\Pi \parallel L', m'')$-context. We can construct a context $D$, where $\left(C\left[\hat{C}[P_0]\right], L\right) \overset{\bullet}{\approx} \left(D\left[\hat{C}[P_0]\right], L\right) \overset{\bullet}{\approx} \left(D\left[\hat{C}[P_1]\right], L\right) \overset{\bullet}{\approx} \left(C\left[\hat{C}[P_1]\right], L\right)$. $D$ is obtained by eliminating channels with secrecy level higher than $k$ from $C$. See Section F.7 for details. □ □

## 5. Conclusion

We have defined $\pi^L$-calculus, an extension of $\pi$-calculus with secrecy types and an operation to extend the lattice of secrecy levels. Then, we have given a type system for secure information flow and shown the lock-freedom and non-interference properties. Our system has extended previous work [6] with general lattices and its dynamic extensions, requiring deliberate definitions and proofs for sound generalization and safe extension of the security lattices. Future work would include further extending the calculus with polymorphism for secrecy levels so that processes can communicate and share the new levels they create, as well as considering other operations—such as deletion—to dynamically change the security lattice.

## Acknowledgments

This work was supported by JST CREST, Japan, Grant Number JPMJCR22M3 and the Acquisition, Technology & Logistics Agency (ATLA), Japan, under the Innovative Science and Technology Initiative for Security program, Grant Number JPJ013268 and in part by JSPS KAKENHI Grant Numbers 22K19766 and 23K20379 (20H04161).

## References

[1] D. E. Denning, "A lattice model of secure information flow," *Commun. ACM*, vol. 19, no. 5, pp. 236–243, 1976. [Online]. Available: https://doi.org/10.1145/360051.360056

[2] J. A. Goguen and J. Meseguer, "Security policies and security models," in *1982 IEEE Symposium on Security and Privacy, Oakland, CA, USA, April 26-28, 1982*. IEEE Computer Society, 1982, pp. 11–20. [Online]. Available: https://doi.org/10.1109/SP.1982.10014

[3] D. M. Volpano, C. E. Irvine, and G. Smith, "A sound type system for secure flow analysis," *J. Comput. Secur.*, vol. 4, no. 2/3, pp. 167–188, 1996. [Online]. Available: https://doi.org/10.3233/JCS-1996-42-304

[4] A. Sabelfeld and A. C. Myers, "Language-based information-flow security," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 1, pp. 5–19, 2003. [Online]. Available: https://doi.org/10.1109/JSAC.2002.806121

[5] N. Heintze and J. G. Riecke, "The slam calculus: Programming with secrecy and integrity," in *POPL '98, Proceedings of the 25th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, San Diego, CA, USA, January 19-21, 1998*, D. B. MacQueen and L. Cardelli, Eds. ACM, 1998, pp. 365–377. [Online]. Available: https://doi.org/10.1145/268946.268976

[6] N. Kobayashi, "Type-based information flow analysis for the pi-calculus," *Acta Informatica*, vol. 42, no. 4-5, pp. 291–347, 2005. [Online]. Available: https://doi.org/10.1007/s00236-005-0179-x

[7] ——, "A type system for lock-free processes," *Inf. Comput.*, vol. 177, no. 2, pp. 122–159, 2002. [Online]. Available: https://doi.org/10.1006/inco.2002.3171

[8] R. Milner, *Communicating and mobile systems - the Pi-calculus*. Cambridge University Press, 1999.

[9] R. Milner, J. Parrow, and D. Walker, "A calculus of mobile processes, I," *Inf. Comput.*, vol. 100, no. 1, pp. 1–40, 1992. [Online]. Available: https://doi.org/10.1016/0890-5401(92)90008-4

[10] ——, "A calculus of mobile processes, II," *Inf. Comput.*, vol. 100, no. 1, pp. 41–77, 1992. [Online]. Available: https://doi.org/10.1016/0890-5401(92)90009-5

[11] R. Milner and D. Sangiorgi, "Barbed bisimulation," in *Automata, Languages and Programming, 19th International Colloquium, ICALP92, Vienna, Austria, July 13-17, 1992, Proceedings*, ser. Lecture Notes in Computer Science, W. Kuich, Ed., vol. 623. Springer, 1992, pp. 685–695. [Online]. Available: https://doi.org/10.1007/3-540-55719-9_114

[12] K. G. Larsen and A. Skou, "Bisimulation through probabilistic testing," *Inf. Comput.*, vol. 94, no. 1, pp. 1–28, 1991. [Online]. Available: https://doi.org/10.1016/0890-5401(91)90030-6

[13] G. Smith, "Probabilistic noninterference through weak probabilistic bisimulation," in *16th IEEE Computer Security Foundations Workshop (CSFW-16 2003), 30 June - 2 July 2003, Pacific Grove, CA, USA*. IEEE Computer Society, 2003, pp. 3–13. [Online]. Available: https://doi.org/10.1109/CSFW.2003.1212701

[14] V. Castiglioni, R. Lanotte, and S. Tini, "Back to the format: A survey on SOS for probabilistic processes," *J. Log. Algebraic Methods Program.*, vol. 137, p. 100929, 2024. [Online]. Available: https://doi.org/10.1016/j.jlamp.2023.100929

[15] T. Spork, C. Baier, J. Katoen, J. Piribauer, and T. Quatmann, "A spectrum of approximate probabilistic bisimulations," in *35th International Conference on Concurrency Theory, CONCUR 2024, September 9-13, 2024, Calgary, Canada*, ser. LIPIcs, R. Majumdar and A. Silva, Eds., vol. 311. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024, pp. 37:1–37:19. [Online]. Available: https://doi.org/10.4230/LIPIcs.CONCUR.2024.37

[16] R. J. van Glabbeek, "The linear time - branching time spectrum I," in *Handbook of Process Algebra*, J. A. Bergstra, A. Ponse, and S. A. Smolka, Eds. North-Holland / Elsevier, 2001, pp. 3–99. [Online]. Available: https://doi.org/10.1016/b978-044482830-9/50019-9

[17] ——, "The linear time - branching time spectrum II," in *CONCUR '93, 4th International Conference on Concurrency Theory, Hildesheim, Germany, August 23-26, 1993, Proceedings*, ser. Lecture Notes in Computer Science, E. Best, Ed., vol. 715. Springer, 1993, pp. 66–81. [Online]. Available: https://doi.org/10.1007/3-540-57208-2_6

[18] B. Finkbeiner and E. Olderog, "Concurrent hyperproperties," in *Theories of Programming and Formal Methods - Essays Dedicated to Jifeng He on the Occasion of His 80th Birthday*, ser. Lecture Notes in Computer Science, J. P. Bowen, Q. Li, and Q. Xu, Eds., vol. 14080. Springer, 2023, pp. 211–231. [Online]. Available: https://doi.org/10.1007/978-3-031-40436-8_8

[19] nLab, "lattice," https://ncatlab.org/nlab/show/lattice, as of July 2025.

[20] P. T. Johnstone, *Stone Spaces*. Cambridge University Press, 1986.

[21] E. Sumii and N. Kobayashi, "A generalized deadlock-free process calculus," in *3rd International Workshop on High-Level Concurrent Languages, HLCL 1998, Satellite Workshop of CONCUR 1998, Nice, France, September 12, 1998*, ser. Electronic Notes in Theoretical Computer Science, U. Nestmann and B. C. Pierce, Eds., vol. 16, no. 3. Elsevier, 1998, pp. 225–247. [Online]. Available: https://doi.org/10.1016/S1571-0661(04)00144-6

[22] J. Girard, "Linear logic," *Theor. Comput. Sci.*, vol. 50, pp. 1–102, 1987. [Online]. Available: https://doi.org/10.1016/0304-3975(87)90045-4

[23] D. Sangiorgi and D. Walker, *The Pi-Calculus - a theory of mobile processes*. Cambridge University Press, 2001.

[24] N. Kobayashi, "Type systems for concurrent processes: From deadlock-freedom to livelock-freedom, time-boundedness," in *Theoretical Computer Science, Exploring New Frontiers of Theoretical Informatics, International Conference IFIP TCS 2000, Sendai, Japan, August 17-19, 2000, Proceedings*, ser. Lecture Notes in Computer Science, J. van Leeuwen, O. Watanabe, M. Hagiya, P. D. Mosses, and T. Ito, Eds., vol. 1872. Springer, 2000, pp. 365–389. [Online]. Available: https://doi.org/10.1007/3-540-44929-9_27

## Appendix A.
## Basic properties of $\pi^L$-calculus

**Lemma A.1.** *For a lattice of secrecy levels $L$, assume that $\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$ is defined, and $L \sqsubseteq \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$. Let $L' = \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$. Then $\left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)L'$ is defined and $L' \sqsubseteq \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)L'$.*

*Proof.* Straightforward. □

**Lemma A.2.** *For a lattice of secrecy levels $L$ and $\tilde{l_0}, \tilde{l_1}, \tilde{l'_0}, \tilde{l'_1} \subseteq L$, assume that $\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$ and $\left(\tilde{l'_0} < \nu l' < \tilde{l'_1}\right)\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$ are defined, and $L \sqsubseteq \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$ and $\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L \sqsubseteq \left(\tilde{l'_0} < \nu l' < \tilde{l'_1}\right)\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$. Then $\left(\tilde{l'_0} < \nu l' < \tilde{l'_1}\right)L$ and $\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)\left(\tilde{l'_0} < \nu l' < \tilde{l'_1}\right)L$ are defined and $L \sqsubseteq \left(\tilde{l'_0} < \nu l' < \tilde{l'_1}\right)L$, $\left(\tilde{l'_0} < \nu l' < \tilde{l'_1}\right)L \sqsubseteq \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)\left(\tilde{l'_0} < \nu l' < \tilde{l'_1}\right)L$, and $\left(\tilde{l'_0} < \nu l' < \tilde{l'_1}\right)\left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L = \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)\left(\tilde{l'_0} < \nu l' < \tilde{l'_1}\right)L$.*

*Proof.* Straightforward. □

**Proposition A.3.** *If $P_0 \preceq P'_0$ and $P_1 \preceq P'_1$, then $P_0 \mid P_1 \preceq P'_0 \mid P'_1$.*

*Proof.* Assume $P_0 \preceq P'_0$ and $P_1 \preceq P'_1$. By (SP-Commut) and (SP-Par), we see

$$\begin{aligned} P_0 \mid P_1 &\preceq P'_0 \mid P_1 && \text{(SP-Par)} \\ &\preceq P_1 \mid P'_0 && \text{(SP-Commut)} \\ &\preceq P'_1 \mid P'_0 && \text{(SP-Par)} \\ &\preceq P'_0 \mid P'_1 && \text{(SP-Commut).} \end{aligned}$$

□

**Lemma A.4.** $P_0 \mid (P_1 \mid P_2) \preceq (P_0 \mid P_1) \mid P_2$.

*Proof.* By (SP-Commut), (SP-Assoc) and (SP-Par), we see

$$\begin{aligned} P_0 \mid (P_1 \mid P_2) &\preceq (P_1 \mid P_2) \mid P_0 && \text{(SP-Commut)} \\ &\preceq (P_2 \mid P_1) \mid P_0 && \text{(SP-Commut) and (SP-Par)} \\ &\preceq P_2 \mid (P_1 \mid P_0) && \text{(SP-Assoc)} \\ &\preceq P_2 \mid (P_0 \mid P_1) && \text{(SP-Commut) and (SP-Par)} \\ &\preceq (P_0 \mid P_1) \mid P_2 && \text{(SP-Commut).} \end{aligned}$$

□

**Lemma A.5.** *(1) If $P_0 \preceq P_1$, then $\mathrm{FN}(P_0) \supseteq \mathrm{FN}(P_1)$.*
*(2) If $P_0 \simeq P_1$, then $\mathrm{FN}(P_0) = \mathrm{FN}(P_1)$.*

*Proof.* It suffices to show (1). We see (1) by induction on the construction of $P_0 \preceq P_1$. □

**Proposition A.6.** *If $(P, L) \longrightarrow \left(\hat{P}, \hat{L}\right)$, then either*

*(1) $P \preceq \left(\nu\tilde{x} : \tilde{\xi}\right) z!\tilde{v}.P_0 \mid z?\tilde{y}.P_1 \mid P_2$, $\left(\nu\tilde{x} : \tilde{\xi}\right) P_0 \mid P_1[\tilde{y} \mapsto \tilde{v}] \mid P_2 \preceq \hat{P}$ and $\hat{L} = L$, or*
*(2) $P \preceq \left(\nu\tilde{x} : \tilde{\xi}\right)\left(\tilde{l_0} < \nu l < \tilde{l_1}\right) P_0 \mid P_1$, $\left(\nu\tilde{x} : \tilde{\xi}\right) P_0 \mid P_1 \preceq \hat{P}$ and $\hat{L} = \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$.*

*Proof.* By induction on the construction of $(P, L) \longrightarrow \left(\hat{P}, \hat{L}\right)$. □

## Appendix B.
## Basic properties of usages

### B.1. Propositions for usages

**Lemma B.1.** *Let $U$, $U_0$, and $U_1$ be usages. Let $\alpha \in \{I, O\}$. Let $F$ be a partial mapping from usage variables to obligation levels.*
*(1) If $\mathrm{cap}_\alpha(U_0) \leq \mathrm{cap}_\alpha(U_1)$, then $\mathrm{cap}_\alpha(U[\rho \mapsto U_0]) \leq \mathrm{cap}_\alpha(U[\rho \mapsto U_1])$.*
*(2) If $\mathrm{cap}_\alpha(U_0) = \mathrm{cap}_\alpha(U_1)$, then $\mathrm{cap}_\alpha(U[\rho \mapsto U_0]) = \mathrm{cap}_\alpha(U[\rho \mapsto U_1])$.*
*(3) If $\mathrm{ob}_\alpha(U_0) \geq \mathrm{ob}_\alpha(U_1)$, then $\mathrm{ob}_\alpha(U[\rho \mapsto U_0]) \geq \mathrm{ob}_\alpha(U[\rho \mapsto U_1])$.*
*(4) If $\mathrm{ob}_\alpha(U_0) = \mathrm{ob}_\alpha(U_1)$, then $\mathrm{ob}_\alpha(U[\rho \mapsto U_0]) = \mathrm{ob}_\alpha(U[\rho \mapsto U_1])$.*

*Proof.* (1) By induction on the construction of $U$.
(2) By induction on the construction of $U$.
(3) By induction on the construction of $U$.
(4) By induction on the construction of $U$. □

**Lemma B.2.** *(1) If $U_0 \preceq U_0'$ and $U_1 \preceq U_1'$, then $U_0 \mid U_1 \preceq U_0' \mid U_1'$.*
*(2) $U_0 \mid (U_1 \mid U_2) \preceq (U_0 \mid U_1) \mid U_2$.*

*Proof.* We show each clause.
(1) Assume $U_0 \preceq U_0'$ and $U_1 \preceq U_1'$. By (UP-Commut) and (UP-CongP), we see

$$\begin{aligned} U_0 \mid U_1 &\preceq U_0' \mid U_1 && \text{(UP-CongP)} \\ &\preceq U_1 \mid U_0' && \text{(UP-Commut)} \\ &\preceq U_1' \mid U_0' && \text{(UP-CongP)} \\ &\preceq U_0' \mid U_1' && \text{(UP-Commut).} \end{aligned}$$

(2) By (UP-Commut), (UP-Assoc) and (UP-CongP), we see

$$\begin{aligned} U_0 \mid (U_1 \mid U_2) &\preceq (U_1 \mid U_2) \mid U_0 && \text{(UP-Commut)} \\ &\preceq (U_2 \mid U_1) \mid U_0 && \text{(UP-Commut) and (UP-CongP)} \\ &\preceq U_2 \mid (U_1 \mid U_0) && \text{(UP-Assoc)} \\ &\preceq U_2 \mid (U_0 \mid U_1) && \text{(UP-Commut) and (UP-CongP)} \\ &\preceq (U_0 \mid U_1) \mid U_2 && \text{(UP-Commut).} \end{aligned}$$

□

**Lemma B.3.** *If $U \preceq U'$, then $\mathrm{cap}_\alpha(U) \leq \mathrm{cap}_\alpha(U')$ and $\mathrm{ob}_\alpha(U) \geq \mathrm{ob}_\alpha(U')$ for $\alpha \in \{I, O\}$ and a partial mapping $F$ from usage variables to obligation levels.*

*Proof.* We show the claim by induction on the construction of $U \preceq U'$. We consider cases according to the clauses of the definition.
Case 1. If $U = U'$, then we have the claimed result obviously.
Case 2. Assume $U \preceq U''$ and $U'' \preceq U'$. By the induction hypothesis, $\mathrm{cap}_\alpha(U) \leq \mathrm{cap}_\alpha(U'')$, $\mathrm{ob}_\alpha(U) \geq \mathrm{ob}_\alpha(U'')$, $\mathrm{cap}_\alpha(U'') \leq \mathrm{cap}_\alpha(U')$, and $\mathrm{ob}_\alpha(U'') \geq \mathrm{ob}_\alpha(U')$. Then, we have $\mathrm{cap}_\alpha(U) \leq \mathrm{cap}_\alpha(U')$ and $\mathrm{ob}_\alpha(U) \geq \mathrm{ob}_\alpha(U')$.
Case 3. (UP-Zero). Assume $U = \mathtt{0} \mid U_1$ and $U' = U_1$. Then

$$\mathrm{cap}_\alpha(U) = \mathrm{cap}_\alpha(\mathtt{0} \mid U_1) = \min(\mathrm{cap}_\alpha(\mathtt{0}), \mathrm{cap}_\alpha(U_1)) = \min(\infty, \mathrm{cap}_\alpha(U_1)) = \mathrm{cap}_\alpha(U_1) = \mathrm{cap}_\alpha(U')$$

and

$$\mathrm{ob}_\alpha(U) = \mathrm{ob}_\alpha(\mathtt{0} \mid U_1) = \min(\mathrm{ob}_\alpha(\mathtt{0}), \mathrm{ob}_\alpha(U_1)) = \min(\infty, \mathrm{ob}_\alpha(U_1)) = \mathrm{ob}_\alpha(U_1) = \mathrm{ob}_\alpha(U').$$

Case 4. (UP-Commut). Assume $U = U_1 \mid U_2$ and $U' = U_2 \mid U_1$. Then

$$\mathrm{cap}_\alpha(U) = \mathrm{cap}_\alpha(U_1 \mid U_2) = \min(\mathrm{cap}_\alpha(U_1), \mathrm{cap}_\alpha(U_2)) = \mathrm{cap}_\alpha(U_2 \mid U_1) = \mathrm{cap}_\alpha(U')$$

and

$$\mathrm{ob}_\alpha(U) = \mathrm{ob}_\alpha(U_1 \mid U_2) = \min(\mathrm{ob}_\alpha(U_1), \mathrm{ob}_\alpha(U_2)) = \mathrm{ob}_\alpha(U_2 \mid U_1) = \mathrm{ob}_\alpha(U').$$

Case 5. (UP-Assoc). Assume $U = (U_1 \mid U_2) \mid U_3$ and $U' = U_1 \mid (U_2 \mid U_3)$. Then

$$\begin{aligned}
\mathrm{cap}_\alpha(U) &= \mathrm{cap}_\alpha((U_1 \mid U_2) \mid U_3) \\
&= \min(\mathrm{cap}_\alpha(U_1 \mid U_2), \mathrm{cap}_\alpha(U_3)) \\
&= \min(\min(\mathrm{cap}_\alpha(U_1), \mathrm{cap}_\alpha(U_2)), \mathrm{cap}_\alpha(U_3)) \\
&= \min(\mathrm{cap}_\alpha(U_1), \mathrm{cap}_\alpha(U_2), \mathrm{cap}_\alpha(U_3)) \\
&= \min(\mathrm{cap}_\alpha(U_1), \min(\mathrm{cap}_\alpha(U_2), \mathrm{cap}_\alpha(U_3))) \\
&= \min(\mathrm{cap}_\alpha(\mathrm{cap}_\alpha(U_1), U_2 \mid U_3)) \\
&= \mathrm{cap}_\alpha(U_1 \mid (U_2 \mid U_3)) \\
&= \mathrm{cap}_\alpha(U')
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{ob}_\alpha(U) &= \mathrm{ob}_\alpha((U_1 \mid U_2) \mid U_3) \\
&= \min(\mathrm{ob}_\alpha(U_1 \mid U_2), \mathrm{ob}_\alpha(U_3)) \\
&= \min(\mathrm{ob}_\alpha(U_1), \mathrm{ob}_\alpha(U_2), \mathrm{ob}_\alpha(U_3)) \\
&= \min(\mathrm{ob}_\alpha(U_1), \mathrm{ob}_\alpha(U_2 \mid U_3)) \\
&= \mathrm{ob}_\alpha(U_1 \mid (U_2 \mid U_3)) \\
&= \mathrm{ob}_\alpha(U').
\end{aligned}$$

Case 6. (UP-CongP). Assume $U_1 \preceq U_1'$. We also assume $U = U_1 \mid U_2$ and $U' = U_1' \mid U_2$. By the induction hypothesis, we have $\mathrm{cap}_\alpha(U_1) \leq \mathrm{cap}_\alpha(U_1')$ and $\mathrm{ob}_\alpha(U_1) \geq \mathrm{ob}_\alpha(U_1')$. Then

$$\begin{aligned}
\mathrm{cap}_\alpha(U) &= \mathrm{cap}_\alpha(U_1 \mid U_2) \\
&= \min(\mathrm{cap}_\alpha(U_1), \mathrm{cap}_\alpha(U_2)) \\
&\leq \min(\mathrm{cap}_\alpha(U_1'), \mathrm{cap}_\alpha(U_2)) \\
&= \mathrm{cap}_\alpha(U_1' \mid U_2) \\
&= \mathrm{cap}_\alpha(U')
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{ob}_\alpha(U) &= \mathrm{ob}_\alpha(U_1 \mid U_2) \\
&= \min(\mathrm{ob}_\alpha(U_1), \mathrm{ob}_\alpha(U_2)) \\
&\geq \min(\mathrm{ob}_\alpha(U_1'), \mathrm{ob}_\alpha(U_2)) \\
&= \mathrm{ob}_\alpha(U_1' \mid U_2) \\
&= \mathrm{ob}_\alpha(U').
\end{aligned}$$

Case 7. (UP-Rep). Assume $U = *U_0$ and $U' = *U_0 \mid U_0$. Then

$$\begin{aligned}
\mathrm{cap}_\alpha(U') &= \mathrm{cap}_\alpha(*U_0 \mid U_0) \\
&= \min(\mathrm{cap}_\alpha(*U_0), \mathrm{cap}_\alpha(U_0)) \\
&= \mathrm{cap}_\alpha(*U_0) \\
&= \mathrm{cap}_\alpha(U)
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{ob}_\alpha(U') &= \mathrm{ob}_\alpha(*U_0 \mid U_0) \\
&= \min(\mathrm{ob}_\alpha(*U_0), \mathrm{ob}_\alpha(U_0)) \\
&= \mathrm{ob}_\alpha(*U_0) \\
&= \mathrm{ob}_\alpha(U).
\end{aligned}$$

Case 8. (UP-$\uparrow^{(*,*)}$). Assume $U = \uparrow^{(t_I, t_O)} \beta_{t_2}^{t_1}.U_0$ and $U' = \beta_{t_2}^{\max(t_1, t_\alpha)}.U_0$.

Assume $\beta = \alpha$.

$$\mathrm{cap}_\alpha(U) = \mathrm{cap}_\alpha\Big(\uparrow^{(t_I, t_O)} \beta_{t_2}^{t_1}.U_0\Big)$$

$$
\begin{aligned}
&= \mathrm{cap}_\alpha\big(\beta^{t_1}_{t_2}.U_0\big)\\
&= t_2\\
&= \mathrm{cap}_\alpha\Big(\beta^{\max(t_1,t_\alpha)}_{t_2}.U_0\Big)\\
&= \mathrm{cap}_\alpha(U')
\end{aligned}
$$

and

$$
\begin{aligned}
\mathrm{ob}_\alpha(U) &= \mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)}\beta^{t_1}_{t_2}.U_0\Big)\\
&= \max\big(t_\alpha, \mathrm{ob}_\alpha\big(\beta^{t_1}_{t_2}.U_0\big)\big)\\
&= \max(t_\alpha, t_1)\\
&= \mathrm{ob}_\alpha\Big(\beta^{\max(t_1,t_\alpha)}_{t_2}.U_0\Big)\\
&= \mathrm{ob}_\alpha(U').
\end{aligned}
$$

Assume $\beta = \overline{\alpha}$.

$$
\begin{aligned}
\mathrm{cap}_\alpha(U) &= \mathrm{cap}_\alpha\Big(\uparrow^{(t_I,t_O)}\beta^{t_1}_{t_2}.U_0\Big)\\
&= \mathrm{cap}_\alpha\big(\beta^{t_1}_{t_2}.U_0\big)\\
&= \infty\\
&= \mathrm{cap}_\alpha\Big(\beta^{\max(t_1,t_\alpha)}_{t_2}.U_0\Big)\\
&= \mathrm{cap}_\alpha(U')
\end{aligned}
$$

and

$$
\begin{aligned}
\mathrm{ob}_\alpha(U) &= \mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)}\beta^{t_1}_{t_2}.U_0\Big)\\
&= \max\big(t_\alpha, \mathrm{ob}_\alpha\big(\beta^{t_1}_{t_2}.U_0\big)\big)\\
&= \max(t_\alpha, \infty)\\
&= \mathrm{ob}_\alpha\Big(\beta^{\max(t_1,t_\alpha)}_{t_2}.U_0\Big)\\
&= \mathrm{ob}_\alpha(U').
\end{aligned}
$$

Case 9. (UP-DIST). Assume $U = \uparrow^{(t_I,t_O)} U_1 \mid U_2$ and $U' = \uparrow^{(t_I,t_O)} U_1 \mid \uparrow^{(t_I,t_O)} U_2$. Then

$$
\begin{aligned}
\mathrm{cap}_\alpha(U) &= \mathrm{cap}_\alpha\Big(\uparrow^{(t_I,t_O)} U_1 \mid U_2\Big)\\
&= \mathrm{cap}_\alpha(U_1 \mid U_2)\\
&= \min(\mathrm{cap}_\alpha(U_1), \mathrm{cap}_\alpha(U_2))\\
&= \min\Big(\mathrm{cap}_\alpha\Big(\uparrow^{(t_I,t_O)} U_1\Big), \mathrm{cap}_\alpha\Big(\uparrow^{(t_I,t_O)} U_2\Big)\Big)\\
&= \mathrm{cap}_\alpha\Big(\uparrow^{(t_I,t_O)} U_1 \mid \uparrow^{(t_I,t_O)} U_2\Big)\\
&= \mathrm{cap}_\alpha(U')
\end{aligned}
$$

and

$$
\begin{aligned}
\mathrm{ob}_\alpha(U) &= \mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)} U_1 \mid U_2\Big)\\
&= \max(t_\alpha, \mathrm{ob}_\alpha(U_1 \mid U_2))\\
&= \max(t_\alpha, \min(\mathrm{ob}_\alpha(U_1), \mathrm{ob}_\alpha(U_2)))\\
&\geq \min(\max(t_\alpha, \mathrm{ob}_\alpha(U_1)), \max(t_\alpha, \mathrm{ob}_\alpha(U_2)))\\
&= \min\Big(\mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)} U_1\Big), \mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)} U_2\Big)\Big)\\
&= \mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)} U_1 \mid \uparrow^{(t_I,t_O)} U_2\Big)\\
&= \mathrm{ob}_\alpha(U').
\end{aligned}
$$

Case 10. (UP-Or). Fix $i \in \{1,2\}$. Assume $U = U_1 \mathbin{\&} U_2$ and $U' = U_i$. Then

$$\begin{aligned}\mathrm{cap}_\alpha(U) &= \mathrm{cap}_\alpha(U_1 \mathbin{\&} U_2)\\ &= \min(\mathrm{cap}_\alpha(U_1), \mathrm{cap}_\alpha(U_2))\\ &\le \mathrm{cap}_\alpha(U_i)\\ &= \mathrm{cap}_\alpha(U')\end{aligned}$$

and

$$\begin{aligned}\mathrm{ob}_\alpha(U) &= \mathrm{ob}_\alpha(U_1 \mathbin{\&} U_2)\\ &= \max(\mathrm{cap}_\alpha(U_1), \mathrm{cap}_\alpha(U_2))\\ &\ge \mathrm{ob}_\alpha(U_i)\\ &= \mathrm{ob}_\alpha(U').\end{aligned}$$

Case 11. (UP-Cong $\uparrow^{(*,*)}$). Assume $U_0 \preceq U_0'$, $U = \uparrow^{(t_I,t_O)} U_0$, and $U' = \uparrow^{(t_I,t_O)} U_0'$. By the induction hypothesis, we have $\mathrm{cap}_\alpha(U_0) \le \mathrm{cap}_\alpha(U_0')$ and $\mathrm{ob}_\alpha(U_0) \ge \mathrm{ob}_\alpha(U_0')$. Then

$$\begin{aligned}\mathrm{cap}_\alpha(U) &= \mathrm{cap}_\alpha\Big(\uparrow^{(t_I,t_O)} U_0\Big)\\ &= \mathrm{cap}_\alpha(U_0)\\ &\le \mathrm{cap}_\alpha(U_0')\\ &= \mathrm{cap}_\alpha\Big(\uparrow^{(t_I,t_O)} U_0'\Big)\\ &= \mathrm{cap}_\alpha(U')\end{aligned}$$

and

$$\begin{aligned}\mathrm{ob}_\alpha(U) &= \mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)} U_0\Big)\\ &= \max(t_\alpha, \mathrm{ob}_\alpha(U_0))\\ &\ge \max(t_\alpha, \mathrm{ob}_\alpha(U_0'))\\ &= \mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)} U_0'\Big)\\ &= \mathrm{ob}_\alpha(U').\end{aligned}$$

Case 12. (UP-Commut $\uparrow^{(*,*)}$). Assume $U = \uparrow^{(t_I,t_O)} \uparrow^{(t_I',t_O')} U_0$ and $U' = \uparrow^{(t_I',t_O')} \uparrow^{(t_I,t_O)} U_0$. Then

$$\begin{aligned}\mathrm{cap}_\alpha(U) &= \mathrm{cap}_\alpha\Big(\uparrow^{(t_I,t_O)} \uparrow^{(t_I',t_O')} U_0\Big)\\ &= \mathrm{cap}_\alpha\Big(\uparrow^{(t_I',t_O')} U_0\Big)\\ &= \mathrm{cap}_\alpha(U_0)\\ &= \mathrm{cap}_\alpha\Big(\uparrow^{(t_I,t_O)} U_0\Big)\\ &= \mathrm{cap}_\alpha\Big(\uparrow^{(t_I',t_O')} \uparrow^{(t_I,t_O)} U_0\Big)\\ &= \mathrm{cap}_\alpha(U')\end{aligned}$$

and

$$\begin{aligned}\mathrm{ob}_\alpha(U) &= \mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)} \uparrow^{(t_I',t_O')} U_0\Big)\\ &= \max\Big(t_\alpha, \mathrm{ob}_\alpha\Big(\uparrow^{(t_I',t_O')} U_0\Big)\Big)\\ &= \max(t_\alpha, \max(t_\alpha', \mathrm{ob}_\alpha(U_0)))\\ &= \max(t_\alpha', \max(t_\alpha, \mathrm{ob}_\alpha(U_0)))\\ &= \max\Big(t_\alpha', \mathrm{ob}_\alpha\Big(\uparrow^{(t_I,t_O)} U_0\Big)\Big)\\ &= \mathrm{ob}_\alpha\Big(\uparrow^{(t_I',t_O')} \uparrow^{(t_I,t_O)} U_0\Big)\end{aligned}$$

$$= \mathrm{ob}_\alpha(U').$$

□

## B.2. Proof of Proposition 3.8

We show each claim.
(1) Let $U_0$ and $U_1$ usages. Assume $U_0 <: U_1$ and $\mathrm{con}_\alpha(U_0)$. By Definition 3.7 (c), we have $\mathrm{cap}_\alpha(U_0) \leq \mathrm{cap}_\alpha(U_1)$. By Definition 3.7 (d), we have $\mathrm{ob}_{\overline{\alpha}}(U_0) \geq \mathrm{ob}_{\overline{\alpha}}(U_1)$. By Definition 3.6, we have $\mathrm{ob}_{\overline{\alpha}}(U_0) \leq \mathrm{cap}_\alpha(U_0)$. Then $\mathrm{ob}_{\overline{\alpha}}(U_1) \leq \mathrm{ob}_{\overline{\alpha}}(U_0) \leq \mathrm{cap}_\alpha(U_0) \leq \mathrm{cap}_\alpha(U_1)$. Thus, $\mathrm{con}_\alpha(U_1)$.
(2) Let $U_0$ and $U_1$ usages. Assume $U_0 <: U_1$ and $\mathrm{rel}(U_0)$. Fix a usage $U_1'$, where $U_1 \longrightarrow\!\!\!\!\!\rightarrow U_1'$. By induction and Definition 3.7 (b), we see that there exists a usage $U_0'$ such that $U_0 \longrightarrow\!\!\!\!\!\rightarrow U_0'$ and $U_0' <: U_1'$. Since $\mathrm{rel}(U_0)$, we have $\mathrm{con}(U_0')$. By (1) in this proposition, we have $\mathrm{con}(U_1')$. Thus, $\mathrm{rel}(U_1)$.
(3) Since it is obvious that the identity relation on closed usages satisfies all the conditions of Definition 3.7, we have the reflexivity of the subusage relation.

We show the transitivity of the subusage relation. Let

$$R = \left\{ (U_0, U_1) \;\middle|\; \begin{array}{c} U_0 <: U_1, \text{ or} \\ \text{there exits } U_2 \text{ such that} \\ U_0 <: U_2 \text{ and } U_2 <: U_1 \end{array} \right\}.$$

It suffices to show that $R$ satisfies all the conditions of Definition 3.7.

Assume $(U_0, U_1) \in R$. Then, either $U_0 <: U_1$, or there exits $U_2$ such that $U_0 <: U_2$ and $U_2 <: U_1$. If $U_0 <: U_1$, then all the conditions of Definition 3.7 hold by Definition 3.7. Assume $U_0 <: U_2$ and $U_2 <: U_1$.
(a) Fix a usage $U$, where $\mathrm{FV}(U) = \{\rho\}$. By Definition 3.7 (a), we have $U[\rho \mapsto U_0] <: U[\rho \mapsto U_2]$ and $U[\rho \mapsto U_2] <: U[\rho \mapsto U_1]$. Then, we have $(U[\rho \mapsto U_0], U[\rho \mapsto U_1]) \in R$.
(b) Assume $U_1 \longrightarrow U_1'$. By Definition 3.7 (b), there exists $U_2'$ such that $U_2 \longrightarrow U_2'$ and $U_2' <: U_1'$. By Definition 3.7 (b), there exists $U_0'$ such that $U_0 \longrightarrow U_0'$ and $U_0' <: U_2'$. Then, we see that there exists $U_0'$ such that $U_0 \longrightarrow U_0'$ and $(U_0', U_1') \in R$.
(c) By Definition 3.7 (c), we have $\mathrm{cap}_\alpha(U_0) \leq \mathrm{cap}_\alpha(U_2)$ and $\mathrm{cap}_\alpha(U_2) \leq \mathrm{cap}_\alpha(U_1)$, for each $\alpha \in \{I, O\}$. Then, we have $\mathrm{cap}_\alpha(U_0) \leq \mathrm{cap}_\alpha(U_1)$, for each $\alpha \in \{I, O\}$.
(d) Fix $\alpha \in \{I, O\}$. Assume $\mathrm{con}_{\overline{\alpha}}(U_0)$. By Proposition 3.8 (1), we have $\mathrm{con}_{\overline{\alpha}}(U_2)$. Then, by Definition 3.7 (d), we have $\mathrm{ob}_\alpha(U_0) \geq \mathrm{ob}_\alpha(U_2)$ and $\mathrm{ob}_\alpha(U_2) \geq \mathrm{ob}_\alpha(U_1)$. Thus, $\mathrm{ob}_\alpha(U_0) \geq \mathrm{ob}_\alpha(U_1)$. □

## B.3. Property of subusages

**Proposition B.4.** *(1) For closed usages $U$ and $U'$, if $U \preceq U'$, then $U <: U'$.*
*(2) For closed usages $U$, if $\mathrm{ob}(U) = \infty$, $U <: \mathtt{0}$.*
*(3) For closed usages $U$ and $U'$, if $\mathrm{ob}(U) = \infty$, then $U \mid U' <: U'$.*
*(4) Let $U_0$ and $U_1$ be closed usages. Then $(*U_0 \mid *U_1) <: *(U_0 \mid U_1)$.*
*(5) Let $U_0, \ldots, U_n$ be closed usages. Then $(*U_0 \mid \cdots \mid *U_n) <: *(U_0 \mid \cdots \mid U_n)$.*
*(6) For usages $U_0$, $U_1$, $U_0'$, and $U_1'$, if $U_0 <: U_0'$ and $U_1 <: U_1'$, then $U_0 \mid U_1 <: U_0' \mid U_1'$.*
*(7) $\uparrow^{(t_o, t_c)} U <: U$ for a usage $U$ and $t_o, t_c \in \mathbb{N} \cup \{\infty\}$.*
*(8) $\uparrow U <: U$ for a usage $U$.*

*Proof.* We show each claim of Proposition B.4.
(1) For closed usages $U$ and $U'$ with $U \preceq U'$, let

$$R_1^{(U,U')} = \{(U_0[\rho \mapsto U], U_0[\rho \mapsto U']) \mid U_0 \text{ is a usage with } \mathrm{FV}(U_0) \subseteq \{\rho\}\}.$$

It suffices to show that $R_1^{(U,U')}$ satisfies all the conditions of Definition 3.7.

Fix closed usages $U$ and $U'$ with $U \preceq U'$. Assume $(U_0[\rho \mapsto U], U_0[\rho \mapsto U']) \in R_1^{(U,U')}$.
(a) Let $U_0'$ be a usage with $\mathrm{FV}(U_0') = \{\rho'\}$. Since $\mathrm{FV}(U_0) \subseteq \{\rho\}$ and $\mathrm{FV}(U_0') = \{\rho'\}$, we have $U_0'[\rho' \mapsto (U_0[\rho \mapsto U])] = (U_0'[\rho' \mapsto U_0])[\rho \mapsto U]$ and $U_0'[\rho' \mapsto (U_0[\rho \mapsto U'])] = (U_0'[\rho' \mapsto U_0])[\rho \mapsto U']$. Hence, $(U_0'[\rho' \mapsto (U_0[\rho \mapsto U])], U_0'[\rho' \mapsto (U_0[\rho \mapsto U'])]) \in R_1^{(U,U')}$.
(b) To show that $R_1^{(U,U')}$ satisfies Definition 3.7 (b), we show that if $(U_0[\rho \mapsto U], U_0[\rho \mapsto U']) \in R_1^{(U,U')}$, and $U_0[\rho \mapsto U'] \preceq \hat{V}$, then there exists a closed usage $\check{V}$ such that $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $(U_0[\rho \mapsto U], U_0[\rho \mapsto U']) \in R_1^{(U,U')}$ and $U_0[\rho \mapsto U'] \preceq \hat{V}$. We show that there exists a closed usage $\check{V}$ such that $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$. The proof is by induction on the construction of $U_0[\rho \mapsto U] \preceq \hat{V}$.

Assume $U_0 = \rho$. Then, we have $U_0[\rho \mapsto U'] = U'$. Since $U \preceq U'$ and $U' \preceq \hat{V}$, we have $U \preceq \hat{V}$. Let $\check{V} = \hat{V}$. Then, we see that $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$ if $\check{V} = \hat{V}$.

We consider other cases according to the last rule of the construction of $U_0[\rho \mapsto U] \preceq \hat{V}$.

Case 1. Assume $\hat{V} = U_0[\rho \mapsto U']$. Let $\check{V} = U_0[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 2. Assume that there exists $\hat{V}'$ such that $U_0[\rho \mapsto U'] \preceq \hat{V}'$ and $\hat{V}' \preceq \hat{V}$. By the induction hypothesis, there exists a closed usage $\check{V}'$ such that $U_0[\rho \mapsto U] \preceq \check{V}'$ and $\left(\check{V}', \hat{V}'\right) \in R_1^{(U,U')}$. Since $\left(\check{V}', \hat{V}'\right) \in R_1^{(U,U')}$ and $\hat{V}' \preceq \hat{V}$, the induction hypothesis implies that there exists a closed usage $\check{V}$ such that $\check{V}' \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$. Since $U_0[\rho \mapsto U] \preceq \check{V}'$, we have $U_0[\rho \mapsto U] \preceq \check{V}$.

Case 3. (UP-Zero). Assume $U_0 = \mathtt{0} \mid U_1$ and $\hat{V} = U_1[\rho \mapsto U']$. Let $\check{V} = U_1[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 4. (UP-Commut). Assume $U_0 = U_1 \mid U_2$ and $\hat{V} = U_2[\rho \mapsto U'] \mid U_1[\rho \mapsto U']$. Let $\check{V} = U_2[\rho \mapsto U] \mid U_1[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 5. (UP-Assoc). Assume $U_0 = \rho \mid U_3$, $U' = U_1 \mid U_2$ and $\hat{V} = U_1 \mid (U_2 \mid U_3[\rho \mapsto U'])$. Then $U_0[\rho \mapsto U] = U \mid U_3[\rho \mapsto U]$. By (UP-CongP) and transitivity, we have

$$U \mid U_3[\rho \mapsto U] \preceq (U_1 \mid U_2) \mid U_3[\rho \mapsto U] \preceq U_1 \mid (U_2 \mid U_3[\rho \mapsto U]).$$

Let $\check{V} = U_1 \mid (U_2 \mid U_3[\rho \mapsto U'])$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $U_0 = (U_1 \mid U_2) \mid U_3$ and $\hat{V} = U_1[\rho \mapsto U'] \mid (U_2[\rho \mapsto U'] \mid U_3[\rho \mapsto U'])$. Let $\check{V} = U_1[\rho \mapsto U] \mid (U_2[\rho \mapsto U] \mid U_3[\rho \mapsto U])$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 6. (UP-CongP). Assume $U_0 = U_1 \mid U_2$, $U_1[\rho \mapsto U'] \preceq \hat{V}_1$, and $\hat{V} = \hat{V}_1 \mid U_2[\rho \mapsto U']$. Then, we have $(U_1[\rho \mapsto U], U_1[\rho \mapsto U']) \in R_1^{(U,U')}$. By the induction hypothesis, there exists a usage $\check{V}_1$ such that $U_1[\rho \mapsto U] \preceq \check{V}_1$ and $\left(\check{V}_1, \hat{V}_1\right) \in R_1^{(U,U')}$. Since $\left(\check{V}_1, \hat{V}_1\right) \in R_1^{(U,U')}$, there exists a usage $U_1'$ such that $\mathrm{FV}(U_1') \subseteq \{\rho\}$, $\check{V}_1 = U_1'[\rho \mapsto U]$, and $\hat{V}_1 = U_1'[\rho \mapsto U']$. Let $\check{V} = U_1'[\rho \mapsto U] \mid U_2[\rho \mapsto U]$. Then, we have $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$. By (UP-CongP) and transitivity, we see

$$U_1[\rho \mapsto U] \mid U_2[\rho \mapsto U] \preceq U_1'[\rho \mapsto U] \mid U_2[\rho \mapsto U].$$

Case 7. (UP-Rep). Assume $U_0 = *U_1$ and $\hat{V} = *U_1[\rho \mapsto U'] \mid U_1[\rho \mapsto U']$. Let $\check{V} = *U_1[\rho \mapsto U] \mid U_1[\rho \mapsto U']$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 8. (UP-$\uparrow^{(*,*)}$). Assume $U_0 = \uparrow^{(t_I,t_O)} \rho$, $U' = \alpha_{t_2}^{t_1}.U_1$, and $\hat{V} = \alpha_{t_2}^{\max(t_1,t_\alpha)}.U_1$. Since $U \preceq U'$, we have either $U = U'$ or $U = \uparrow^{(t_I',t_O')} \alpha_{t_2}^{t_1'}.U_1$ with $t_1 = \max(t_1', t_\alpha')$.

Assume $U = U'$. Let $\check{V} = \hat{V}$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $U = \uparrow^{(t_I',t_O')} \alpha_{t_2}^{t_1'}.U_1$ with $t_1 = \max(t_1', t_\alpha')$. By (UP-Cong $\uparrow^{(*,*)}$) and transitivity, we have

$$\uparrow^{(t_I,t_O)} \uparrow^{(t_I',t_O')} \alpha_{t_2}^{t_1'}.U_1 \preceq \uparrow^{(t_I,t_O)} \alpha_{t_2}^{t_1}.U_1 \preceq \alpha_{t_2}^{\max(t_1,t_\alpha)}.U_1.$$

Let $\check{V} = \hat{V}$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $U_0 = \uparrow^{(t_I,t_O)} \alpha_{t_2}^{t_1}.U_1$ and $\hat{V} = \alpha_{t_2}^{\max(t_1,t_\alpha)}.U_1[\rho \mapsto U']$. Let $\check{V} = \alpha_{t_2}^{\max(t_1,t_\alpha)}.U_1[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 9. (UP-Dist). Assume $U_0 = \uparrow^{(t_I,t_O)} \rho$, $U' = U_1 \mid U_2$, and $\hat{V} = \uparrow^{(t_I,t_O)} U_1 \mid \uparrow^{(t_I,t_O)} U_2$. By (UP-Cong $\uparrow^{(*,*)}$) and transitivity,

$$\uparrow^{(t_I,t_O)} U \preceq \uparrow^{(t_I,t_O)} U' \preceq \uparrow^{(t_I,t_O)} U_1 \mid \uparrow^{(t_I,t_O)} U_2.$$

Let $\check{V} = \hat{V}$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $U_0 = \uparrow^{(t_I,t_O)} U_1 \mid U_2$ and $\hat{V} = \uparrow^{(t_I,t_O)} U_1[\rho \mapsto U'] \mid \uparrow^{(t_I,t_O)} U_2[\rho \mapsto U']$. Let $\check{V} = \uparrow^{(t_I,t_O)} U_1[\rho \mapsto U] \mid \uparrow^{(t_I,t_O)} U_2[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 10. (UP-Or). Fix $i \in \{1,2\}$. Assume $U_0 = U_1 \,\&\, U_2$ and $\hat{V} = U_i[\rho \mapsto U']$. Let $\check{V} = U_i[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 11. (UP-Cong $\uparrow^{(*,*)}$). Assume $U_0 = \uparrow^{(t_I,t_O)} \rho$, $U' \preceq U''$, and $\hat{V} = \uparrow^{(t_I,t_O)} U''$. By (UP-Cong $\uparrow^{(*,*)}$) and transitivity, we have

$$\uparrow^{(t_I,t_O)} U \preceq \uparrow^{(t_I,t_O)} U' \preceq \uparrow^{(t_I,t_O)} U''.$$

Assume $U_0 = \uparrow^{(t_I,t_O)} U_1$, $U_1[\rho \mapsto U'] \preceq \hat{V}_1$, and $\hat{V} = \uparrow^{(t_I,t_O)} \hat{V}_1$. By the induction hypothesis, there exists a usage $\check{V}_1$ such that $U_1[\rho \mapsto U] \preceq \check{V}_1$ and $\left(\check{V}_1, \hat{V}_1\right) \in R_1^{(U,U')}$. By (UP-Cong $\uparrow^{(*,*)}$), we have

$$\uparrow^{(t_I,t_O)} U_1[\rho \mapsto U] \preceq \uparrow^{(t_I,t_O)} \check{V}_1.$$

Let $\check{V} = \uparrow^{(t_I,t_O)} \check{V}_1$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 12. (UP-Commut $\uparrow^{(*,*)}$). Assume $U_0 = \uparrow^{(t_I,t_O)} \rho$, $U' = \uparrow^{(t'_I,t'_O)} U_1$, and $\hat{V} = \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} U_1$. Let $\check{V} = \hat{V}$. Then $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$. By (UP-Cong $\uparrow^{(*,*)}$), we have

$$U_0[\rho \mapsto U] = \uparrow^{(t_I,t_O)} U \preceq \uparrow^{(t_I,t_O)} U' \preceq \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} U_1 = \check{V}.$$

Hence, $U_0[\rho \mapsto U] \preceq \check{V}$.

Assume $U_0 = \uparrow^{(t_I,t_O)} \uparrow^{(t'_I,t'_O)} U_1$ and $\hat{V} = \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} U_1[\rho \mapsto U']$. Let $\check{V} = \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} U_1[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Now, we show that if $(U_0[\rho \mapsto U], U_0[\rho \mapsto U']) \in R_1^{(U,U')}$ and there exists a closed usage $\hat{V}$ such that $U_0[\rho \mapsto U'] \longrightarrow \hat{V}$, then there exists a usage $\check{V}$ such that $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $(U_0[\rho \mapsto U], U_0[\rho \mapsto U']) \in R_1^{(U,U')}$ and $U_0[\rho \mapsto U'] \longrightarrow \hat{V}$. We show that there exists a usage $\check{V}$ such that $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$. We show the claim by induction on the construction of $U_0[\rho \mapsto U'] \longrightarrow \hat{V}$.

Assume $U_0 = \rho$. Then, we have $U_0[\rho \mapsto U'] = U'$ and $U_0[\rho \mapsto U] = U$. Then, we see

$$U \preceq U' \longrightarrow \hat{V}$$

Let $\check{V} = \hat{V}$. Then, we see that $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$ if $\check{V} = \hat{V}$.

We consider other cases according to the last rule of the construction of $U_0[\rho \mapsto U'] \longrightarrow \hat{V}$.

Case 1. Assume $U_0 = \rho \mid O_{t_c}^{t'_o}.U_2$, $U' = I_{t_c}^{t_o}.U_1$, and $\hat{V} = U_1 \mid U_2[\rho \mapsto U']$.

Since $U \preceq U'$, we have either $U = U'$ or $U = \uparrow^{(t''_I,t''_O)} I_{t_c}^{t_1}.U_1$ with $t_o = \max(t_1, t''_I)$.

Assume $U = U'$. Let $\check{V} = \hat{V}$. Then, we have $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $U = \uparrow^{(t''_I,t''_O)} I_{t_c}^{t_1}.U_1$ with $t_o = \max(t_1, t''_I)$. By (UP-$\uparrow^{(*,*)}$), we have

$$\uparrow^{(t''_I,t''_O)} I_{t_c}^{t_1}.U_1 \mid O_{t_c}^{t'_o}.U_2[\rho \mapsto U] \preceq I_{t_c}^{t_o}.U_1 \mid O_{t_c}^{t'_o}.U_2[\rho \mapsto U] \longrightarrow U_1 \mid U_2[\rho \mapsto U].$$

Let $\check{V} = U_1 \mid U_2[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $U_0 = I_{t_c}^{t_o}.U_1 \mid \rho$, $U' = O_{t_c}^{t'_o}.U_2$, and $\hat{V} = U_1[\rho \mapsto U'] \mid U_2$.

Since $U \preceq U'$, we have either $U = U'$ or $U = \uparrow^{(t''_I,t''_O)} O_{t_c}^{t_1}.U_1$ with $t'_o = \max(t_1, t''_O)$.

Assume $U = U'$. Let $\check{V} = \hat{V}$. Then, we have $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $U = \uparrow^{(t''_I,t''_O)} O_{t_c}^{t_1}.U_1$ with $t'_o = \max(t_1, t''_O)$. By (UP-Commut) and (UP-$\uparrow^{(*,*)}$), we have

$$\begin{aligned} I_{t_c}^{t_o}.U_1[\rho \mapsto U] \mid \uparrow^{(t''_I,t''_O)} O_{t_c}^{t_1}.U_2 &\preceq \uparrow^{(t''_I,t''_O)} O_{t_c}^{t_1}.U_2 \mid I_{t_c}^{t_o}.U_1[\rho \mapsto U] \\ &\preceq O_{t_c}^{t'_o}.U_2 \mid I_{t_c}^{t_o}.U_1[\rho \mapsto U] \\ &\preceq I_{t_c}^{t_o}.U_1[\rho \mapsto U] \mid O_{t_c}^{t'_o}.U_2 \\ &\longrightarrow U_1[\rho \mapsto U] \mid U_2. \end{aligned}$$

Let $\check{V} = U_1[\rho \mapsto U] \mid U_2$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Assume $U_0 = I^{t_o}_{t_c}.U_1 \mid O^{t'_o}_{t'_c}.U_2$ and $\hat{V} = U_1[\rho \mapsto U'] \mid U_2[\rho \mapsto U']$. Let $\check{V} = U_1[\rho \mapsto U] \mid U_2[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 2. Assume $U_0 = U_1 \mid U_2$, $U_1[\rho \mapsto U'] \longrightarrow \hat{V}_1$, and $\hat{V} = \hat{V}_1 \mid U_2[\rho \mapsto U']$. By the induction hypothesis, there exists a usage $\check{V}_1$ such that $U_1[\rho \mapsto U] \longrightarrow \check{V}_1$ and $\left(\check{V}_1, \hat{V}_1\right) \in R_1^{(U,U')}$. Let $\check{V} = \check{V}_1 \mid U_2[\rho \mapsto U]$. Since $\left(\check{V}_1, \hat{V}_1\right) \in R_1^{(U,U')}$, there exists a usage $U'_1$ such that $\mathrm{FV}(U'_1) \subseteq \{\rho\}$, $\check{V}_1 = U'_1[\rho \mapsto U]$, and $\hat{V}_1 = U'_1[\rho \mapsto U']$. Hence, we see $\check{V} = U'_1[\rho \mapsto U] \mid U_2[\rho \mapsto U]$ and $\hat{V} = U'_1[\rho \mapsto U'] \mid U_2[\rho \mapsto U']$. Then, we have $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$.

Case 3. Assume that there exist usages $\hat{V}_1$ and $\hat{V}_2$ such that $U_0[\rho \mapsto U'] \preceq \hat{V}_1$, $\hat{V}_1 \longrightarrow \hat{V}_2$, and $\hat{V}_2 \preceq \hat{V}$. Since $(U_0[\rho \mapsto U], U_0[\rho \mapsto U']) \in R_1^{(U,U')}$ and $U_0[\rho \mapsto U'] \preceq \hat{V}_1$, there exists a closed usage $\check{V}_1$ such that $U_0[\rho \mapsto U] \preceq \check{V}_1$ and $\left(\check{V}_1, \hat{V}_1\right) \in R_1^{(U,U')}$. By the induction hypothesis, there exists a closed usage $\check{V}_2$ such that $\check{V}_1 \longrightarrow \check{V}_2$ and $\left(\check{V}_2, \hat{V}_2\right) \in R_1^{(U,U')}$. Since $\left(\check{V}_2, \hat{V}_2\right) \in R_1^{(U,U')}$ and $\hat{V}_2 \preceq \hat{V}$, there exists a closed usage $\check{V}$ such that $\check{V}_2 \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_1^{(U,U')}$. Since $U_0[\rho \mapsto U] \preceq \check{V}_1$, $\check{V}_1 \longrightarrow \check{V}_2$, and $\check{V}_2 \preceq \check{V}$, we have $U_0[\rho \mapsto U] \longrightarrow \check{V}$.

(c) By Lemma B.1 (1) and Lemma B.3.

(d) By Lemma B.1 (3) and Lemma B.3.

(2) For a closed usage $U$ with $\mathrm{ob}(U) = \infty$, let

$$R_2^{(U)} = \{(U_0[\rho \mapsto U], U_0[\rho \mapsto \mathsf{0}]) \mid U_0 \text{ is a usage with } \mathrm{FV}(U_0) = \{\rho\}\}.$$

It suffices to show that $R_2^{(U)}$ satisfies all the conditions of Definition 3.7.

Fix a usage $U_0$ with $\mathrm{FV}(U_0) \subseteq \{\rho\}$. Fix a closed usage $U$ with $\mathrm{ob}(U) = \infty$. Assume $(U_0[\rho \mapsto U], U_0[\rho \mapsto \mathsf{0}]) \in R_2^{(U)}$.

(a) Let $U'$ be a usage with $\mathrm{FV}(U') = \{\rho'\}$. Since $\mathrm{FV}(U_0) \subseteq \{\rho\}$ and $\mathrm{FV}(U') = \{\rho'\}$, we have $U'[\rho' \mapsto (U_0[\rho \mapsto U])] = (U'[\rho' \mapsto U_0])[\rho \mapsto U]$ and $U'[\rho' \mapsto (U_0[\rho \mapsto \mathsf{0}])] = (U'[\rho' \mapsto U_0])[\rho \mapsto \mathsf{0}]$. Hence, $(U'[\rho' \mapsto (U_0[\rho \mapsto U])], U'[\rho' \mapsto (U_0[\rho \mapsto \mathsf{0}])]) \in R_2^{(U)}$.

(b) To show that $R_2^{(U)}$ satisfies Definition 3.7 (b), if $(U_0[\rho \mapsto U], U_0[\rho \mapsto \mathsf{0}]) \in R_2^{(U)}$ and $U_0[\rho \mapsto \mathsf{0}] \preceq \hat{V}$, then there exists $\check{V}$ such that $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Assume $(U_0[\rho \mapsto U], U_0[\rho \mapsto \mathsf{0}]) \in R_2^{(U)}$ and $U_0[\rho \mapsto \mathsf{0}] \preceq \hat{V}$. We show that there exists a closed usage $\check{V}$ such that $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$. The proof is by the induction on the construction of $U_0[\rho \mapsto \mathsf{0}] \preceq \hat{V}$. We consider cases according to the last rule of the construction.

Case 1. Assume $\hat{V} = U_0[\rho \mapsto \mathsf{0}]$. Let $\check{V} = U_0[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 2. Assume $U_0[\rho \mapsto \mathsf{0}] \preceq V'$ and $V' \preceq \hat{V}$. By the induction hypothesis, there exists a closed usage $\check{V}'$ such that $U_0[\rho \mapsto U] \preceq \check{V}'$ and $(\check{V}', V') \in R_2^{(U)}$. Since $(\check{V}', V') \in R_2^{(U)}$ and $V' \preceq \hat{V}$, the induction hypothesis implies that there exists a closed usage $\check{V}$ such that $\check{V}' \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$. Since $U_0[\rho \mapsto U] \preceq \check{V}'$ and $\check{V}' \preceq \check{V}$, we have $U_0[\rho \mapsto U] \preceq \check{V}$.

Case 3. (UP-Zero). Assume $U_0 = \mathsf{0} \mid U_1$ and $\hat{V} = U_1[\rho \mapsto \mathsf{0}]$. Let $\check{V} = U_1[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 4. (UP-Commut). Assume $U_0 = U_1 \mid U_2$ and $\hat{V} = U_2[\rho \mapsto \mathsf{0}] \mid U_1[\rho \mapsto \mathsf{0}]$. Let $\check{V} = U_2[\rho \mapsto U] \mid U_1[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 5. (UP-Assoc). Assume $U_0 = (U_1 \mid U_2) \mid U_3$ and $\hat{V} = U_1[\rho \mapsto \mathsf{0}] \mid (U_2[\rho \mapsto \mathsf{0}] \mid U_3[\rho \mapsto \mathsf{0}])$. Let $\check{V} = U_1[\rho \mapsto U] \mid (U_2[\rho \mapsto U] \mid U_3[\rho \mapsto U])$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 6. (UP-CongP). Assume $U_0 = U_1 \mid U_2$, $U_1[\rho \mapsto \mathsf{0}] \preceq \hat{V}_1$, and $\hat{V} = \hat{V}_1 \mid U_2[\rho \mapsto \mathsf{0}]$. By the induction hypothesis, there exists a closed usage $\check{V}_1$ such that $U_1[\rho \mapsto U] \preceq \check{V}_1$ and $\left(\check{V}_1, \hat{V}_1\right) \in R_2^{(U)}$. Since $\left(\check{V}_1, \hat{V}_1\right) \in R_2^{(U)}$, there exists $\check{U}_0$ such that $\check{V}_1 = \check{U}_1[\rho \mapsto U]$ and $\hat{V}_1 = \check{U}_1[\rho \mapsto \mathsf{0}]$. Let $\check{V} = \check{U}_1[\rho \mapsto U] \mid U_2[\rho \mapsto U]$. Then, we have $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$. By (UP-CongP), we have $U_1[\rho \mapsto U] \mid U_2[\rho \mapsto U] \preceq \check{U}_1[\rho \mapsto U] \mid U_2[\rho \mapsto U]$.

Case 7. (UP-Rep). Assume $U_0 = *U_1$ and $\hat{V} = *U_1[\rho \mapsto \mathsf{0}] \mid U_1[\rho \mapsto \mathsf{0}]$. Let $\check{V} = *U_1[\rho \mapsto U] \mid U_1[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 8. (UP-$\uparrow^{(*,*)}$). Assume $U_0 = \uparrow^{(t_I, t_O)} \alpha^{t_1}_{t_2}.U_1$ and $\hat{V} = \alpha^{\max(t_1,t_\alpha)}_{t_2}.U_1[\rho \mapsto \mathsf{0}]$. Let $\check{V} = \alpha^{\max(t_1,t_\alpha)}_{t_2}.U_1[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 9. (UP-Dist). Assume $U_0 = \uparrow^{(t_I,t_O)} U_1 \mid U_2$ and $\hat{V} = \uparrow^{(t_I,t_O)} U_1[\rho \mapsto \mathsf{0}] \mid \uparrow^{(t_I,t_O)} U_2[\rho \mapsto \mathsf{0}]$. Let $\check{V} = \uparrow^{(t_I,t_O)} U_1[\rho \mapsto U] \mid \uparrow^{(t_I,t_O)} U_2[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 10. (UP-Or). Fix $i \in \{1,2\}$. Assume $U_0 = U_1 \,\&\, U_2$ and $\hat{V} = U_i[\rho \mapsto \mathsf{0}]$. Let $\check{V} = U_i[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 11. (UP-Cong $\uparrow^{(*,*)}$). Assume $U_0 = \uparrow^{(t_I,t_O)} U_1$, $U_1[\rho \mapsto \mathsf{0}] \preceq \hat{V}_1$, and $\hat{V} = \uparrow^{(t_I,t_O)} \hat{V}_1$. By the induction hypothesis, there exists a closed usage $\check{V}_1$ such that $U_1[\rho \mapsto U] \preceq \check{V}_1$ and $\left(\check{V}_1, \hat{V}_1\right) \in R_2^{(U)}$. Since $\left(\check{V}_1, \hat{V}_1\right) \in R_2^{(U)}$, there exists $\check{U}_0$ such that $\check{V}_1 = \check{U}_1[\rho \mapsto U]$ and $\hat{V}_1 = \check{U}_1[\rho \mapsto \mathsf{0}]$. Let $\check{V} = \uparrow^{(t_I,t_O)} \check{U}_1[\rho \mapsto U]$. Then, we have $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$. By (UP-Cong $\uparrow^{(*,*)}$), we have $\uparrow^{(t_I,t_O)} U_1[\rho \mapsto U] \preceq \uparrow^{(t_I,t_O)} \check{U}_1[\rho \mapsto U]$.

Case 12. (UP-Commut $\uparrow^{(*,*)}$). Assume $U_0 = \uparrow^{(t_I,t_O)} \uparrow^{(t'_I,t'_O)} U_1$ and $\hat{V} = \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} U_1[\rho \mapsto \mathsf{0}]$. Let $\check{V} = \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} U_1[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Now, we show that if $(U_0[\rho \mapsto U], U_0[\rho \mapsto \mathsf{0}]) \in R_2^{(U)}$ and $U_0[\rho \mapsto \mathsf{0}] \longrightarrow \hat{V}$, then there exists $\check{V}$ such that $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Assume $(U_0[\rho \mapsto U], U_0[\rho \mapsto \mathsf{0}]) \in R_2^{(U)}$ and $U_0[\rho \mapsto \mathsf{0}] \longrightarrow \hat{V}$. We show that there exists a closed usage $\check{V}$ such that $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$. The proof is by the induction on the construction of $U_0[\rho \mapsto \mathsf{0}] \longrightarrow \hat{V}$. We consider cases according to the last rule of the construction.

Case 1. Assume $U_0 = I^{t_o}_{t_c}.U_1 \mid O^{t'_o}_{t'_c}.U_2$ and $\hat{V} = U_1[\rho \mapsto \mathsf{0}] \mid U_2[\rho \mapsto \mathsf{0}]$. Let $\check{V} = U_1[\rho \mapsto U] \mid U_2[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 2. Assume $U_0 = U_1 \mid U_2$, $U_1[\rho \mapsto \mathsf{0}] \longrightarrow \hat{V}_1$, and $\hat{V} = \hat{V}_1 \mid U_2[\rho \mapsto \mathsf{0}]$. By the induction hypothesis, there exists $\check{V}_1$ such that $U_1[\rho \mapsto U] \longrightarrow \check{V}_1$ and $\left(\check{V}_1, \hat{V}_1\right) \in R_2^{(U)}$. Since $\left(\check{V}_1, \hat{V}_1\right) \in R_2^{(U)}$, there exists $\check{U}_1$ such that $\check{V}_1 = \check{U}_1[\rho \mapsto U]$ and $\hat{V}_1 = \check{U}_1[\rho \mapsto \mathsf{0}]$. Let $\check{V} = \check{U}_1[\rho \mapsto U] \mid U_2[\rho \mapsto U]$. Then, we have $U_0[\rho \mapsto U] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$.

Case 3. Assume there exists usages $V_1$ and $V_2$ such that $U_0[\rho \mapsto \mathsf{0}] \preceq V_1$, $V_1 \longrightarrow V_2$, and $V_2 \preceq \hat{V}$. Since $U_0[\rho \mapsto \mathsf{0}] \preceq V_1$, there exists $\check{V}_1$ such that $U_1[\rho \mapsto U] \preceq \check{V}_1$ and $\left(\check{V}_1, V_1\right) \in R_2^{(U)}$. Since $\left(\check{V}_1, V_1\right) \in R_2^{(U)}$ and $V_1 \longrightarrow V_2$, the induction hypothesis implies that there exists $\check{V}_2$ such that $\check{V}_1 \longrightarrow \check{V}_2$ and $\left(\check{V}_2, V_2\right) \in R_2^{(U)}$. Since $V_2 \preceq \hat{V}$, there exists $\check{V}$ such that $\check{V}_2 \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_2^{(U)}$. Since $U_1[\rho \mapsto U] \preceq \check{V}_1$, $\check{V}_1 \longrightarrow \check{V}_2$, and $\check{V}_2 \preceq \check{V}$, we have $U_1[\rho \mapsto U] \longrightarrow \check{V}$.

(c) Let $\alpha \in \{I, O\}$. Then, we have $\mathrm{cap}_\alpha(U) \leq \infty = \mathrm{cap}_\alpha(\mathsf{0})$. By Lemma B.1 (1), we see $\mathrm{cap}_\alpha(U_0[\rho \mapsto U]) \leq \mathrm{cap}_\alpha(U_0[\rho \mapsto \mathsf{0}])$.

(d) Let $\alpha \in \{I, O\}$. By assumption, $\mathrm{ob}_\alpha(U) = \infty$. Then $\mathrm{ob}_\alpha(U) = \infty = \mathrm{ob}_\alpha(\mathsf{0})$. By Lemma B.1 (4), we have $\mathrm{ob}_\alpha(U_0[\rho \mapsto U]) = \mathrm{ob}_\alpha(U_0[\rho \mapsto \mathsf{0}])$. Thus, $\mathrm{ob}_\alpha(U_0[\rho \mapsto U]) \geq \mathrm{ob}_\alpha(U_0[\rho \mapsto \mathsf{0}])$.

(3) For closed usages $U$ and $U'$, assume $\mathrm{ob}(U) = \infty$. By this proposition (2), we have $U <: \mathsf{0}$. From Definition 3.7 (a), we see $U \mid U' <: \mathsf{0} \mid U'$. By (UP-Zero), $\mathsf{0} \mid U' \preceq U'$. By this proposition (1), we have $\mathsf{0} \mid U' <: U'$. By Proposition 3.8 (3), we have $U \mid U' <: U'$.

(4) For closed usages $U_0$, $U_1$, let

$$R_4^{(U_0,U_1)} = \{(U[\rho \mapsto *U_0 \mid *U_1], U[\rho \mapsto *(U_0 \mid U_1)]) \mid U \text{ is a usage with } \mathrm{FV}(U) \subseteq \{\rho\}\}.$$

It suffices to show that $R_4^{(U_0,U_1)}$ satisfies all the conditions of Definition 3.7.

Fix closed usages $U_0$, $U_1$. Fix a usage $U$ with $\mathrm{FV}(U) \subseteq \{\rho\}$. Assume

$$(U[\rho \mapsto (*U_0 \mid *U_1)], U[\rho \mapsto *(U_0 \mid U_1)]) \in R_4^{(U_0,U_1)}.$$

Let $W_0 = *U_0 \mid *U_1$ and $W_1 = *(U_0 \mid U_1)$.

(a) Let $U'$, where $\mathrm{FV}(U') = \{\rho'\}$. Since $\mathrm{FV}(U) = \{\rho\}$ and $\mathrm{FV}(U') = \{\rho'\}$, we have $U'[\rho' \mapsto (U[\rho \mapsto W_0])] = (U'[\rho' \mapsto U])[\rho \mapsto W_0]$ and $U'[\rho' \mapsto (U[\rho \mapsto W_1])] = (U'[\rho' \mapsto U])[\rho \mapsto W_1]$. Hence,

$$(U'[\rho' \mapsto (U[\rho \mapsto (*U_0 \mid *U_1)])], U'[\rho' \mapsto (U[\rho \mapsto *U_0 \mid U_1])]) \in R_4^{(U_0,U_1)}.$$

(b) To show that $R_4^{(U_0,U_1)}$ satisfies the condition Definition 3.7 (b), we show that if $(U[\rho \mapsto W_0], U[\rho \mapsto W_1]) \in R_4^{(U_0,U_1)}$ and there exists a usage $\hat{V}$ such that $U[\rho \mapsto W_1] \preceq \hat{V}$, then there exists $\check{V}$ such that $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Assume $U[\rho \mapsto W_1] \preceq \hat{V}$. The proof is by induction on the construction of $V[\rho \mapsto W_1] \preceq \hat{V}$. We consider cases according to the last rule of the construction.

Case 1. Assume $\hat{V} = U[\rho \mapsto W_1]$. Let $\check{V} = U[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 2. Assume $U[\rho \mapsto W_1] \preceq \hat{V}'$ and $\hat{V}' \preceq \hat{V}$. By the induction hypothesis, then there exists $\check{V}'$ such that $U[\rho \mapsto W_0] \preceq \check{V}'$ and $\left(\check{V}', \hat{V}'\right) \in R_4^{(U_0,U_1)}$. Since $\left(\check{V}', \hat{V}'\right) \in R_4^{(U_0,U_1)}$ and $\hat{V}' \preceq \hat{V}$, induction implies that there exists $\check{V}$ such that $\check{V}' \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$. Since $U[\rho \mapsto W_0] \preceq \check{V}'$ and $\check{V}' \preceq \check{V}$, we have $U[\rho \mapsto W_0] \preceq \check{V}$.

Case 3. (UP-Zero). Assume $U = \mathsf{0} \mid U'$ and $\hat{V} = U'[\rho \mapsto W_1]$. Let $\check{V} = U'[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 4. (UP-Commut). Assume $U = U_0' \mid U_1'$ and $\hat{V} = U_1'[\rho \mapsto W_1] \mid U_0'[\rho \mapsto W_1]$. Let $\check{V} = U_1'[\rho \mapsto W_0] \mid U_0'[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 5. (UP-Assoc). Assume $U = (U_0' \mid U_1') \mid U_2'$ and $\hat{V} = U_0'[\rho \mapsto W_1] \mid (U_1'[\rho \mapsto W_1] \mid U_2'[\rho \mapsto W_1])$. Let $\hat{V} = U_0'[\rho \mapsto W_0] \mid (U_1'[\rho \mapsto W_0] \mid U_2'[\rho \mapsto W_0])$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 6. (UP-CongP). Assume $U = U_0' \mid U_1'$, $U_0'[\rho \mapsto W_1] \preceq \hat{V}_0$, and $\hat{V} = \hat{V}_0 \mid U_1'[\rho \mapsto W_1]$. By the induction hypothesis, there exists a closed usage $\check{V}_0$ such that $U_0'[\rho \mapsto W_0] \preceq \check{V}_0$ and $\left(\check{V}_0, \hat{V}_0\right) \in R_4^{(U_0,U_1)}$. Since $\left(\check{V}_0, \hat{V}_0\right) \in R_4^{(U_0,U_1)}$, there exists $\check{U}_0$ such that $\check{V}_0 = \check{U}_0[\rho \mapsto W_0]$ and $\check{V}_1 = \check{U}_0[\rho \mapsto W_1]$. Let $\check{V} = \check{U}_0[\rho \mapsto W_0] \mid U_1'[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 7. (UP-Rep). Assume $U = \rho$ and $\hat{V} = (*(U_0 \mid U_1)) \mid (U_0 \mid U_1)$. Let $U' = \rho \mid (U_0 \mid U_1)$ and $\check{V} = U'[\rho \mapsto W_0]$. Then, we have $\hat{V} = U'[\rho \mapsto W_1]$. Hence, we have $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$. By (UP-Commut), (UP-Rep) and Lemma B.2, we have

$$\begin{aligned} W_0 &= *U_0 \mid *U_1 \\ &\preceq (*U_0 \mid U_0) \mid (*U_1 \mid U_1) \\ &\preceq *U_0 \mid *U_1 \mid (U_0 \mid U_1) \\ &= \check{V}. \end{aligned}$$

Assume $U = *U'$ and $\hat{V} = *U'[\rho \mapsto W_1] \mid U'[\rho \mapsto W_1]$. Let $\check{V} = *U'[\rho \mapsto W_0] \mid U'[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 8. (UP-$\uparrow^{(*,*)}$). Assume $U = \uparrow^{(t_I,t_O)} \alpha_{t_2}^{t_1}.U'$ and $\hat{V} = \alpha_{t_2}^{\max(t_1,t_\alpha)}.U'[\rho \mapsto W_1]$. Let $\check{V} = \alpha_{t_2}^{\max(t_1,t_\alpha)}.U'[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 9. (UP-Dist). Assume $U = \uparrow^{(t_I,t_O)} U_0' \mid U_1'$ and $\hat{V} = \uparrow^{(t_I,t_O)} U_0'[\rho \mapsto W_1] \mid \uparrow^{(t_I,t_O)} U_1'[\rho \mapsto W_1]$. Let $\hat{V} = \uparrow^{(t_I,t_O)} U_0'[\rho \mapsto W_0] \mid \uparrow^{(t_I,t_O)} U_1'[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 10. (UP-Or). Fix $i \in \{0, 1\}$. Assume $U = U_0' \,\&\, U_1'$ and $\hat{V} = U_i'[\rho \mapsto W_1]$. Let $\check{V} = U_i'[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 11. (UP-Cong $\uparrow^{(*,*)}$). Assume $U = \uparrow^{(t_I,t_O)} U'$, $U'[\rho \mapsto W_1] \preceq \hat{V}'$, and $\hat{V} = \uparrow^{(t_I,t_O)} \hat{V}'$. By the induction hypothesis, there exists a closed usage $\check{V}'$ such that $U'[\rho \mapsto W_0] \preceq \check{V}'$ and $\left(\check{V}', \hat{V}'\right) \in R_4^{(U_0,U_1)}$. Let $\check{V} = \uparrow^{(t_I,t_O)} \check{V}'$. Then, we have $U[\rho \mapsto W_0] \preceq \check{V}$. By Definition 3.7 (a) we have shown, $\left(\uparrow^{(t_I,t_O)} \check{V}', \uparrow^{(t_I,t_O)} \hat{V}'\right) \in R_4^{(U_0,U_1)}$ i. e. $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 12. (UP-Commut $\uparrow^{(*,*)}$). Assume $U_0 = \uparrow^{(t_I,t_O)} \uparrow^{(t_I',t_O')} U_1$ and $\hat{V} = \uparrow^{(t_I',t_O')} \uparrow^{(t_I,t_O)} U_1[\rho \mapsto W_1]$. Let $\check{V} = \uparrow^{(t_I',t_O')} \uparrow^{(t_I,t_O)} U_1[\rho \mapsto W_0]$. Then, we have $U_0[\rho \mapsto U] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Now, we show that if $(U[\rho \mapsto W_0], U[\rho \mapsto W_1]) \in R_4^{(U_0,U_1)}$ and there exists a usage $\hat{V}$ such that $U[\rho \mapsto W_1] \longrightarrow \hat{V}$, then there exists $\check{V}$ such that $U[\rho \mapsto W_0] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Assume $U[\rho \mapsto W_1] \longrightarrow \hat{V}$. The proof is by induction on the construction of $V[\rho \mapsto W_1] \longrightarrow \hat{V}$. We consider cases according to the last rule of the construction.

Case 1. Assume $U = I_{t_c}^{t_o}.U_0' \mid O_{t_c}^{t_o'}.U_1'$ and $\hat{V} = U_0'[\rho \mapsto W_1] \mid U_1'[\rho \mapsto W_1]$. Let $\check{V} = U_0'[\rho \mapsto W_0] \mid U_1'[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 2. Assume $U = U_0' \mid U_1'$, $U_0'[\rho \mapsto W_1] \longrightarrow \hat{V}_0$, and $\hat{V} = \hat{V}_0 \mid U_1'[\rho \mapsto W_1]$. By the induction hypothesis, there exists $\check{V}_0$ such that $U_0'[\rho \mapsto W_0] \longrightarrow \check{V}_0$ and $\left(\check{V}_0, \hat{V}_0\right) \in R_4^{(U_0,U_1)}$. Since $\left(\check{V}_0, \hat{V}_0\right) \in R_4^{(U_0,U_1)}$, there exists $\check{U}_0$ such that

$\check{V}_0 = \check{U}_0[\rho \mapsto W_0]$ and $\check{V}_1 = \check{U}_0[\rho \mapsto W_1]$. Let $\check{V} = \check{U}_0[\rho \mapsto W_0] \mid U_1'[\rho \mapsto W_0]$. Then, we have $U[\rho \mapsto W_0] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$.

Case 3. Assume there exists usages $V_0$ and $V_1$ such that $U[\rho \mapsto W_1] \preceq V_0$, $V_0 \longrightarrow V_1$, and $V_1 \preceq \hat{V}$. Since $U[\rho \mapsto W_1] \preceq V_0$, there exists $\check{V}_0$ such that $U[\rho \mapsto W_0] \preceq \check{V}_0$ and $\left(\check{V}_0, V_0\right) \in R_4^{(U_0,U_1)}$. Since $\left(\check{V}_0, V_0\right) \in R_4^{(U_0,U_1)}$ and $V_0 \longrightarrow V_1$, the induction hypothesis implies that there exists $\check{V}_1$ such that $\check{V}_0 \longrightarrow \check{V}_1$ and $\left(\check{V}_1, V_1\right) \in R_4^{(U_0,U_1)}$. Since $\left(\check{V}_1, V_1\right) \in R_4^{(U_0,U_1)}$ and $V_1 \preceq \hat{V}$, there exists $\check{V}$ such that $\check{V}_1 \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_4^{(U_0,U_1)}$. Since $U[\rho \mapsto W_0] \preceq \check{V}_0$, $\check{V}_0 \longrightarrow \check{V}_1$, and $\check{V}_1 \preceq \check{V}$, we have $U[\rho \mapsto W_0] \longrightarrow \check{V}$.

(c) Let $\alpha \in \{I, O\}$. Then

$$\begin{aligned}\mathrm{cap}_\alpha(*(U_0 \mid U_1)) &= \mathrm{cap}_\alpha(U_0 \mid U_1)\\ &= \min(\mathrm{cap}_\alpha(U_0), \mathrm{cap}_\alpha(U_1))\\ &= \min(\mathrm{cap}_\alpha(*U_0), \mathrm{cap}_\alpha(*U_1))\\ &= \mathrm{cap}_\alpha(*U_0 \mid *U_1).\end{aligned}$$

By Lemma B.1 (2), we have $\mathrm{cap}_\alpha(U[\rho \mapsto *(U_0 \mid U_1)]) = \mathrm{cap}_\alpha(U[\rho \mapsto (*U_0 \mid *U_1)])$. Thus,

$$\mathrm{cap}_\alpha(U[\rho \mapsto *(U_0 \mid U_1)]) \leq \mathrm{cap}_\alpha(U[\rho \mapsto (*U_0 \mid *U_1)]).$$

(d) Let $\alpha \in \{I, O\}$. Then

$$\begin{aligned}\mathrm{ob}_\alpha(*(U_0 \mid U_1)) &= \mathrm{ob}_\alpha(U_0 \mid U_1)\\ &= \min(\mathrm{ob}_\alpha(U_0), \mathrm{ob}_\alpha(U_1))\\ &= \min(\mathrm{ob}_\alpha(*U_0), \mathrm{ob}_\alpha(*U_1))\\ &= \mathrm{ob}_\alpha(*U_0 \mid *U_1).\end{aligned}$$

By Lemma B.1 (4), we have $\mathrm{ob}_\alpha(U[\rho \mapsto *(U_0 \mid U_1)]) = \mathrm{ob}_\alpha(U[\rho \mapsto (*U_0 \mid *U_1)])$. Thus,

$$\mathrm{ob}_\alpha(U[\rho \mapsto *(U_0 \mid U_1)]) \geq \mathrm{ob}_\alpha(U[\rho \mapsto (*U_0 \mid *U_1)]).$$

(5) By this proposition (4) and Proposition 3.8 (3),

$$\begin{aligned}*(U_0 \mid \cdots \mid U_n) &:> *(U_0 \mid \cdots \mid U_{n-1}) \mid *U_n\\ &:> \quad \vdots\\ \vdots &\quad \vdots\\ &:> (*U_0 \mid \cdots \mid *U_n).\end{aligned}$$

(6) Assume $U_0 <: U_0'$ and $U_1 <: U_1'$. By Definition 3.7 (a), we have $U_0 \mid U_1 <: U_0' \mid U_1$. We also have $U_0' \mid U_1 <: U_0' \mid U_1'$. By Proposition 3.8 (3), we see $U_0 \mid U_1 <: U_0' \mid U_1'$.

(7) For a tuple of variables $\tilde{\rho} = (\rho_0, \ldots, \rho_n)$ and a tuple of usages $\tilde{U} = (U_0, \ldots, U_n)$, we abbreviate $U[\rho_0 \mapsto U_0, \ldots, \rho_n \mapsto U_n]$ for $U\left[\tilde{\rho} \mapsto \tilde{U}\right]$.

Let

$$R_5 = \bigcup_{n=0}^{\infty} \left\{ \left( \begin{matrix} V\left[\rho_0 \mapsto \uparrow^{(t_{I0}, t_{O0})} U_0, \ldots, \rho_n \mapsto \uparrow^{(t_{In}, t_{On})} U_n\right], \\ V[\rho_0 \mapsto U_0, \ldots, \rho_n \mapsto U_n] \end{matrix} \right) \;\middle|\; \begin{matrix} U_0, \ldots, U_n \text{ are closed usages, and} \\ V \text{ is a usage with } \mathrm{FV}(V) \subseteq \{\rho_0, \ldots, \rho_n\} \end{matrix} \right\}.$$

It suffices to show that $R_5$ satisfies all the conditions of Definition 3.7.

Fix closed usages $U_0, \ldots, U_n$, a usage $V$ with $\mathrm{FV}(V) \subseteq \{\rho_0, \ldots, \rho_n\}$, and $t_{O0}, \ldots, t_{On}, t_{I0}, \ldots t_{In} \in \mathbb{N} \cup \{\infty\}$. Let $\tilde{\rho} = (\rho_0, \ldots, \rho_n)$, $\tilde{U} = (U_0, \ldots, U_n)$, and $\tilde{U'} = \left(\uparrow^{(t_{I0}, t_{O0})} U_0, \ldots, \uparrow^{(t_{In}, t_{On})} U_n\right)$. Assume $\left(V\left[\tilde{\rho} \mapsto \tilde{U'}\right], V\left[\tilde{\rho} \mapsto \tilde{U}\right]\right) \in R_5$.

(a) Let $V'$ be a usage with $\mathrm{FV}(V') = \{\rho'\}$. Since $\mathrm{FV}(V) \subseteq \{\rho_0, \ldots, \rho_n\}$ and $\mathrm{FV}(V') = \{\rho'\}$, we have $V'\left[\rho' \mapsto \left(V\left[\tilde{\rho} \mapsto \tilde{U}\right]\right)\right] = (V'[\rho' \mapsto V])\left[\tilde{\rho} \mapsto \tilde{U}\right]$ and $V'\left[\rho' \mapsto \left(V\left[\tilde{\rho} \mapsto \tilde{U'}\right]\right)\right] = (V'[\rho' \mapsto V])\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Hence, $\left(V'\left[\rho' \mapsto \left(V\left[\tilde{\rho} \mapsto \tilde{U'}\right]\right)\right], V'\left[\rho' \mapsto \left(V\left[\tilde{\rho} \mapsto \tilde{U}\right]\right)\right]\right) \in R_5$.

(b) To show that $R_5$ satisfies Definition 3.7 (b), if $\left(V\left[\tilde{\rho} \mapsto \tilde{U'}\right], V\left[\tilde{\rho} \mapsto \tilde{U}\right]\right) \in R_5$ and $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \preceq \hat{V}$, then there exists $\check{V}$ such that $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Assume $\left(V\left[\tilde{\rho} \mapsto \tilde{U'}\right], V\left[\tilde{\rho} \mapsto \tilde{U}\right]\right) \in R_5$ and $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \preceq \hat{V}$. We show that there exists a closed usage $\check{V}$ such that $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$. The proof is by the induction on the construction of $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \preceq \hat{V}$.

Assume $V = \rho_i$ with some $i = 0, \ldots, n$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U}\right] = U_i$ and $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] = \uparrow^{(t_{I_i}, t_{O_i})} U_i$. Let $\check{V} = \uparrow^{(t_{I_i}, t_{O_i})} \hat{V}$. Then, we have $\left(\uparrow^{(t_{I_i}, t_{O_i})} \hat{V}, \hat{V}\right) \in R_5$. By (UP-Cong $\uparrow^{(*,*)}$), $U_i \preceq \hat{V}$ implies $\uparrow^{(t_{I_i}, t_{O_i})} U_i \preceq \check{V}$.

We consider other cases according to the last rule of the construction of $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \preceq \hat{V}$.

Case 1. Assume $\hat{V} = V\left[\tilde{\rho} \mapsto \tilde{U}\right]$. Let $\check{V} = V\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Case 2. Assume $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \preceq V'$ and $V' \preceq \hat{V}$. By the induction hypothesis, there exists a closed usage $\check{V}'$ such that $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}'$ and $\left(\check{V}', V'\right) \in R_5$. Since $\left(\check{V}', V'\right) \in R_5$ and $V' \preceq \hat{V}$, the induction hypothesis implies that there exists a closed usage $\check{V}$ such that $\check{V}' \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$. Since $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}'$ and $\check{V}' \preceq \check{V}$, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$.

Case 3. (UP-Zero). Assume $V = \mathtt{0} \mid V_0$ and $\hat{V} = V_0\left[\tilde{\rho} \mapsto \tilde{U}\right]$. Let $\check{V} = V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Case 4. (UP-Commut). Assume $V = V_0 \mid V_1$ and $\hat{V} = V_1\left[\tilde{\rho} \mapsto \tilde{U}\right] \mid V_0\left[\tilde{\rho} \mapsto \tilde{U}\right]$. Let $\check{V} = V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right] \mid V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Case 5. (UP-Assoc). Assume $V = \rho_i \mid V_2$, $U_i = V_0 \mid V_1$ and $\hat{V} = V_0 \mid \left(V_1 \mid V_2\left[\tilde{\rho} \mapsto \tilde{U}\right]\right)$ for some $i = 0, \ldots, n$. Then $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] = \left(\uparrow^{(t_{I_i}, t_{O_i})} (V_0 \mid V_1)\right) \mid V_2\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. By (UP-Dist) and transitivity, we have

$$\begin{aligned}\uparrow^{(t_{I_i}, t_{O_i})} (V_0 \mid V_1) \mid V_2\left[\tilde{\rho} \mapsto \tilde{U'}\right] &\preceq \uparrow^{(t_{I_i}, t_{O_i})} V_0 \mid \uparrow^{(t_{I_i}, t_{O_i})} V_1 \mid V_2\left[\tilde{\rho} \mapsto \tilde{U'}\right] \\ &\preceq \uparrow^{(t_{I_i}, t_{O_i})} V_0 \mid \left(\uparrow^{(t_{I_i}, t_{O_i})} V_1 \mid V_2\left[\tilde{\rho} \mapsto \tilde{U'}\right]\right).\end{aligned}$$

Let $\check{V} = \uparrow^{(t_{I_i}, t_{O_i})} V_0 \mid \left(\uparrow^{(t_{I_i}, t_{O_i})} V_1 \mid V_2\left[\tilde{\rho} \mapsto \tilde{U'}\right]\right)$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Assume $V = (V_0 \mid V_1) \mid V_2$ and $\hat{V} = V_0\left[\tilde{\rho} \mapsto \tilde{U}\right] \mid \left(V_1\left[\tilde{\rho} \mapsto \tilde{U}\right] \mid V_2\left[\tilde{\rho} \mapsto \tilde{U}\right]\right)$. Let $\check{V} = V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \mid \left(V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right] \mid V_2\left[\tilde{\rho} \mapsto \tilde{U'}\right]\right)$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Case 6. (UP-CongP). Assume $V = V_0 \mid V_1$, $V_0\left[\tilde{\rho} \mapsto \tilde{U}\right] \preceq \hat{V}_0$, and $\hat{V} = \hat{V}_0 \mid V_1\left[\tilde{\rho} \mapsto \tilde{U}\right]$. By the induction hypothesis, there exists a closed usage $\check{V}_0$ such that $V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}_0$ and $\left(\check{V}_0, \hat{V}_0\right) \in R_5$. Since $\left(\check{V}_0, \hat{V}_0\right) \in R_5$, there exists closed usages $W_0, \ldots, W_m$, a usage $V'$ with $\mathrm{FV}(V') \subseteq \{\rho'_0, \ldots, \rho'_m\}$, and $t'_{O0}, \ldots, t'_{Om}, t'_{I0}, \ldots t'_{Im} \in \mathbb{N} \cup \{\infty\}$ such that

$$\begin{aligned}\check{V}_0 &= V'\left[\rho'_0 \mapsto \uparrow^{(t_{I_0}, t_{O_0})} W_0, \ldots, \rho'_m \mapsto \uparrow^{(t_{I_m}, t_{O_m})} W_m\right] \text{ and} \\ \hat{V}_0 &= V'[\rho'_0 \mapsto W_0, \ldots, \rho'_m \mapsto W_m].\end{aligned}$$

Without loss of generality, we can assume $\{\rho_0, \ldots, \rho_n\} \cap \{\rho'_0, \ldots, \rho'_m\} = \emptyset$. Let $\tilde{\rho'} = (\rho'_0, \ldots, \rho'_m)$, $\tilde{W} = (W_0, \ldots, W_m)$, and $\tilde{W'} = \left(\uparrow^{(t'_{I0}, t'_{O0})} W_0, \ldots, \uparrow^{(t'_{Im}, t'_{Om})} W_m\right)$.

Let $\check{V} = V'\left[\tilde{\rho'} \mapsto \tilde{W'}\right] \mid V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $\left(\check{V}, \hat{V}\right) \in R_5$. By (UP-CongP), we have $V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \mid V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq V'\left[\tilde{\rho'} \mapsto \tilde{W'}\right] \mid V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right]$.

Case 7. (UP-Rep). Assume $V = *V_0$ and $\hat{V} = *V_0\left[\tilde{\rho} \mapsto \tilde{U}\right] \mid V_0\left[\tilde{\rho} \mapsto \tilde{U}\right]$. Let $\check{V} = *V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \mid V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Case 8. (UP-$\uparrow^{(*,*)}$). Assume $V = \uparrow^{(t_I, t_O)} \rho_i$, $U_i = \alpha^{t_1}_{t_2}.V_0$, and $\hat{V} = \alpha^{\max(t_1, t_\alpha)}_{t_2}.V_0$. Let $\check{V} = \uparrow^{(t_{I_i}, t_{O_i})} \alpha^{\max(t_1, t_\alpha)}_{t_2}.V_0$. Then, we have $\left(\check{V}, \hat{V}\right) \in R_5$. By (UP-Commut $\uparrow^{(*,*)}$) and (UP-Rep), we have

$$V\left[\tilde{\rho} \mapsto \tilde{U'}\right] = \uparrow^{(t_I, t_O)} \uparrow^{(t_{I_i}, t_{O_i})} \alpha^{t_1}_{t_2}.V_0 \preceq \uparrow^{(t_{I_i}, t_{O_i})} \uparrow^{(t_I, t_O)} \alpha^{t_1}_{t_2}.V_0 \preceq \uparrow^{(t_{I_i}, t_{O_i})} \alpha^{\max(t_1, t_\alpha)}_{t_2}.V_0 = \check{V}.$$

Therefore, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$.

Assume $V = \uparrow^{(t_I,t_O)} \alpha_{t_2}^{t_1}.V_0$ and $\hat{V} = \alpha_{t_2}^{\max(t_1,t_\alpha)}.V_0\left[\tilde{\rho} \mapsto \tilde{U}\right]$. Let $\check{V} = \alpha_{t_2}^{\max(t_1,t_\alpha)}.V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Case 9. (UP-Dist). Assume $V = \uparrow^{(t_I,t_O)} V_0 \mid V_1$ and $\hat{V} = \uparrow^{(t_I,t_O)} V_0\left[\tilde{\rho} \mapsto \tilde{U}\right] \mid \uparrow^{(t_I,t_O)} V_1\left[\tilde{\rho} \mapsto \tilde{U}\right]$. Let $\check{V} = \uparrow^{(t_I,t_O)} V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \mid \uparrow^{(t_I,t_O)} V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Case 10. (UP-Or). Fix $j \in \{0,1\}$. Assume $V = V_0 \,\&\, V_1$ and $\hat{V} = V_j\left[\tilde{\rho} \mapsto \tilde{U}\right]$. Let $\check{V} = V_j\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Case 11. (UP-Cong $\uparrow^{(*,*)}$). Assume $V = \uparrow^{(t_I,t_O)} V_0$, $V_0\left[\tilde{\rho} \mapsto \tilde{U}\right] \preceq \hat{V}_0$, and $\hat{V} = \uparrow^{(t_I,t_O)} \hat{V}_0$. By the induction hypothesis, there exists a closed usage $\check{V}_0$ such that $V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}_0$ and $\left(\check{V}_0, \hat{V}_0\right) \in R_5$. Since $\left(\check{V}_0, \hat{V}_0\right) \in R_5$, there exist closed usages $W_0, \ldots, W_m$, a usage $V'$ with $\mathrm{FV}(V') \subseteq \{\rho'_0, \ldots, \rho'_m\}$, and $t'_{O0}, \ldots, t'_{Om}, t'_{I0}, \ldots t'_{Im} \in \mathbb{N} \cup \{\infty\}$ such that

$$\check{V}_0 = V'\left[\rho'_0 \mapsto \uparrow^{(t_{I_0},t_{O_0})} W_0, \ldots, \rho'_m \mapsto \uparrow^{(t_{I_m},t_{O_m})} W_m\right] \text{ and}$$
$$\hat{V}_0 = V'[\rho'_0 \mapsto W_0, \ldots, \rho'_m \mapsto W_m].$$

Let $\tilde{\rho'} = (\rho'_0, \ldots, \rho'_m)$, $\tilde{W} = (W_0, \ldots, W_m)$, and $\tilde{W'} = \left(\uparrow^{(t'_{I0},t'_{O0})} W_0, \ldots, \uparrow^{(t'_{Im},t'_{Om})} W_m\right)$. Let $\check{V} = \uparrow^{(t_I,t_O)} V'[\rho'_0 \mapsto W_0, \ldots, \rho'_m \mapsto W_m]$. Then, we have $\left(\check{V}, \hat{V}\right) \in R_5$. By (UP-Cong $\uparrow^{(*,*)}$), we have $\uparrow^{(t_I,t_O)} V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \uparrow^{(t_I,t_O)} V'\left[\tilde{\rho'} \mapsto \tilde{W'}\right]$.

Case 12. (UP-Commut $\uparrow^{(*,*)}$). Assume $V = \uparrow^{(t_I,t_O)} \rho_i$, $U_i = \uparrow^{(t'_I,t'_O)} V_0$, and $\hat{V} = \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} V_0$. Let $\check{V} = \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} \uparrow^{(t_{I_i},t_{O_i})} V_0$. Then, we have $\left(\check{V}, \hat{V}\right) \in R_5$. By (UP-Commut $\uparrow^{(*,*)}$) and (UP-Cong $\uparrow^{(*,*)}$), we have

$$\begin{aligned} V\left[\tilde{\rho} \mapsto \tilde{U'}\right] &= \uparrow^{(t_I,t_O)} \uparrow^{(t_{I_i},t_{O_i})} \uparrow^{(t'_I,t'_O)} V_0 \\ &\preceq \uparrow^{(t_I,t_O)} \uparrow^{(t'_I,t'_O)} \uparrow^{(t_{I_i},t_{O_i})} V_0 \\ &\preceq \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} \uparrow^{(t_{I_i},t_{O_i})} V_0 \\ &= \check{V}. \end{aligned}$$

Hence, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$.

Assume $V = \uparrow^{(t_I,t_O)} \uparrow^{(t'_I,t'_O)} V_0$ and $\hat{V} = \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} V_0\left[\tilde{\rho} \mapsto \tilde{U}\right]$. Let $\check{V} = \uparrow^{(t'_I,t'_O)} \uparrow^{(t_I,t_O)} V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Now, we show that if $\left(V\left[\tilde{\rho} \mapsto \tilde{U'}\right], V\left[\tilde{\rho} \mapsto \tilde{U}\right]\right) \in R_5$ and $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \longrightarrow \hat{V}$, then there exists $\check{V}$ such that $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Assume $\left(V\left[\tilde{\rho} \mapsto \tilde{U'}\right], V\left[\tilde{\rho} \mapsto \tilde{U}\right]\right) \in R_5$ and $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \longrightarrow \hat{V}$. We show that there exists a closed usage $\check{V}$ such that that $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$. The proof is by the induction on the construction of $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \longrightarrow \hat{V}$.

Case 1. Assume $V = I_{t_c}^{t_o}.V_0 \mid O_{t'_c}^{t'_o}.V_1$ and $\hat{V} = V_0\left[\tilde{\rho} \mapsto \tilde{U}\right] \mid V_1\left[\tilde{\rho} \mapsto \tilde{U}\right]$. Let $\hat{V} = V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \mid V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \longrightarrow \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$.

Case 2. Assume $V = V_0 \mid V_1$, $V_0\left[\tilde{\rho} \mapsto \tilde{U}\right] \longrightarrow \hat{V}_0$, and $\hat{V} = \hat{V}_0 \mid V_1\left[\tilde{\rho} \mapsto \tilde{U}\right]$. By the induction hypothesis, there exists a closed usage $\check{V}_0$ such that $V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \longrightarrow \check{V}_0$ and $\left(\check{V}_0, \hat{V}_0\right) \in R_5$. Since $\left(\check{V}_0, \hat{V}_0\right) \in R_5$, there exists closed usages $W_0, \ldots, W_m$, a usage $V'$ with $\mathrm{FV}(V') \subseteq \{\rho'_0, \ldots, \rho'_m\}$, and $t'_{O0}, \ldots, t'_{Om}, t'_{I0}, \ldots t'_{Im} \in \mathbb{N} \cup \{\infty\}$ such that

$$\check{V}_0 = V'\left[\rho'_0 \mapsto \uparrow^{(t_{I_0},t_{O_0})} W_0, \ldots, \rho'_m \mapsto \uparrow^{(t_{I_m},t_{O_m})} W_m\right] \text{ and}$$
$$\hat{V}_0 = V'[\rho'_0 \mapsto W_0, \ldots, \rho'_m \mapsto W_m].$$

Without loss of generality, we can assume $\{\rho_0, \ldots, \rho_n\} \cap \{\rho'_0, \ldots, \rho'_m\} = \emptyset$. Let $\tilde{\rho'} = (\rho'_0, \ldots, \rho'_m)$, $\tilde{W} = (W_0, \ldots, W_m)$, and $\tilde{W'} = \left(\uparrow^{(t'_{I0}, t'_{O0})} W_0, \ldots, \uparrow^{(t'_{Im}, t'_{Om})} W_m\right)$.

Let $\check{V} = V'\left[\tilde{\rho'} \mapsto \tilde{W'}\right] \mid V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right]$. Then, we have $\left(\check{V}, \hat{V}\right) \in R_5$. We also have $V_0\left[\tilde{\rho} \mapsto \tilde{U'}\right] \mid V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right] \longrightarrow V'\left[\tilde{\rho'} \mapsto \tilde{W'}\right] \mid V_1\left[\tilde{\rho} \mapsto \tilde{U'}\right]$.

Case 3. Assume there exists usages $V_0$ and $V_1$ such that $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \preceq V_0$, $V_0 \longrightarrow V_1$, and $V_1 \preceq \hat{V}$. Since $V\left[\tilde{\rho} \mapsto \tilde{U}\right] \preceq V_0$, there exists $\check{V}_0$ such that $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}_0$ and $\left(\check{V}_0, V_0\right) \in R_5$. Since $\left(\check{V}_0, V_0\right) \in R_5$ and $V_0 \longrightarrow V_1$, the induction hypothesis implies that there exists $\check{V}_1$ such that $\check{V}_0 \longrightarrow \check{V}_1$ and $\left(\check{V}_1, V_1\right) \in R_5$. Since $V_1 \preceq \hat{V}$, there exists $\check{V}$ such that $\check{V}_1 \preceq \check{V}$ and $\left(\check{V}, \hat{V}\right) \in R_5$. Since $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \preceq \check{V}_0$, $\check{V}_0 \longrightarrow \check{V}_1$ and $\check{V}_1 \preceq \check{V}$, we have $V\left[\tilde{\rho} \mapsto \tilde{U'}\right] \longrightarrow \check{V}$.

(c) By Lemma B.1 (2).

(d) By Lemma B.1 (4).

(8) By this proposition (7). □

# Appendix C. Basic properties of types and type environments

## C.1. A basic property of types

**Proposition C.1.** *(1) Let $\tau_0$ and $\tau_1$ be types. Then $\tau_0 \mid \tau_1 <: \tau_1 \mid \tau_0$.*
*(2) Let $\tau_0$, $\tau_1$, and $\tau_2$ be types. Then $(\tau_0 \mid \tau_1) \mid \tau_2 <: \tau_0 \mid (\tau_1 \mid \tau_2)$.*
*(3) For types $\tau_0$, $\tau'_0$, $\tau_1$ and $\tau'_1$, if $\tau_i <: \tau'_i$ for each $i = 0, 1$, then $\tau_0 \mid \tau_1 <: \tau'_0 \mid \tau'_1$.*
*(4) Let $\tau_0$, $\tau_1$, and $\tau_2$ be types. Then $\tau_0 \mid (\tau_1 \mid \tau_2) <: (\tau_0 \mid \tau_1) \mid \tau_2$.*
*(5) For types $\tau$ and $\tau'$, $\mathrm{ob}(\tau) = \infty$ implies $\tau \mid \tau' <: \tau'$.*
*(6) For types $\tau$ and $\tau'$, if $\tau <: \tau'$, then $*\tau <: *\tau'$.*
*(7) Let $\tau$ be a type. Then $*\tau <: *\tau \mid \tau$.*
*(8) Let $\tau_0, \ldots, \tau_n$ be types. Then $(*\tau_0 \mid \cdots \mid *\tau_n) <: *(\tau_0 \mid \cdots \mid \tau_n)$.*
*(9) Let $\tau$ be a type. Then $\uparrow^{(t_I, t_O)} \tau <: \tau$.*
*(10) Let $\tau$ be a type. Then $\uparrow \tau <: \tau$.*

*Proof.* We show each claim.

(1) We show $\tau_0 \mid \tau_1 <: \tau_1 \mid \tau_0$.

Assume $\tau_0$ is a base type and $\tau_0 = \tau_1$. Then $\tau_0 \mid \tau_1 = \tau_0$. Since $\tau_0 = \tau_1$, we see that $\tau_1$ is a base type. Then $\tau_1 \mid \tau_0 = \tau_1$. Since $\tau_0 = \tau_1$, we have $\tau_0 \mid \tau_1 = \tau_1 \mid \tau_0$. Hence, we have $\tau_0 \mid \tau_1 <: \tau_1 \mid \tau_0$.

Assume $\tau_0 = \xi/U_0$ and $\tau_1 = \xi/U_1$. Then, we have $\tau_0 \mid \tau_1 \equiv \xi/U_0 \mid U_1$ and $\tau_1 \mid \tau_0 \equiv \xi/U_1 \mid U_0$. Since $U_0 \mid U_1 \preceq U_1 \mid U_0$, Proposition B.4 (1) implies $U_0 \mid U_1 <: U_1 \mid U_0$. Thus, $\tau_0 \mid \tau_1 <: \tau_1 \mid \tau_0$.

(2) We show $(\tau_0 \mid \tau_1) \mid \tau_2 <: \tau_0 \mid (\tau_1 \mid \tau_2)$.

Assume $\tau_0$ is a base type and $\tau_0 = \tau_1$. Then $\tau_0 \mid \tau_1 = \tau_0$. Because $\tau_0$ is a base type and $\tau_0 \mid \tau_2$ is defined, we have $\tau_0 = \tau_2$ and $\tau_0 \mid \tau_2 = \tau_0$. Hence, $(\tau_0 \mid \tau_1) \mid \tau_2 = \tau_0 = \tau_0 \mid \tau_1 = \tau_0 \mid (\tau_1 \mid \tau_2)$.

Assume $\tau_0 = \xi/U_0$ and $\tau_1 = \xi/U_1$. Then $\tau_0 \mid \tau_1 = \xi/U_0 \mid U_1$. Because $(\tau_0 \mid \tau_1) \mid \tau_2$ is defined, there exists a usage $U_2$ such that $\tau_2 = \xi/U_2$. Hence, $(\tau_0 \mid \tau_1) \mid \tau_2 = \xi/((U_0 \mid U_1) \mid U_2)$. We also have $\tau_0 \mid (\tau_1 \mid \tau_2) = \xi/(U_0 \mid (U_1 \mid U_2))$. Since $(U_0 \mid U_1) \mid U_2 \preceq U_0 \mid (U_1 \mid U_2)$, we see $(U_0 \mid U_1) \mid U_2 <: U_0 \mid (U_1 \mid U_2)$. Thus, $(\tau_0 \mid \tau_1) \mid \tau_2 <: \tau_0 \mid (\tau_1 \mid \tau_2)$.

(3) Assume $\tau_i <: \tau'_i$ for each $i = 0, 1$. We show $\tau_0 \mid \tau_1 <: \tau'_0 \mid \tau'_1$.

Assume $\tau_0$ is a base type and $\tau_0 = \tau_1$. Then $\tau_0 \mid \tau_1 = \tau_0$. Since $\tau_0 <: \tau'_0$, we have $\tau'_0 = \tau_0$. Since $\tau_0 = \tau_1$, we see that $\tau_1$ is a base type. Since $\tau_1 <: \tau'_1$, we have $\tau'_1 = \tau_1$. Then $\tau_0 \mid \tau_1 \equiv \tau'_0 \mid \tau'_1$. Hence, we have $\tau_0 \mid \tau_1 <: \tau'_0 \mid \tau'_1$.

Assume $\tau_0 = \xi/U_0$ and $\tau_1 = \xi/U_1$. Then $\tau_0 \mid \tau_1 \equiv \xi/U_0 \mid U_1$. For each $i = 0, 1$, because of $\tau_i <: \tau'_i$, we have $\tau'_i = \xi/U'_i$ and $U_i <: U'_i$. By Proposition B.4 (6), we have $U_0 \mid U_1 <: U'_0 \mid U'_1$. Then

$$\tau_0 \mid \tau_1 \equiv \xi/U_0 \mid U_1 <: \xi/U'_0 \mid U'_1 \equiv \tau'_0 \mid \tau'_1.$$

(4) We show $\tau_0 \mid (\tau_1 \mid \tau_2) <: (\tau_0 \mid \tau_1) \mid \tau_2$. By (1), (2), (3), and transitivity of $<:$, we have

$$\begin{aligned} \tau_0 \mid (\tau_1 \mid \tau_2) &<: (\tau_1 \mid \tau_2) \mid \tau_0 \\ &<: (\tau_2 \mid \tau_1) \mid \tau_0 \\ &<: \tau_2 \mid (\tau_1 \mid \tau_0) \\ &<: (\tau_1 \mid \tau_0) \mid \tau_2 \end{aligned}$$

$$<: (\tau_0 \mid \tau_1) \mid \tau_2.$$

Thus, $\tau_0 \mid (\tau_1 \mid \tau_2) <: (\tau_0 \mid \tau_1) \mid \tau_2$.
(5) Assume $\mathrm{ob}(\tau) = \infty$.

Assume that $\tau$ is a base type. Since $\tau \mid \tau'$ is defined, we have $\tau'$ is a base type and $\tau = \tau'$. Then, we have $\tau \mid \tau' = \tau = \tau'$. Therefore, we have $\tau \mid \tau' <: \tau'$.

Assume that $\tau \equiv \xi/U$ and $\mathrm{ob}(U) = \infty$. Since $\tau \mid \tau'$ is defined, there exists a usage $U'$ such that $\tau' \equiv \xi/U'$. Then, we have $\tau \mid \tau' = \xi/U \mid U'$. By Proposition B.4 (3), we have $U \mid U' <: U'$. By Definition 3.9, $\tau \mid \tau' <: \tau'$.
(6) Assume $\tau <: \tau'$.

Assume that $\tau$ is a base type. Then, we have $\tau = \tau'$. We also have $*\tau = \tau$. Because $\tau'$ is a base type, $*\tau' = \tau'$. Hence, $*\tau = *\tau'$. Therefore, $*\tau <: *\tau'$.

Assume that $\tau \equiv \xi/U$. Then $*\tau \equiv \xi/*U$. Since $\tau <: \tau'$, there exists $U'$ such that $U <: U'$ and $\tau' \equiv \xi/U'$. Then $*\tau' \equiv \xi/*U'$. By Definition 3.7 (a), we have $*U <: *U'$. Thus, $*\tau <: *\tau'$.
(7) We show $*\tau <: *\tau \mid \tau$.

Assume that $\tau$ is a base type. Then, we have $*\tau = \tau$. Since $\tau$ is a base type, we have $*\tau \mid \tau = \tau \mid \tau = \tau$. Therefore, $*\tau <: *\tau \mid \tau$.

Assume that $\tau \equiv \xi/U$. Then $*\tau \equiv \xi/*U$ and $*\tau \mid \tau \equiv \xi/*U \mid U$. Since $*U \preceq *U \mid U$, Proposition B.4 (1) implies $*U <: *U \mid U$. Therefore, $*\tau <: *\tau \mid \tau$.
(8) We show $(*\tau_0 \mid \cdots \mid *\tau_n) <: *(\tau_0 \mid \cdots \mid \tau_n)$.

Assume that $\tau_0$ is a base type. Then, we have $*\tau_0 = \tau_0$. Since $(*\tau_0 \mid \cdots \mid *\tau_n)$ is defined, $*\tau_1, \ldots, *\tau_n$ are base types. Then, we see that $*\tau_i = \tau_i$ and $\tau_i$ is a base type for each $i = 0, \ldots, n$. Hence, $(*\tau_0 \mid \cdots \mid *\tau_n) = (\tau_0 \mid \cdots \mid \tau_n)$. Since $\tau_0 \mid \cdots \mid \tau_n$ is defined and $\tau_0$ is a base type, we have $\tau_0 \mid \cdots \mid \tau_n = \tau_0$. Then $*\tau_0 \mid \cdots \mid \tau_n = *\tau_0 = \tau_0$. Therefore, $(*\tau_0 \mid \cdots \mid *\tau_n) <: *(\tau_0 \mid \cdots \mid \tau_n)$.

Assume that $\tau_0 \equiv \xi/U_0$. Then $*\tau_0 \equiv \xi/*U_0$. Since $*(\tau_0 \mid \cdots \mid \tau_n)$ is defined, $\tau_0 \mid \cdots \mid \tau_n$ is defined. Hence, $\tau_i$ is the form of $\xi/U_i$ for each $i = 1, \ldots, n$. Then, we have

$$(*\tau_0 \mid \cdots \mid *\tau_n) = \xi/(*U_0 \mid \cdots \mid *U_n) \text{ and}$$
$$*(\tau_0 \mid \cdots \mid \tau_n) = \xi/*(U_0 \mid \cdots \mid U_n).$$

By Proposition B.4 (5), we have $(*\tau_0 \mid \cdots \mid *\tau_n) <: *(\tau_0 \mid \cdots \mid \tau_n)$.
(9) We show $\uparrow^{(t_I,t_O)} \tau <: \tau$.

Assume $\tau$ is a base type. Then $\uparrow^{(t_I,t_O)} \tau = \tau$. Hence, $\uparrow^{(t_I,t_O)} \tau <: \tau$

Assume $\tau = \xi/U$. Then $\uparrow^{(t_I,t_O)} \tau = \xi/\uparrow^{(t_I,t_O)} U$. By Proposition B.4 (7), we have $\uparrow^{(t_I,t_O)} U <: U$. Hence, $\uparrow^{(t_I,t_O)} \tau <: \tau$.
(10) We show $\uparrow \tau <: \tau$.

Assume $\tau$ is a base type. Then $\uparrow \tau = \tau$. Hence, $\uparrow \tau <: \tau$

Assume $\tau = \xi/U$. Then $\uparrow \tau = \xi/\uparrow U$. By Proposition B.4 (8), we have $\uparrow U <: U$. Hence, $\uparrow \tau <: \tau$.

□

## C.2. A basic property of type environments

**Proposition C.2.** (1) *For type environments* $\Gamma_0$ *and* $\Gamma_1$, $\Gamma_0 \mid \Gamma_1 <: \Gamma_1 \mid \Gamma_0$.
(2) *For type environments* $\Gamma_0$, $\Gamma_1$, *and* $\Gamma_2$, $\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2) <: (\Gamma_0 \mid \Gamma_1) \mid \Gamma_2$.
(3) *For type environments* $\Gamma_0$, $\Gamma_1$, *and* $\Gamma_0'$, *if* $\Gamma_0 <: \Gamma_0'$, *then* $\Gamma_0 \mid \Gamma_1 <: \Gamma_0' \mid \Gamma_1$.
(4) *For type environments* $\Gamma_0$, $\Gamma_1$, $\Gamma_0'$, *and* $\Gamma_1'$, *if* $\Gamma_0 <: \Gamma_0'$ *and* $\Gamma_1 <: \Gamma_1'$, *then* $\Gamma_0 \mid \Gamma_1 <: \Gamma_0' \mid \Gamma_1'$.
(5) *For type environments* $\Gamma_0$, $\Gamma_1$, *and* $\Gamma_2$, $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2 <: \Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)$.
(6) *For type environments* $\Gamma$ *and* $\Gamma'$, *if* $\Gamma <: \Gamma'$, *then* $*\Gamma <: *\Gamma'$.
(7) *For type environments* $\Gamma$, $*\Gamma <: *\Gamma \mid \Gamma$.
(8) *For type environments* $\Gamma$ *and* $\Gamma'$, *if* $\Gamma <: \Gamma'$, *then* $\Gamma, x : \tau <: \Gamma', x : \tau$.
(9) *For type environments* $\Gamma$ *and* $\Gamma'$, *if* $(\Gamma, x : \tau) <: (\Gamma', x : \tau)$, *then* $\Gamma <: \Gamma'$.
(10) *For a type environment* $\Gamma$, $\uparrow^{(t_I,t_O)} \Gamma <: \Gamma$.
(11) *For a type environment* $\Gamma$, $\uparrow \Gamma <: \Gamma$.

*Proof.* We show each claim.
(1) We show $\Gamma_0 \mid \Gamma_1 <: \Gamma_1 \mid \Gamma_0$.
(a) Since $\mathrm{Dom}(\Gamma_0 \mid \Gamma_1) = \mathrm{Dom}(\Gamma_0) \cup \mathrm{Dom}(\Gamma_1) = \mathrm{Dom}(\Gamma_1 \mid \Gamma_0)$, we have $\mathrm{Dom}(\Gamma_0 \mid \Gamma_1) \supseteq \mathrm{Dom}(\Gamma_1 \mid \Gamma_0)$.
(b) Let $x \in \mathrm{Dom}(\Gamma_1 \mid \Gamma_0)$.

Assume $x \in \mathrm{Dom}(\Gamma_1) \cap \mathrm{Dom}(\Gamma_0)$. Then, we have $\Gamma_0 \mid \Gamma_1(x) = \Gamma_0(x) \mid \Gamma_1(x)$ and $\Gamma_1 \mid \Gamma_0(x) = \Gamma_1(x) \mid \Gamma_0(x)$. By Proposition C.1 (1), we have $\Gamma_0(x) \mid \Gamma_1(x) <: \Gamma_1(x) \mid \Gamma_0(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_1) \setminus \mathrm{Dom}(\Gamma_0)$. Then, we have $\Gamma_0 \mid \Gamma_1(x) = \Gamma_1(x)$ and $\Gamma_1 \mid \Gamma_0(x) = \Gamma_1(x)$. Hence, $\Gamma_0(x) \mid \Gamma_1(x) <: \Gamma_1(x) \mid \Gamma_0(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_0) \setminus \mathrm{Dom}(\Gamma_1)$. Then, we have $\Gamma_0 \mid \Gamma_1(x) = \Gamma_0(x)$ and $\Gamma_1 \mid \Gamma_0(x) = \Gamma_0(x)$. Hence, $\Gamma_0(x) \mid \Gamma_1(x) <: \Gamma_1(x) \mid \Gamma_0(x)$.

(c) $\mathrm{Dom}(\Gamma_0 \mid \Gamma_1) = \mathrm{Dom}(\Gamma_1 \mid \Gamma_0)$. Then $\mathrm{Dom}(\Gamma_0 \mid \Gamma_1) \setminus \mathrm{Dom}(\Gamma_1 \mid \Gamma_0) = \emptyset$. Thus, Definition 3.12 (c) holds obviously.

(2) We show $\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2) <: (\Gamma_0 \mid \Gamma_1) \mid \Gamma_2$.

(a) We see

$$\mathrm{Dom}(\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)) = \mathrm{Dom}(\Gamma_0) \cup \mathrm{Dom}(\Gamma_1) \cup \mathrm{Dom}(\Gamma_2) = \mathrm{Dom}((\Gamma_0 \mid \Gamma_1) \mid \Gamma_2).$$

Then, we have

$$\mathrm{Dom}(\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)) \supseteq \mathrm{Dom}((\Gamma_0 \mid \Gamma_1) \mid \Gamma_2).$$

(b) Let $x \in \mathrm{Dom}((\Gamma_0 \mid \Gamma_1) \mid \Gamma_2)$.

Assume $x \in \mathrm{Dom}(\Gamma_0 \mid \Gamma_1) \cap \mathrm{Dom}(\Gamma_2)$. Then $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_0 \mid \Gamma_1(x) \mid \Gamma_2(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_0) \cap \mathrm{Dom}(\Gamma_1)$. Then $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = (\Gamma_0(x) \mid \Gamma_1(x)) \mid \Gamma_2(x)$. By Proposition C.1 (2), $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_0(x) \mid (\Gamma_1(x) \mid \Gamma_2(x))$. Since $\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x) = \Gamma_0(x) \mid (\Gamma_1(x) \mid \Gamma_2(x))$, we have $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_0) \setminus \mathrm{Dom}(\Gamma_1)$. Then $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_0(x) \mid \Gamma_2(x)$. Since $\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x) = \Gamma_0 \mid \Gamma_2(x)$, we have $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_1) \setminus \mathrm{Dom}(\Gamma_0)$. Then $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_1(x) \mid \Gamma_2(x)$. Since $\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x) = \Gamma_1 \mid \Gamma_2(x)$, we have $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_0 \mid \Gamma_1) \setminus \mathrm{Dom}(\Gamma_2)$. Then $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_0 \mid \Gamma_1(x)$. Since $\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x) = \Gamma_0 \mid \Gamma_1(x)$, we have $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_2) \setminus \mathrm{Dom}(\Gamma_0 \mid \Gamma_1)$. Then $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_2(x)$. Since $\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x) = \Gamma_2(x)$, we have $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2(x) = \Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)(x)$.

(c) $\mathrm{Dom}(\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)) = \mathrm{Dom}((\Gamma_0 \mid \Gamma_1) \mid \Gamma_2)$. Then $\mathrm{Dom}(\Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)) \setminus \mathrm{Dom}((\Gamma_0 \mid \Gamma_1) \mid \Gamma_2) = \emptyset$. Thus, Definition 3.12 (c) holds obviously.

(3) Assume $\Gamma_0 <: \Gamma_0'$. We show $\Gamma_0 \mid \Gamma_1 <: \Gamma_0' \mid \Gamma_1$.

(a) Since $\Gamma_0 <: \Gamma_0'$, we have $\mathrm{Dom}(\Gamma_0) \supseteq \mathrm{Dom}(\Gamma_0')$. Thus,

$$\mathrm{Dom}(\Gamma_0 \mid \Gamma_1) = \mathrm{Dom}(\Gamma_0) \cup \mathrm{Dom}(\Gamma_1) \supseteq \mathrm{Dom}(\Gamma_0') \cup \mathrm{Dom}(\Gamma_1) = \mathrm{Dom}(\Gamma_0' \mid \Gamma_1).$$

(b) Let $x \in \mathrm{Dom}(\Gamma_0' \mid \Gamma_1)$. Since $\mathrm{Dom}(\Gamma_0 \mid \Gamma_1) \supseteq \mathrm{Dom}(\Gamma_0' \mid \Gamma_1)$, we have $x \in \mathrm{Dom}(\Gamma_0 \mid \Gamma_1)$.

Assume $x \in \mathrm{Dom}(\Gamma_0') \cap \mathrm{Dom}(\Gamma_1)$. Then, we have $\Gamma_0' \mid \Gamma_1(x) = \Gamma_0'(x) \mid \Gamma_1(x)$. Since $\mathrm{Dom}(\Gamma_0) \supseteq \mathrm{Dom}(\Gamma_0')$, we have $x \in \mathrm{Dom}(\Gamma_0) \cap \mathrm{Dom}(\Gamma_1)$. Then, we see $\Gamma_0 \mid \Gamma_1(x) = \Gamma_0(x) \mid \Gamma_1(x)$. Since $\Gamma_0 <: \Gamma_0'$, we have $\Gamma_0(x) <: \Gamma_0'(x)$. By Proposition C.1 (3), $\Gamma_0(x) \mid \Gamma_1(x) <: \Gamma_0'(x) \mid \Gamma_1(x)$. Thus, $\Gamma_0 \mid \Gamma_1(x) <: \Gamma_0' \mid \Gamma_1(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_0') \setminus \mathrm{Dom}(\Gamma_1)$. Then $\Gamma_0' \mid \Gamma_1(x) = \Gamma_0'(x)$. Since $\mathrm{Dom}(\Gamma_0) \supseteq \mathrm{Dom}(\Gamma_0')$, we have $x \in \mathrm{Dom}(\Gamma_0') \setminus \mathrm{Dom}(\Gamma_1)$. Then $\Gamma_0 \mid \Gamma_1(x) = \Gamma_0(x)$. Since $\Gamma_0 <: \Gamma_0'$, we have $\Gamma_0(x) <: \Gamma_0'(x)$. Thus, $\Gamma_0 \mid \Gamma_1(x) <: \Gamma_0' \mid \Gamma_1(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_1) \setminus \mathrm{Dom}(\Gamma_0')$. Then $\Gamma_0' \mid \Gamma_1(x) = \Gamma_1(x)$.

Assume $x \in \mathrm{Dom}(\Gamma_0)$. Then $\Gamma_0 \mid \Gamma_1(x) = \Gamma_0(x) \mid \Gamma_1(x)$. Since $x \in \mathrm{Dom}(\Gamma_0) \setminus \mathrm{Dom}(\Gamma_0')$, and $\Gamma_0 <: \Gamma_0'$, we have $\mathrm{ob}(\Gamma_0(x)) = \infty$. By Proposition C.1 (5), we see $\Gamma_0(x) \mid \Gamma_1(x) <: \Gamma_1(x)$. Thus, $\Gamma_0 \mid \Gamma_1(x) <: \Gamma_0' \mid \Gamma_1(x)$.

Assume $x \notin \mathrm{Dom}(\Gamma_0)$. Then $\Gamma_0 \mid \Gamma_1(x) = \Gamma_1(x)$. Thus, $\Gamma_0 \mid \Gamma_1(x) <: \Gamma_0' \mid \Gamma_1(x)$.

(c) Let $x \in \mathrm{Dom}(\Gamma_0 \mid \Gamma_1) \setminus \mathrm{Dom}(\Gamma_0' \mid \Gamma_1)$. Then $x \in (\mathrm{Dom}(\Gamma_0) \cup \mathrm{Dom}(\Gamma_1)) \setminus (\mathrm{Dom}(\Gamma_0') \cup \mathrm{Dom}(\Gamma_1))$. Hence, $x \in \mathrm{Dom}(\Gamma_0) \setminus \mathrm{Dom}(\Gamma_0')$ and $x \notin \mathrm{Dom}(\Gamma_1)$. Therefore, $\Gamma_0 \mid \Gamma_1(x) = \Gamma_0(x)$. Since $\Gamma_0 <: \Gamma_0'$, we have $\mathrm{ob}(\Gamma_0(x)) = \infty$. Thus, $\mathrm{ob}(\Gamma_0 \mid \Gamma_1(x)) = \infty$.

(4) Assume $\Gamma_0 <: \Gamma_0'$ and $\Gamma_1 <: \Gamma_1'$. By this proposition (3), $\Gamma_0 \mid \Gamma_1 <: \Gamma_0' \mid \Gamma_1$. From this proposition (1), $\Gamma_0' \mid \Gamma_1 <: \Gamma_1 \mid \Gamma_0'$. This proposition (3) implies $\Gamma_1 \mid \Gamma_0' <: \Gamma_1' \mid \Gamma_0'$. From this proposition (1), $\Gamma_1' \mid \Gamma_0' <: \Gamma_0' \mid \Gamma_1'$. By transitivity, $\Gamma_0 \mid \Gamma_1 <: \Gamma_0' \mid \Gamma_1'$.

(5) By (1), (2), (4), and transitivity of $<:$, we have

$$\begin{aligned}(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2 &<: \Gamma_2 \mid (\Gamma_0 \mid \Gamma_1) \\ &<: \Gamma_2 \mid (\Gamma_1 \mid \Gamma_0) \\ &<: (\Gamma_2 \mid \Gamma_1) \mid \Gamma_0 \\ &<: \Gamma_0 \mid (\Gamma_2 \mid \Gamma_1) \\ &<: \Gamma_0 \mid (\Gamma_1 \mid \Gamma_2).\end{aligned}$$

Thus, $(\Gamma_0 \mid \Gamma_1) \mid \Gamma_2 <: \Gamma_0 \mid (\Gamma_1 \mid \Gamma_2)$.

(6) Assume $\Gamma <: \Gamma'$. We show $*\Gamma <: *\Gamma'$.

(a) Since $\Gamma <: \Gamma'$, we have $\mathrm{Dom}(\Gamma) \supseteq \mathrm{Dom}(\Gamma')$. Since $\mathrm{Dom}(*\Gamma) = \mathrm{Dom}(\Gamma)$ and $\mathrm{Dom}(*\Gamma') = \mathrm{Dom}(\Gamma')$, we have $\mathrm{Dom}(*\Gamma) \supseteq \mathrm{Dom}(*\Gamma')$.
(b) Let $x \in \mathrm{Dom}(*\Gamma')$. Since $\mathrm{Dom}(*\Gamma') = \mathrm{Dom}(\Gamma')$, we have $x \in \mathrm{Dom}(\Gamma')$. Since $\Gamma <: \Gamma'$, we see $\Gamma(x) <: \Gamma'(x)$. By Proposition C.1 (7), $*\Gamma(x) <: *\Gamma'(x)$. Then, we have $*\Gamma(x) <: *\Gamma'(x)$.
(c) Let $x \in \mathrm{Dom}(*\Gamma) \setminus \mathrm{Dom}(*\Gamma')$. Since $\mathrm{Dom}(*\Gamma) = \mathrm{Dom}(\Gamma)$ and $\mathrm{Dom}(*\Gamma') = \mathrm{Dom}(\Gamma')$, we have $x \in \mathrm{Dom}(\Gamma) \setminus \mathrm{Dom}(\Gamma')$. Since $\Gamma <: \Gamma'$, we see $\mathrm{ob}(\Gamma(x)) = \infty$. Then

$$\mathrm{ob}(*\Gamma(x)) = \mathrm{ob}(*\Gamma(x)) = \mathrm{ob}(\Gamma(x)) = \infty.$$

(7) We show $*\Gamma <: *\Gamma \mid \Gamma$.
(a) Since $\mathrm{Dom}(*\Gamma) = \mathrm{Dom}(\Gamma)$ and $\mathrm{Dom}(*\Gamma \mid \Gamma) = \mathrm{Dom}(*\Gamma) \cup \mathrm{Dom}(\Gamma) = \mathrm{Dom}(\Gamma) \cup \mathrm{Dom}(\Gamma) = \mathrm{Dom}(\Gamma)$, we have $\mathrm{Dom}(*\Gamma) \supseteq \mathrm{Dom}(*\Gamma \mid \Gamma)$.
(b) Let $x \in \mathrm{Dom}(*\Gamma \mid \Gamma)$. By Proposition C.1 (7), we have $*\Gamma(x) <: (*\Gamma \mid \Gamma)(x)$.
(c) $\mathrm{Dom}(*\Gamma) = \mathrm{Dom}(*\Gamma \mid \Gamma)$. Then $\mathrm{Dom}(*\Gamma) \setminus \mathrm{Dom}(*\Gamma \mid \Gamma) = \emptyset$. Thus, Definition 3.12 (c) holds obviously.
(8) Assume $\Gamma <: \Gamma'$. We show $(\Gamma, x : \tau) <: (\Gamma', x : \tau)$.
(a) Since $\Gamma <: \Gamma'$, we have $\mathrm{Dom}(\Gamma) \supseteq \mathrm{Dom}(\Gamma')$. Hence, $\mathrm{Dom}(\Gamma, x : \tau) \supseteq \mathrm{Dom}(\Gamma', x : \tau)$.
(b) Let $y \in \mathrm{Dom}(\Gamma', x : \tau)$. If $y = x$, then $(\Gamma', x : \tau)(y) = \tau = (\Gamma, x : \tau)(y)$. Assume $y \neq x$. Then $y \in \mathrm{Dom}(\Gamma')$. Since $\Gamma <: \Gamma'$, $\Gamma(y) <: \Gamma'(y)$. Thus, $(\Gamma, x : \tau)(y) <: (\Gamma', x : \tau)(y)$.
(c) Let $y \in \mathrm{Dom}(\Gamma, x : \tau) \setminus \mathrm{Dom}(\Gamma', x : \tau)$. Then, we have $y \in \mathrm{Dom}(\Gamma) \setminus \mathrm{Dom}(\Gamma')$. Since $\Gamma <: \Gamma'$, we see $\mathrm{ob}(\Gamma(y)) = \infty$. Thus, $\mathrm{ob}((\Gamma, x : \tau)(y)) = \infty$.
(9) Assume $(\Gamma, x : \tau) <: (\Gamma', x : \tau)$. Then $x \notin \mathrm{Dom}(\Gamma)$ and $x \notin \mathrm{Dom}(\Gamma')$. We show $\Gamma <: \Gamma'$.
(a) Since $(\Gamma, x : \tau) <: (\Gamma', x : \tau)$, $x \notin \mathrm{Dom}(\Gamma)$, and $x \notin \mathrm{Dom}(\Gamma')$, we have $\mathrm{Dom}(\Gamma) \supseteq \mathrm{Dom}(\Gamma')$.
(b) Let $y \in \mathrm{Dom}(\Gamma')$. Since $x \notin \mathrm{Dom}(\Gamma')$, we have $y \neq x$. We also see $y \in \mathrm{Dom}(\Gamma', x : \tau)$. Since $(\Gamma, x : \tau) <: (\Gamma', x : \tau)$, we have $(\Gamma', x : \tau)(y) <: (\Gamma, x : \tau)(y)$. Thus, $\Gamma'(y) <: \Gamma(y)$.
(c) Let $y \in \mathrm{Dom}(\Gamma) \setminus \mathrm{Dom}(\Gamma')$. Then, we have $y \in \mathrm{Dom}((\Gamma, x : \tau)) \setminus \mathrm{Dom}((\Gamma', x : \tau))$. Since $(\Gamma, x : \tau) <: (\Gamma', x : \tau)$, we see $\mathrm{ob}((\Gamma, x : \tau)(y)) = \infty$. Thus, $\mathrm{ob}(\Gamma(y)) = \infty$.
(10) We show $\uparrow^{(t_I, t_O)} \Gamma <: \Gamma$.
(a) Since $\mathrm{Dom}\left(\uparrow^{(t_I, t_O)} \Gamma\right) = \mathrm{Dom}(\Gamma)$, we have $\mathrm{Dom}\left(\uparrow^{(t_I, t_O)} \Gamma\right) \supseteq \mathrm{Dom}(\Gamma)$.
(b) Let $x \in \mathrm{Dom}(\Gamma)$. By Proposition C.1 (9), we have $\uparrow^{(t_I, t_O)} \Gamma(x) = \Gamma(x)$.
(c) $\mathrm{Dom}\left(\uparrow^{(t_I, t_O)} \Gamma\right) = \mathrm{Dom}(\Gamma)$. Then $\mathrm{Dom}\left(\uparrow^{(t_I, t_O)} \Gamma\right) \setminus \mathrm{Dom}(\Gamma) = \emptyset$. Thus, Definition 3.12 (c) holds obviously.
(11) We show $\uparrow \Gamma <: \Gamma$.
(a) Since $\mathrm{Dom}(\uparrow \Gamma) = \mathrm{Dom}(\Gamma)$, we have $\mathrm{Dom}(\uparrow \Gamma) \supseteq \mathrm{Dom}(\Gamma)$.
(b) Let $x \in \mathrm{Dom}(\Gamma)$. By Proposition C.1 (10), we have $\uparrow \Gamma(x) = \Gamma(x)$.
(c) $\mathrm{Dom}(\uparrow \Gamma) = \mathrm{Dom}(\Gamma)$. Then $\mathrm{Dom}(\uparrow \Gamma) \setminus \mathrm{Dom}(\Gamma) = \emptyset$. Thus, Definition 3.12 (c) holds obviously.

□

**Proposition C.3.** *For type environments $\Gamma_0$ and $\Gamma_1$, if $\Gamma_0 <: \Gamma_1$ and $\mathrm{rel}(\Gamma_0)$, then $\mathrm{rel}(\Gamma_1)$.*

*Proof.* Straightforward. □

**Lemma C.4.** *Let $\Gamma$, $\Delta$ be type environments and $L$ be a lattice of secrecy levels. Assume that both $\Gamma \parallel L$ and $\Delta \parallel L$ are $l$-secure. Then:*
*(1) $\Gamma \mid \Delta \parallel L$ is $l$-secure.*
*(2) $*\Gamma \parallel L$ is $l$-secure.*
*(3) $\uparrow^{(t_I, t_O)} \Gamma \parallel L$ is $l$-secure.*
*(4) $\uparrow \Gamma \parallel L$ is $l$-secure.*

*Proof.* Straightforward. □

# Appendix D. The details of proof of subject reduction

## D.1. Inversion lemma

**Lemma D.1** (Inversion). *Assume that $\Gamma \parallel L \rhd_m P$ is $l$-securely derivable.*
*(1) If $P \equiv \mathtt{0}$, then $\Gamma <: \emptyset$.*
*(2) If $P \equiv P_0 \mid P_1$, then there exist two type environments $\Gamma'_0$, $\Gamma'_1$ and $m' \in L$ such that $\Gamma <: \Gamma'_0 \mid \Gamma'_1$, $L' \sqsubseteq L$, and $m \leq_L m'$ hold, and that $\Gamma'_i \parallel L' \rhd_{m'} P_i$ is $l$-securely derivable for each $i = 0, 1$.*

(3) *If* $P \equiv x!(\tilde{v}).P_0$, *then there exist a type environments* $\Gamma'$, *secrecy levels* $l_0, m_0 \in L$, *types* $\tilde{\tau}$, *a usage* $U$ *and* $t_c \in \mathbb{N} \cup \{\infty\}$ *such that* $\Gamma <: \Gamma''$, $m \leq_L l_0$, *and* $m \leq_L m_0$, $\Gamma', x : \langle \tilde{\tau} \rangle^{l_0}/U \parallel L \rhd_{m_0} P_0$ *is* $l$*-securely derivable,* $\Gamma'' \parallel L$ *is* $l$*-secure, and* $t_c = \infty$ *implies* $l_0 \leq_L m_0$, *where* $\Gamma'' \equiv \left(\uparrow^{(t_c+1,t_c+1)} \Gamma' \mid \tilde{v} : \uparrow \tilde{\tau} \mid x : \langle \tilde{\tau} \rangle^{l_0}/O^0_{t_c} U\right)$.

(4) *If* $P \equiv x?(\tilde{y}).P_0$, *then there exist a type environments* $\Gamma'$, *secrecy levels* $l_0, m_0 \in L$, *types* $\tilde{\tau}$, *a usage* $U$ *and* $t_c \in \mathbb{N} \cup \{\infty\}$ *such that* $\Gamma <: \Gamma''$, $m \leq_L l_0$, *and* $m \leq_L m_0$ *hold,* $\Gamma', x : \langle \tilde{\tau} \rangle^{l_0}/U, \tilde{y} : \tilde{\tau} \parallel L \rhd_{m_0} P_0$ *is* $l$*-securely derivable,* $\Gamma'' \parallel L$ *is* $l$*-secure, and* $t_c = \infty$ *implies* $l_0 \leq_L m_0$, *where* $\Gamma'' \equiv \left(\uparrow^{(t_c+1,t_c+1)} \Gamma', x : \langle \tilde{\tau} \rangle^{l_0}/I^0_{t_c} U\right)$.

(5) *If* $P \equiv *P_0$, *then there exist a type environments* $\Gamma'$, *and* $m' \in L$ *such that* $m \leq_L m'$, *and* $\Gamma <: *\Gamma'$, *and* $\Gamma' \parallel L \rhd_{m'} P_0$ *is* $l$*-securely derivable.*

(6) *If* $P \equiv (\nu x : \xi)P_0$, *then there exist a type environments* $\Gamma'$, *a usage* $U$, *and* $m' \in L$ *such that* $m \leq_L m'$, $\mathrm{rel}(U)$ *and* $\Gamma <: \Gamma'$, *and* $\Gamma', x : \xi/U \parallel L \rhd_{m'} P_0$ *is* $l$*-securely derivable.*

(7) *If* $P \equiv \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)P_0$, *then there exist a type environments* $\Gamma'$, *and* $m' \in L$ *such that* $m \leq_L m'$ *and* $\Gamma <: \Gamma'$, $m' \leq_L l'$ *for any* $l' \in \tilde{l_1}, \tilde{l_2}$, *and* $\Gamma' \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right) L \rhd_{m'} P_0$ *is* $l$*-securely derivable.*

(8) *If* $P \equiv \mathtt{if}\, v\, \mathtt{then}\, Q_0\, \mathtt{else}\, Q_1$, *then there exist a type environments* $\Gamma'$, *and* $m' \in L$ *such that* $m \leq_L m'$, *and* $\Gamma <: \Gamma' \mid v : \mathtt{Bool}^{m'}$, *and* $\Gamma' \parallel L \rhd_{m'} Q_0$ *and* $\Gamma' \parallel L \rhd_{m'} Q_1$ *are* $l$*-securely derivable.*

*Proof.* By induction on the size of derivation tree of $\Gamma \parallel L \rhd_m P$. □

**Lemma D.2.** *If* $\Gamma \parallel L \rhd_m P$ *is* $l$*-securely derivable and* $x \notin \mathrm{FV}(P)$, *then* $\Gamma' \parallel L \rhd_m P$ *is* $l$*-securely derivable and* $\Gamma <: \Gamma'$, *where* $\Gamma'$ *is the restriction of* $\Gamma$ *to* $(\mathrm{Dom}(\Gamma) \setminus \{x\})$.

*Proof.* By induction on the size of derivation tree of $\Gamma \parallel L \rhd_m P$. □

**Lemma D.3.** *If* $\Gamma \parallel L \rhd_m P$ *is* $l$*-securely derivable and* $x \in \mathrm{FV}(P)$, *then* $x \in \mathrm{Dom}(\Gamma)$.

*Proof.* By induction on a derivation tree of $\Gamma \parallel L \rhd_m P$. □

## D.2. Proof of Lemma 4.2

We show Lemma 4.2.

Let $P$ and $P'$ be processes, $\Gamma$ be a type environment, $L$ be a lattice of secrecy levels. Let $m \in L$. Assume that $\Gamma \parallel L \rhd_m P$ is $l$-securely derivable and $P \preceq P'$. We show that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable. The proof is by induction on the construction of $P \preceq P'$. We consider cases according to the last rule of the construction of $P \preceq P'$.
Case 1. If $P' \equiv P$, the assumptions immediately imply that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.
Case 2. Assume that there exists a process $P''$ such that $P \preceq P''$ and $P'' \preceq P'$. By the induction hypothesis, $\Gamma \parallel L \rhd_m P''$ is $l$-securely derivable. Then $P'' \preceq P'$ and the induction hypothesis imply that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.
Case 3. (SP-Zero1). Assume $P' \equiv P \mid \mathsf{0}$. By assumption, there exists an $\bar{l}$-secure derivation tree $\pi$ of $\Gamma \parallel L \rhd_m P$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\begin{array}{c}\vdots\,\pi\\ \Gamma \parallel L \rhd_m P\end{array} \qquad \dfrac{}{\emptyset \parallel L \rhd_m \mathsf{0}}\,(\text{T-Zero})}{\Gamma \mid \emptyset \parallel L \rhd_m P \mid \mathsf{0}} \ .$$

Since $\Gamma \mid \emptyset \equiv \Gamma$, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

Assume $P \equiv P' \mid \mathsf{0}$. By Lemma D.1 (2), there exist two type environments $\Gamma'_0, \Gamma'_1$ and $m' \in L$ such that $\Gamma <: \Gamma'_0 | \Gamma'_1$ and $m \leq_L m'$ hold, and that $\Gamma'_0 \parallel L \rhd_{m'} P'$ and $\Gamma'_1 \parallel L \rhd_{m'} \mathsf{0}$ are $l$-securely derivable. By Lemma D.1 (1), we have $\Gamma'_1 <: \emptyset$. By Proposition C.2 (4), $\Gamma'_0 \mid \Gamma'_1 <: \Gamma'_0 \mid \emptyset$. Since $\Gamma'_0 \mid \emptyset \equiv \Gamma'_0$, we have $\Gamma'_0 \mid \Gamma'_1 <: \Gamma'_0$. By $\Gamma <: \Gamma'_0 \mid \Gamma'_1$, we have $\Gamma <: \Gamma'_0$. Let $\pi'$ be an $l$-secure derivation tree of $\Gamma'_0 \parallel L \rhd_{l'} P'$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\begin{array}{c}\vdots\,\pi'\\ \Gamma'_0 \parallel L \rhd_{m'} P'\end{array} \qquad \Gamma <: \Gamma'_0 \qquad m \leq_L m'}{\Gamma \parallel L \rhd_m P'}\,(\text{T-Weak}) \ .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is derivable.

Case 4. (SP-Zero2). Assume $P \equiv \mathsf{0}$ and $P' \equiv (\nu x : \xi)\mathsf{0}$. By Lemma D.1 (1), $\Gamma <: \emptyset$. We have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\dfrac{}{\emptyset \parallel L \rhd_m \mathsf{0}}\,(\text{T-Zero})}{\emptyset \parallel L \rhd_m P'}\,(\text{T-Weak}) \qquad \Gamma <: \emptyset}{\Gamma \parallel L \rhd_m P'}\,(\text{T-Weak}) \quad .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

Assume $P \equiv (\nu x : \xi)\mathsf{0}$ and $P' \equiv \mathsf{0}$. By Lemma D.1 (6), there exist a type environments $\Gamma'$, a usage $U$, and $m' \in L$ such that $m \leq_L m'$, $\mathrm{rel}(U)$ and $\Gamma <: \Gamma'$, and $\Gamma', x : \xi/U \parallel L \rhd_{m'} \mathsf{0}$ is $l$-securely derivable. By Lemma D.1 (1), $\Gamma', x : \xi/U <: \emptyset$. By Definition 3.12 (c), we have $\mathrm{ob}(\xi/U) = \infty$. Then $\Gamma' <: \Gamma', x : \xi/U$. Hence, we have $\Gamma' <: \emptyset$. Therefore, $\Gamma <: \emptyset$. We have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{}{\emptyset \parallel L \rhd_m \mathsf{0}}\,(\text{T-Zero}) \qquad \Gamma <: \emptyset \qquad m \leq_L m}{\Gamma \parallel L \rhd_m P'}\,(\text{T-Weak}) \quad .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

Case 5. (SP-Commut). Assume $P \equiv P_0 \mid P_1$ and $P' \equiv P_1 \mid P_0$. By Lemma D.1 (2), there exist two type environments $\Gamma'_0$, $\Gamma'_1$ and $m' \in L$ such that $\Gamma <: \Gamma'_0 \mid \Gamma'_1$ and $m \leq_L m'$ hold, and that $\Gamma'_i \parallel L \rhd_{m'} P_i$ is $l$-securely derivable for each $i = 0, 1$. By Proposition C.2 (1), $\Gamma'_0 \mid \Gamma'_1 <: \Gamma'_1 \mid \Gamma'_0$. Hence, $\Gamma <: \Gamma'_1 \mid \Gamma'_0$. Let $\pi_i$ be an $l$-secure derivation tree of $\Gamma'_i \parallel L \rhd_{m'} P_i$ for each $i = 0, 1$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\begin{array}{cc}\vdots\,\pi_1 & \vdots\,\pi_0 \\ \Gamma'_1 \parallel L \rhd_{m'} P_1 & \Gamma'_0 \parallel L \rhd_{m'} P_0\end{array}}{\Gamma'_1 \mid \Gamma'_0 \parallel L \rhd_{m'} P_1 \mid P_0}\,(\text{T-Par}) \qquad \Gamma <: \Gamma'_1 \mid \Gamma'_0 \qquad m \leq_L m'}{\Gamma \parallel L \rhd_m P'}\,(\text{T-Weak}) \quad .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

In case $P \equiv P_1 \mid P_0$ and $P' \equiv P_0 \mid P_1$, we have an $l$-secure derivation tree of $\Gamma \parallel L \rhd_m P'$ in the same way.

Case 6. (SP-Assoc). Assume $P \equiv (P_0 \mid P_1) \mid P_2$ and $P' \equiv P_0 \mid (P_1 \mid P_2)$. By Lemma D.1 (2), there exist two type environments $\Gamma'_{01}$, $\Gamma'_2$ and $m' \in L$ such that $\Gamma <: \Gamma'_{01} \mid \Gamma'_2$ and $m \leq_L m'$ hold, and that $\Gamma'_{01} \parallel L \rhd_{m'} P_0 \mid P_1$ and $\Gamma'_2 \parallel L \rhd_{m'} P_2$ are $l$-securely derivable. Because $\Gamma'_{01} \parallel L \rhd_{m'} P_0 \mid P_1$ is $l$-securely derivable, Lemma D.1 (2) implies that there exist two type environments $\Gamma''_0$, $\Gamma''_1$ and $m'' \in L$ such that $\Gamma'_{01} <: \Gamma''_0 \mid \Gamma''_1$, and $m' \leq_L m''$ hold, and that $\Gamma''_i \parallel L \rhd_{m''} P_i$ is $l$-securely derivable for each $i = 0, 1$. By Proposition C.2 (4) and transitivity of $<:$, we have $\Gamma <: (\Gamma''_0 \mid \Gamma''_1) \mid \Gamma'_2$. By Proposition C.2 (5) and transitivity of $<:$, we see $\Gamma <: \Gamma''_0 \mid (\Gamma''_1 \mid \Gamma'_2)$. Let $\pi_i$ be an $l$-secure derivation tree of $\Gamma''_i \parallel L \rhd_{m''} P_i$ for each $i = 0, 1$. Let $\pi_2$ be an $l$-secure derivation tree of $\Gamma'_2 \parallel L \rhd_{m'} P_2$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\dfrac{\vdots\,\pi_0}{\Gamma''_0 \parallel L \rhd_{m''} P_0}\,(\text{T-Weak})}{\Gamma''_0 \parallel L \rhd_{m'} P_0} \qquad \dfrac{\dfrac{\vdots\,\pi_1}{\Gamma''_1 \parallel L \rhd_{m''} P_1}\,(\text{T-Weak}) \qquad \vdots\,\pi_2}{\Gamma''_1 \parallel L \rhd_{m'} P_1 \qquad \Gamma'_2 \parallel L \rhd_{m'} P_2}\,(\text{T-Par})}{\Gamma''_1 \mid \Gamma'_2 \parallel L \rhd_{m'} P_1 \mid P_2}\,(\text{T-Par})}{\Gamma''_0 \mid (\Gamma''_1 \mid \Gamma'_2) \parallel L \rhd_{m'} P_0 \mid (P_1 \mid P_2)}\,(\text{T-Weak})}{\Gamma \parallel L \rhd_m P'}\,(\text{T-Weak}) \quad .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

Case 7. (SP-New). Assume $P \equiv (\nu x : \xi)(P_0) \mid P_1$, $P' \equiv (\nu x : \xi)(P_0 \mid P_1)$, and $x \notin \mathrm{FN}(P_1)$. By Lemma D.1 (2), there exist two type environments $\Gamma'_0$, $\Gamma'_1$ and $m' \in L$ such that $\Gamma <: \Gamma'_0 \mid \Gamma'_1$ and $m \leq_L m'$ hold, and that $\Gamma'_0 \parallel L \rhd_{m'} (\nu x : \xi)P_0$ and $\Gamma'_1 \parallel L \rhd_{m'} P_1$ are $l$-securely derivable. Because $\Gamma'_0 \parallel L \rhd_{m'} (\nu x : \xi)P_0$ is $l$-securely derivable, Lemma D.1 (6) implies that there exist a type environments $\Gamma''_0$, a usage $U$, and $m'' \in L$ such that $m' \leq_L m''$, $\mathrm{rel}(U)$ and $\Gamma'_0 <: \Gamma''_0$, and $\Gamma''_0, x : \xi/U \parallel L \rhd_{m''} P_0$ is $l$-securely derivable. Since $\Gamma'_1 \parallel L \rhd_{m'} P_1$ is $l$-securely derivable, and $x \notin \mathrm{FN}(P_1)$, Lemma D.2 implies that $\Gamma''_1 \parallel L \rhd_{m'} P_1$ is $l$-securely derivable and $\Gamma'_1 <: \Gamma''_1$,

where $\Gamma_1''$ is the restriction of $\Gamma_1'$ to $(\mathrm{Dom}(\Gamma_1') \setminus \{x\})$. Then $(\Gamma_0'', x : \xi/U) \mid \Gamma_1'' \equiv (\Gamma_0'' \mid \Gamma_1''), x : \xi/U$. Since $\Gamma_0' <: \Gamma_0''$ and $\Gamma_1' <: \Gamma_1''$, Proposition C.2 (4) implies that $\Gamma_0' \mid \Gamma_1' <: \Gamma_0'' \mid \Gamma_1''$. By transitivity of $<:$, we have $\Gamma <: \Gamma_0'' \mid \Gamma_1''$. Let $\pi_0$ be an $l$-secure derivation tree of $\Gamma_0'', x : \xi/U \parallel L \rhd_{m''} P_0$, and $\pi_1$ be an $l$-secure derivation tree of $\Gamma_1'' \parallel L \rhd_{m'} P_1$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\dfrac{\begin{array}{cc}\vdots\,\pi_0 & \vdots\,\pi_1 \\ \Gamma_0'', x : \xi/U \parallel L \rhd_{m''} P_0 & \Gamma_1'' \parallel L \rhd_{m''} P_1\end{array}}{(\Gamma_0'' \mid \Gamma_1''), x : \xi/U \parallel L \rhd_{m'} P_0 \mid P_1}\,(\text{T-Par})}{\Gamma_0'' \mid \Gamma_1'' \parallel L \rhd_{m'} (\nu x : \xi)(P_0 \mid P_1)}\,(\text{T-New})}{\Gamma \parallel L \rhd_m P'}\,(\text{T-Weak})\ .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

The case $P = (\nu x : \xi)(P_0 \mid P_1)$, $P' = (\nu x : \xi)(P_0) \mid P_1$, and $x \notin \mathrm{FN}(P_1)$ is straightforward.

Case 8. (SP-IfT). Assume $P = \mathtt{if}\,\mathrm{true}^{m''}\,\mathtt{then}\,P_0\,\mathtt{else}\,P_1$ and $P' = P_0$. By Lemma D.1 (8), there exist a type environments $\Gamma'$ and $m' \in L$ such that $m \leq_L m'$, and $\Gamma <: \Gamma' \mid \mathrm{true}^{m''} : \mathtt{Bool}^{m'}$, and $\Gamma' \parallel L \rhd_{m'} P_0$ and $\Gamma' \parallel L \rhd_{m'} P_1$ are $l$-securely derivable. Since the type of $\mathrm{true}^{m''}$ is $\mathtt{Bool}^{m''}$, we see $m'' = m'$ and $\Gamma' \mid \mathrm{true}^{m'} : \mathtt{Bool}^{m'} = \Gamma'$. Hence, $\Gamma <: \Gamma'$. Let $\pi$ be an $l$-secure derivation tree of $\Gamma' \parallel L \rhd_{m'} P_0$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\vdots\,\pi}{\Gamma' \parallel L \rhd_{m'} P_0}\,(\text{T-Weak})\ .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

Case 9. (SP-IfF). Assume $P = \mathtt{if}\,\mathrm{false}^{m''}\,\mathtt{then}\,P_0\,\mathtt{else}\,P_1$ and $P' = P_1$. By Lemma D.1 (8), there exist a type environments $\Gamma'$, and $m' \in L$ such that $m \leq_L m'$, and $\Gamma <: \Gamma' \mid \mathrm{false}^{m''} : \mathtt{Bool}^{m'}$, and $\Gamma' \parallel L \rhd_{m'} P_0$ and $\Gamma' \parallel L \rhd_{m'} P_1$ are $l$-securely derivable. Since the type of $\mathrm{false}^{m''}$ is $\mathtt{Bool}^{m''}$, we see $m'' = m'$ and $\Gamma' \mid \mathrm{false}^{m'} : \mathtt{Bool}^{m'} = \Gamma'$. Hence, $\Gamma <: \Gamma'$. Let $\pi$ be an $l$-secure derivation tree of $\Gamma' \parallel L \rhd_m P_1$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\vdots\,\pi}{\Gamma' \parallel L \rhd_{m'} P_1}\,(\text{T-Weak})\ .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

Case 10. (SP-Rep). Assume $P = *P_0$ and $P' = *P_0 \mid P_0$. By Lemma D.1 (5), there exist a type environments $\Gamma'$, and $m' \in L$ such that $m \leq_L m'$, and $\Gamma <: *\Gamma'$, and $\Gamma' \parallel L \rhd_{m'} P_0$ is $l$-securely derivable. By Proposition C.2 (7), we have $*\Gamma' <: *\Gamma' \mid \Gamma'$. Hence, we have $\Gamma <: *\Gamma' \mid \Gamma'$. Let $\pi$ be an $l$-secure derivation tree of $\Gamma' \parallel L \rhd_{m'} P_0$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\dfrac{\begin{array}{cc}\vdots\,\pi & \\ \Gamma' \parallel L \rhd_{m'} P_0 & \end{array}}{*\Gamma' \parallel L \rhd_{m'} *P_0}\,(\text{T-Rep}) & \begin{array}{c}\vdots\,\pi \\ \Gamma' \parallel L \rhd_{m'} P_0\end{array}}{*\Gamma' \mid \Gamma' \parallel L \rhd_{m'} *P_0 \mid P_0}\,(\text{T-Par})}{\Gamma \parallel L \rhd_m P'}\,(\text{T-Weak})\ .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

Case 11. (SP-Par). Assume $P = P_0 \mid Q$ and $P' = P_1 \mid Q$ with $P_0 \preceq P_1$. By Lemma D.1 (2), there exist two type environments $\Gamma'$, $\Gamma''$ and $m' \in L$ such that $\Gamma <: \Gamma' \mid \Gamma''$ and $m \leq_L m'$ hold, and that $\Gamma' \parallel L \rhd_{m'} P_0$ and $\Gamma'' \parallel L \rhd_{m'} Q$ are $l$-securely derivable. Since $P_0 \preceq P_1$, the induction hypothesis implies that $\Gamma' \parallel L \rhd_{m'} P_1$ is $l$-securely derivable.

Let $\pi_1$ be an $l$-secure derivation tree of $\Gamma' \parallel L \rhd_{m'} P_1$, and $\pi$ be an $l$-secure derivation tree of $\Gamma'' \parallel L \rhd_{m'} Q$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\begin{array}{cc}\vdots\,\pi_1 & \vdots\,\pi \\ \Gamma' \parallel L \rhd_{m'} P_1 & \Gamma'' \parallel L \rhd_{m'} Q\end{array}}{\Gamma' \mid \Gamma'' \parallel L \rhd_{m'} P_1 \mid Q}\,(\text{T-Par})}{\Gamma \parallel L \rhd_m P'}\,(\text{T-Weak})\ .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

Case 12. (SP-CNew). Assume $P = (\nu x : \xi)P_0$ and $P' = (\nu x : \xi)P_1$ with $P_0 \preceq P_1$. By Lemma D.1 (6), there exist a type environments $\Gamma'$, a usage $U$, and $m' \in L$ such that $m \leq_L m'$, $\mathrm{rel}(U)$ and $\Gamma <: \Gamma'$, and $\Gamma', x : \xi/U \parallel L \rhd_{m'} P_0$ is $l$-securely derivable. Since $P_0 \preceq P_1$, the induction hypothesis implies that $\Gamma', x : \xi/U \parallel L \rhd_{m'} P_1$ is $l$-securely derivable. Let $\pi_1$ be an $l$-secure derivation tree of $\Gamma', x : \xi/U \parallel L \rhd_{m'} P_1$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\,\pi_1 \\ \Gamma', x : \xi/U \parallel L \rhd_{m'} P_1\end{array}}{\Gamma' \parallel L \rhd_{m'} (\nu x : \xi)P_1}\,(\text{T-New})}{\Gamma \parallel L \rhd_m P'}\,(\text{T-Weak})\ .$$

Thus, we see that $\Gamma \parallel L \rhd_m P'$ is $l$-securely derivable.

## D.3. Proof of substitution lemma

**Lemma D.4.** *For type environments $\Gamma_0$, $\Gamma_1$, a tuple of variables $\tilde{x} = (x_0, \ldots, x_n)$, and values $\tilde{v} = (v_0, \ldots, v_n)$, if $\Gamma_0[\tilde{x} \mapsto \tilde{v}]$ is well-defined and $\Gamma_0 <: \Gamma_1$, then $\Gamma_1[\tilde{x} \mapsto \tilde{v}]$ is well-defined and $\Gamma_0[\tilde{x} \mapsto \tilde{v}] <: \Gamma_1[\tilde{x} \mapsto \tilde{v}]$.*

*Proof.* For type environments $\Gamma_0$, $\Gamma_1$, a tuple of variables $\tilde{x} = (x_0, \ldots, x_n)$, and values $\tilde{v} = (v_0, \ldots, v_n)$, assume that $\Gamma_0[\tilde{x} \mapsto \tilde{v}]$ is well-defined and $\Gamma_0 <: \Gamma_1$. Let

$$D_j = (\mathrm{Dom}(\Gamma_j) \setminus \{x_0, \ldots, x_n\}) \cup \{v_i \mid x_i \in \mathrm{Dom}(\Gamma_j)\}$$

for $j = 0, 1$. We note that $D_0 \supseteq D_1$ because of $\mathrm{Dom}(\Gamma_0) \supseteq \mathrm{Dom}(\Gamma_1)$.

We show that $\Gamma_1[\tilde{x} \mapsto \tilde{v}]$ is well-defined. By the assumption $\Gamma_0 <: \Gamma_1$, we have $\mathrm{Dom}(\Gamma_0) \supseteq \mathrm{Dom}(\Gamma_1)$ and $\Gamma_0(w) <: \Gamma_1(w)$ for each $w \in \mathrm{Dom}(\Gamma_0)$. For each $w \in \mathrm{Dom}(\Gamma_1)$, by $\Gamma_0(w) <: \Gamma_1(w)$, we have $\Gamma_0(w) \sim \Gamma_1(w)$.

Let $w \in D_1$.

When $w \notin \tilde{v}$ holds, $\Gamma_1[\tilde{x} \mapsto \tilde{v}](w)$ is defined as $\Gamma_1(w)$.

Assume that $w \in \tilde{v}$, $w \notin \mathrm{Dom}(\Gamma_1)$, and $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_1)\} = \{x_{j_0}, \ldots, x_{j_k}\}$ with $0 \leq j_0 < \cdots < j_k \leq n$. We show $\Gamma_1(x_{i_0}) \sim \Gamma_1(x_{i_1})$ for any $i_0$, $i_1 \in \{j_0, \ldots, j_k\}$. From $D_1 \subseteq D_0$, we have $w \in D_0$. Let $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_0)\} = \{x_{j'_0}, \ldots, x_{j'_l}\}$ with $0 \leq j'_0 < \cdots < j'_l \leq n$. Since $\Gamma_0[\tilde{x} \mapsto \tilde{v}]$ is well-defined, either $\Gamma_0(x_{j'_0}) \mid \cdots \mid \Gamma_0(x_{j'_k})$ or $\Gamma_0(x_{j'_0}) \mid \cdots \mid \Gamma_0(x_{j'_l}) \mid \Gamma(w)$ is defined. Hence, $\Gamma_0(x_{i_0}) \sim \Gamma_0(x_{i_1})$ for any $i_0$, $i_1 \in \{0, \ldots, l\}$. Since $\{x_{j_0}, \ldots, x_{j_k}\} \subseteq \{x_{j'_0}, \ldots, x_{j'_l}\}$, we have $\Gamma_0(x_{i_0}) \sim \Gamma_0(x_{i_1})$ for any $i_0$, $i_1 \in \{0, \ldots, k\}$. Since $\Gamma_0(x) \sim \Gamma_1(x)$ for each $x \in \mathrm{Dom}(\Gamma_1)$, we see that $\Gamma_1(x_{i_0}) \sim \Gamma_0(x_{i_0}) \sim \Gamma_0(x_{i_1}) \sim \Gamma_1(x_{i_1})$. Therefore, $\Gamma_1(x_{j_0}) \mid \cdots \mid \Gamma_1(x_{j_k})$ is defined. Thus, $\Gamma_1[\tilde{x} \mapsto \tilde{v}](w)$ is defined.

In a similar way, we can show that $\Gamma_1[\tilde{x} \mapsto \tilde{v}](w)$ is defined in case $w \in \tilde{v}$ and $w \in \mathrm{Dom}(\Gamma_1)$.

We show $\Gamma_0[\tilde{x} \mapsto \tilde{v}] <: \Gamma_1[\tilde{x} \mapsto \tilde{v}]$.

(a) We see $\mathrm{Dom}(\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \supseteq \mathrm{Dom}(\Gamma_1[\tilde{x} \mapsto \tilde{v}])$ because of $\mathrm{Dom}(\Gamma_j[\tilde{x} \mapsto \tilde{v}]) = D_j$ for $j = 0, 1$.

(b) We show $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w) <: \Gamma_1[\tilde{x} \mapsto \tilde{v}](w)$ for each $w \in \mathrm{Dom}(\Gamma_1[\tilde{x} \mapsto \tilde{v}])$.

Let $w \in \mathrm{Dom}(\Gamma_1[\tilde{x} \mapsto \tilde{v}])$.

When $w \notin \tilde{v}$, we have $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w) = \Gamma_0(w) <: \Gamma_1(w) = \Gamma_1[\tilde{x} \mapsto \tilde{v}](w)$.

Assume that $w \in \tilde{v}$, $w \notin \mathrm{Dom}(\Gamma_1)$, and $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_1)\} = \{x_{j_0}, \ldots, x_{j_k}\}$ with $0 \leq j_0 < \cdots < j_k \leq n$. Then, we have $\Gamma_1[\tilde{x} \mapsto \tilde{v}](w) = \Gamma_1(x_{j_0}) \mid \cdots \mid \Gamma_1(x_{j_k})$. Assume $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_1)\} = \{y_0, \ldots, y_k\} \cup \{z_0, \ldots, z_l\}$. By Proposition C.1 (1) and (2), we have $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w) <: \Gamma_0(y_0) \mid \cdots \mid \Gamma_0(y_k) \mid \Gamma_0(z_0) \mid \cdots \mid \Gamma_0(z_l)$. Since $z_i \in \mathrm{Dom}(\Gamma_0) \setminus \mathrm{Dom}(\Gamma_1)$ for $i = 0, \ldots, l$, we have $\mathrm{ob}(\Gamma_0[\tilde{x} \mapsto \tilde{v}](z_i)) = \infty$. By Proposition C.1 (5), we have $\Gamma_0(y_0) \mid \cdots \mid \Gamma_0(y_k) \mid \Gamma_0(z_0) \mid \cdots \mid \Gamma_0(z_l) <: \Gamma_0(y_0) \mid \cdots \mid$

$\Gamma_0(y_k)$. Since $\Gamma_0(w) <: \Gamma_1(w)$ for any $w \in \mathrm{Dom}(\Gamma_1)$, we have $\Gamma_0(y_i) <: \Gamma_1(y_i)$ for $i = 0, \ldots, k$. From Proposition C.1 (3), we have $\Gamma_0(y_0) \mid \cdots \mid \Gamma_0(y_k) <: \Gamma_1(y_0) \mid \cdots \mid \Gamma_1(y_k)$. Then, we see $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w) <: \Gamma_1[\tilde{x} \mapsto \tilde{v}](w)$.

In a similar way, we can show $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w) <: \Gamma_1[\tilde{x} \mapsto \tilde{v}](w)$ in case $w \in \tilde{v}$ and $w \in \mathrm{Dom}(\Gamma_1)$.

(c) We show $\mathrm{ob}(\Gamma_0[\tilde{x} \mapsto \tilde{v}](w)) = \infty$ for each $w \in \mathrm{Dom}(\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \setminus \mathrm{Dom}(\Gamma_1[\tilde{x} \mapsto \tilde{v}])$.

Assume $w \in \mathrm{Dom}(\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \setminus \mathrm{Dom}(\Gamma_1[\tilde{x} \mapsto \tilde{v}])$.

Assuming $w \notin \tilde{v}$, we have $w \in \mathrm{Dom}(\Gamma_0) \setminus \mathrm{Dom}(\Gamma_1)$. In case, we have $\mathrm{ob}(\Gamma_0[\tilde{x} \mapsto \tilde{v}](w)) = \mathrm{ob}(\Gamma_0(w)) = \infty$ because of $\Gamma_0 <: \Gamma_1$.

Now, assume $w \in \tilde{v}$ and $w \notin \mathrm{Dom}(\Gamma_0)$. By $w \in \mathrm{Dom}(\Gamma_0[\tilde{x} \mapsto \tilde{v}])$, we see that

$$X = \{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_0)\}$$

is not empty. Assume $X = \{x_{j_0}, \ldots, x_{j_k}\}$ with $0 \leq j_0 < \cdots < j_k \leq n$. Then, we have $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w) = \Gamma_0(x_{j_0}) \mid \cdots \mid \Gamma_0(x_{j_k})$. By $w \notin \mathrm{Dom}(\Gamma_1[\tilde{x} \mapsto \tilde{v}])$, we see that $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_1)\}$ is empty. Hence, $x_{j_i} \notin \mathrm{Dom}(\Gamma_1)$ for $i = 0, \ldots, k$. Therefore, $\mathrm{ob}(\Gamma_0(x_{j_i})) = \infty$ for $i = 0, \ldots, k$. Thus, $\mathrm{ob}(\Gamma_0[\tilde{x} \mapsto \tilde{v}](w)) = \infty$.

Now, assume $w \in \tilde{v}$ and $w \in \mathrm{Dom}(\Gamma_0)$. Let $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_0)\} = \{x_{j_0}, \ldots, x_{j_k}\}$. Then, we have $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w) = \Gamma_0(x_{j_0}) \mid \cdots \mid \Gamma_0(x_{j_k}) \mid \Gamma_0(w)$. In a similar way to the case $w \notin \mathrm{Dom}(\Gamma_0)$, we have $\mathrm{ob}(\Gamma_0(x_{j_i})) = \infty$ for $i = 0, \ldots, k$. Since $w \notin \mathrm{Dom}(\Gamma_1)$, we have $\mathrm{ob}(\Gamma_0(w)) = \infty$. Thus, $\mathrm{ob}(\Gamma_0[\tilde{x} \mapsto \tilde{v}](w)) = \infty$. □

**Lemma D.5.** *(1) For a type environment $\Gamma$, a tuple of variables $\tilde{x} = (x_0, \ldots, x_n)$, and values $\tilde{v} = (v_0, \ldots, v_n)$, if $(*\Gamma)[\tilde{x} \mapsto \tilde{v}]$ is well-defined, then $\Gamma[\tilde{x} \mapsto \tilde{v}]$ is well-defined and $(*\Gamma)[\tilde{x} \mapsto \tilde{v}] <: *\Gamma[\tilde{x} \mapsto \tilde{v}]$.*

*(2) For type environments $\Gamma_0$ and $\Gamma_1$, a tuple of variables $\tilde{x} = (x_0, \ldots, x_n)$, and values $\tilde{v} = (v_0, \ldots, v_n)$, if $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}]$ is well-defined, then $\Gamma_0[\tilde{x} \mapsto \tilde{v}]$ and $\Gamma_1[\tilde{x} \mapsto \tilde{v}]$ are well-defined, and $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}] = (\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])$.*

*Proof.* We show each statement.

(1) For a type environment $\Gamma$, a tuple of variables $\tilde{x} = (x_0, \ldots, x_n)$, and values $\tilde{v} = (v_0, \ldots, v_n)$, assume that $(*\Gamma)[\tilde{x} \mapsto \tilde{v}]$ is well-defined.

We show that $\Gamma[\tilde{x} \mapsto \tilde{v}]$ is well-defined. Let $D = (\mathrm{Dom}(\Gamma) \setminus \{x_0, \ldots, x_n\}) \cup \{v_i \mid x_i \in \mathrm{Dom}(\Gamma)\}$. Since $\mathrm{Dom}(*\Gamma) = \mathrm{Dom}(\Gamma)$ and $(*\Gamma)[\tilde{x} \mapsto \tilde{v}]$ is well-defined, $\mathrm{Dom}((*\Gamma)[\tilde{x} \mapsto \tilde{v}]) = D$.

Let $w \in D$.

When $w \notin \tilde{v}$ holds, $\Gamma[\tilde{x} \mapsto \tilde{v}](w) = \Gamma(w)$. Hence, $\Gamma[\tilde{x} \mapsto \tilde{v}](w)$ is defined.

Assume that $w \in \tilde{v}$, $w \notin \mathrm{Dom}(\Gamma)$, and $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma)\} = \{x_{j_0}, \ldots, x_{j_k}\}$ with $0 \leq j_0 < \cdots < j_k \leq n$. In this case, $w \notin \mathrm{Dom}(*\Gamma)$. Then $(*\Gamma)[\tilde{x} \mapsto \tilde{v}](w) = (*\Gamma)(x_{j_0}) \mid \cdots \mid (*\Gamma)(x_{j_k})$. Since $(*\Gamma)[\tilde{x} \mapsto \tilde{v}]$ is well-defined, $*\Gamma(x_{j_0}) \mid \cdots \mid *\Gamma(x_{j_k})$ is defined. Then, we can show that $\Gamma(x_{j_0}) \mid \cdots \mid \Gamma(x_{j_k})$ is defined. Therefore, $\Gamma[\tilde{x} \mapsto \tilde{v}](w)$ is defined and $\Gamma[\tilde{x} \mapsto \tilde{v}](w) = \Gamma(x_{j_0}) \mid \cdots \mid \Gamma(x_{j_k})$.

In a similar way, we can show that $\Gamma[\tilde{x} \mapsto \tilde{v}](w)$ is defined in case $w \in \tilde{v}$ and $w \in \mathrm{Dom}(\Gamma)$.

We show $(*\Gamma)[\tilde{x} \mapsto \tilde{v}] <: *\Gamma[\tilde{x} \mapsto \tilde{v}]$.

(a) We have

$$\begin{aligned}\mathrm{Dom}((*\Gamma)[\tilde{x} \mapsto \tilde{v}]) &= D \\ &= \mathrm{Dom}(\Gamma[\tilde{x} \mapsto \tilde{v}]) \\ &= \mathrm{Dom}(*\Gamma[\tilde{x} \mapsto \tilde{v}]).\end{aligned}$$

Hence, $\mathrm{Dom}((*\Gamma)[\tilde{x} \mapsto \tilde{v}]) \supseteq \mathrm{Dom}(*\Gamma[\tilde{x} \mapsto \tilde{v}])$.

(b) Let $w \in \mathrm{Dom}(*\Gamma[\tilde{x} \mapsto \tilde{v}])$. Then $w \in D$.

In case $w \notin \tilde{v}$, we have

$$\begin{aligned}(*\Gamma)[\tilde{x} \mapsto \tilde{v}](w) &= *\Gamma(w) \\ &= *\Gamma(w) \\ &= *\Gamma[\tilde{x} \mapsto \tilde{v}](w).\end{aligned}$$

Then, we have $(*\Gamma)[\tilde{x} \mapsto \tilde{v}](w) <: *\Gamma[\tilde{x} \mapsto \tilde{v}](w)$.

Assume that $w \in \tilde{v}$, $w \notin \mathrm{Dom}(\Gamma)$, and $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_1)\} = \{x_{j_0}, \ldots, x_{j_k}\}$ with $0 \leq j_0 < \cdots < j_k \leq n$. Then $\Gamma[\tilde{x} \mapsto \tilde{v}](w) = \Gamma(x_{j_0}) \mid \cdots \mid \Gamma(x_{j_k})$ and $(*\Gamma)[\tilde{x} \mapsto \tilde{v}](w) = (*\Gamma)(x_{j_0}) \mid \cdots \mid (*\Gamma)(x_{j_k}) = *\Gamma(x_{j_0}) \mid \cdots \mid *\Gamma(x_{j_k})$. We also have $*\Gamma[\tilde{x} \mapsto \tilde{v}](w) = *\Gamma(x_{j_0}) \mid \cdots \mid \Gamma(x_{j_k})$. By Proposition C.1 (8), we have

$$*\Gamma(x_{j_0}) \mid \cdots \mid *\Gamma(x_{j_k}) <: *\Gamma(x_{j_0}) \mid \cdots \mid \Gamma(x_{j_k}).$$

Thus, $(*\Gamma)[\tilde{x} \mapsto \tilde{v}](w) <: *\Gamma[\tilde{x} \mapsto \tilde{v}](w)$.

In a similar way, we can show $(*\Gamma)[\tilde{x} \mapsto \tilde{v}](w) <: *\Gamma[\tilde{x} \mapsto \tilde{v}](w)$ in case $w \in \tilde{v}$ and $w \in \mathrm{Dom}(\Gamma)$.

(c) Because $\mathrm{Dom}((*\Gamma)[\tilde{x} \mapsto \tilde{v}]) = \mathrm{Dom}(*\Gamma[\tilde{x} \mapsto \tilde{v}])$, Definition 3.12 (c) holds obviously.

(2) For type environments $\Gamma_0$ and $\Gamma_1$, a tuple of variables $\tilde{x} = (x_0, \ldots, x_n)$, and values $\tilde{v} = (v_0, \ldots, v_n)$, assume that $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}]$ is well-defined.

We show that $\Gamma_0[\tilde{x} \mapsto \tilde{v}]$ is well-defined. Let $D_0 = (\mathrm{Dom}(\Gamma_0) \setminus \{x_0, \ldots, x_n\}) \cup \{v_i \mid x_i \in \mathrm{Dom}(\Gamma_0)\}$.

Let $w \in D_0$.

When $w \notin \tilde{v}$ holds, $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w) = \Gamma_0(w)$.

Assume that $w \in \tilde{v}$, $w \notin \mathrm{Dom}(\Gamma_0)$, and $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_0)\} = \{x_{j_0}, \ldots, x_{j_k}\}$ with $0 \leq j_0 < \cdots < j_k \leq n$. Let $\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}(\Gamma_0 \mid \Gamma_1)\} = \{x_{j'_0}, \ldots, x_{j'_l}\}$ with $0 \leq j'_0 < \cdots < j'_l \leq n$. Since $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}]$ is well-defined, we have $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}](w) = (\Gamma_0 \mid \Gamma_1)(x_{j'_0}) \mid \cdots \mid (\Gamma_0 \mid \Gamma_1)(x_{j'_l})$. Since $\{x_{j_0}, \ldots, x_{j_k}\} \subseteq \{x_{j'_0}, \ldots, x_{j'_l}\}$, we see that $\Gamma_0(x_{j_i})$ is defined for each $i = 0, \ldots, k$. Then, we have $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w) = \Gamma_0(x_{j_0}) \mid \cdots \mid \Gamma_0(x_{j_k})$. Thus, $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w)$ is defined.

In a similar way, we can show that $\Gamma_0[\tilde{x} \mapsto \tilde{v}](w)$ is defined in case $w \in \tilde{v}$ and $w \in \mathrm{Dom}(\Gamma_0)$. Thus, we see that $\Gamma_0[\tilde{x} \mapsto \tilde{v}]$ is well-defined.

In a similar way to the case $\Gamma_0[\tilde{x} \mapsto \tilde{v}]$, we can show that $\Gamma_1[\tilde{x} \mapsto \tilde{v}]$ is well-defined.

We show $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}] = (\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])$. Let

$$D_i = (\mathrm{Dom}(\Gamma_i) \setminus \{x_0, \ldots, x_n\}) \cup \{v_i \mid x_i \in \mathrm{Dom}(\Gamma_i)\}$$

for $i = 0, 1$. Then $\mathrm{Dom}((\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])) = D_0 \cup D_1$. Since $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}]$ is well-defined, we have

$$\begin{aligned}\mathrm{Dom}((\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}]) &= (\mathrm{Dom}(\Gamma_0 \mid \Gamma_1) \setminus \{x_0, \ldots, x_n\}) \cup \{v_0, \ldots, v_n\} \\ &= ((\mathrm{Dom}(\Gamma_0) \cup \mathrm{Dom}(\Gamma_1)) \setminus \{x_0, \ldots, x_n\}) \cup \{v_0, \ldots, v_n\}.\end{aligned}$$

Then

$$\begin{aligned}&((\mathrm{Dom}(\Gamma_0) \cup \mathrm{Dom}(\Gamma_1)) \setminus \{x_0, \ldots, x_n\}) \cup \{v_0, \ldots, v_n\} \\ &= ((\mathrm{Dom}(\Gamma_0) \setminus \{x_0, \ldots, x_n\}) \cup (\mathrm{Dom}(\Gamma_1) \setminus \{x_0, \ldots, x_n\})) \cup \{v_0, \ldots, v_n\} \\ &= ((\mathrm{Dom}(\Gamma_0) \setminus \{x_0, \ldots, x_n\}) \cup \{v_0, \ldots, v_n\}) \cup ((\mathrm{Dom}(\Gamma_1) \setminus \{x_0, \ldots, x_n\}) \cup \{v_0, \ldots, v_n\}) \\ &= D_0 \cup D_1.\end{aligned}$$

Hence, we have

$$\mathrm{Dom}((\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}]) = \mathrm{Dom}((\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])).$$

Let $w \in \mathrm{Dom}((\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}]))$. Then $w \in D_0 \cup D_1$.

If $w \notin \tilde{v}$, then we have

$$\begin{aligned}(\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])(w) &= \Gamma_0(w) \mid \Gamma_1(w) \\ &= \Gamma_0 \mid \Gamma_1(w) \\ &= (\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}](w).\end{aligned}$$

Hence, $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}](w) <: (\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])(w)$.

Assume that $w \in \tilde{v}$, $w \notin \mathrm{Dom}((\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}]))$, and

$$\{x_i \in \tilde{x} \mid w = v_i \text{ and } x_i \in \mathrm{Dom}((\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}]))\} = \{x_{j_0}, \ldots, x_{j_k}\}$$

with $0 \leq j_0 < \cdots < j_k \leq n$. Then

$$(\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])(w) = (\Gamma_0 \mid \Gamma_1)(x_{j_0}) \mid \cdots \mid (\Gamma_0 \mid \Gamma_1)(x_{j_k})$$

and

$$(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}](w) = (\Gamma_0 \mid \Gamma_1)(x_{j_0}) \mid \cdots \mid (\Gamma_0 \mid \Gamma_1)(x_{j_k}).$$

Hence, $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}](w) = (\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])(w)$.

In a similar way, we can show $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}](w) = (\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])(w)$ in case $w \in \tilde{v}$ and $w \in \mathrm{Dom}((\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}]))$. □

*Proof of Lemma 4.4.* Assume that $\Gamma \parallel L \rhd_m P$ is $l$-securely derivable, and $\Gamma[\tilde{x} \mapsto \tilde{v}]$ is well-defined. Let $\tilde{x} = (x_0, \ldots, x_n)$, $\tilde{v} = (v_0, \ldots, v_n)$, $\tau_i = \Gamma(x_i)$ for $i = 0, \ldots, n$, and $\tilde{\tau} = (\tau_0, \ldots, \tau_n)$.

We show the statement by induction on an $l$-secure derivation tree of $\Gamma \parallel L \rhd_m P$. We proceed by a case analysis of the rule used at the root.

Case 1. Assume that the rule used at the root is (T-Zero). Then $\Gamma = \Gamma[\tilde{x} \mapsto \tilde{v}] = \emptyset$ and $P = P[\tilde{x} \mapsto \tilde{v}] = \mathsf{0}$. Thus, $\Gamma[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P[\tilde{x} \mapsto \tilde{v}]$ is $l$-securely derivable.

Case 2. Assume that the rule used at the root is (T-New). Assume that $\Gamma, y : \xi/U \parallel L \rhd_m P'$ is the assumption of the rule instance, where $P = (\nu y : \xi)P'$ and $\mathrm{rel}(U)$ with $y \notin \tilde{x}$. Then, we see that $\Gamma, y : \xi/U \parallel L \rhd_m P'$ is $l$-securely derivable. By the induction hypothesis, $\Gamma[\tilde{x} \mapsto \tilde{v}], y : \xi/U \parallel L \rhd_m P'[\tilde{x} \mapsto \tilde{v}]$ is $l$-securely derivable. Let $\pi$ be an $l$-secure derivation tree of $\Gamma[\tilde{x} \mapsto \tilde{v}], y : \xi/U \parallel L \rhd_m P'[\tilde{x} \mapsto \tilde{v}]$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\begin{array}{c}\vdots\\ \pi \\ \vdots\end{array}}{\Gamma[\tilde{x} \mapsto \tilde{v}], y : \xi/U \parallel L \rhd_m P'[\tilde{x} \mapsto \tilde{v}]}\ (\text{T-New})}{\Gamma[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P[\tilde{x} \mapsto \tilde{v}]}\ (\text{T-New})$$

Thus, $\Gamma[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P[\tilde{x} \mapsto \tilde{v}]$ is $l$-securely derivable.
Case 3. Assume that the rule used at the root is (T-Rep). Assume that $\Gamma' \parallel L \rhd_m P'$ is the assumption of the rule instance, where $P = *P'$ and $\Gamma = *\Gamma'$. Then, we see that $\Gamma' \parallel L \rhd_m P'$ is $l$-securely derivable. By the induction hypothesis, $\Gamma'[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P'[\tilde{x} \mapsto \tilde{v}]$ is $l$-securely derivable. By Lemma D.5 (1), $\Gamma'[\tilde{x} \mapsto \tilde{v}]$ is well-defined and $(*\Gamma')[\tilde{x} \mapsto \tilde{v}] <: *\Gamma'[\tilde{x} \mapsto \tilde{v}]$. Let $\pi$ be an $l$-secure derivation tree of $\Gamma'[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P'[\tilde{x} \mapsto \tilde{v}]$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \pi \\ \vdots\end{array}}{\Gamma'[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P'[\tilde{x} \mapsto \tilde{v}]}\ (\text{T-Rep})}{*\Gamma'[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m *P'[\tilde{x} \mapsto \tilde{v}]}\ (\text{T-Weak})}{(*\Gamma')[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m *P'[\tilde{x} \mapsto \tilde{v}]}\ (\text{T-Weak})$$

Thus, $\Gamma[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P[\tilde{x} \mapsto \tilde{v}]$ is $l$-securely derivable.
Case 4. Assume that the rule used at the root is (T-Par). Assume that $\Gamma_0 \parallel L \rhd_m P_0$ and $\Gamma_1 \parallel L \rhd_m P_1$ are the assumptions of the rule instance, where $P = P_0 \mid P_1$ and $\Gamma = \Gamma_0 \mid \Gamma_1$. Then, we see that $\Gamma_0 \parallel L \rhd_m P_0$ and $\Gamma_1 \parallel L \rhd_m P_1$ are $l$-securely derivable. By the induction hypothesis, we see that $\Gamma_0[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P_0[\tilde{x} \mapsto \tilde{v}]$ and $\Gamma_1[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P_1[\tilde{x} \mapsto \tilde{v}]$ are $l$-securely derivable. By Lemma D.5 (2), we have $(\Gamma_0 \mid \Gamma_1)[\tilde{x} \mapsto \tilde{v}] = (\Gamma_0[\tilde{x} \mapsto \tilde{v}]) \mid (\Gamma_1[\tilde{x} \mapsto \tilde{v}])$. Let $\pi_i$ be an $l$-secure derivation tree of $\Gamma_0[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P_0[\tilde{x} \mapsto \tilde{v}]$ for $i = 0, 1$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\begin{array}{c}\vdots\\ \pi_0 \\ \vdots\end{array} \qquad \begin{array}{c}\vdots\\ \pi_1 \\ \vdots\end{array}}{\Gamma_0[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P_0[\tilde{x} \mapsto \tilde{v}] \qquad \Gamma_1[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P_1[\tilde{x} \mapsto \tilde{v}]}\ (\text{T-Par})}{\Gamma[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P[\tilde{x} \mapsto \tilde{v}]}\ (\text{T-Par})$$

Thus, $\Gamma[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P[\tilde{x} \mapsto \tilde{v}]$ is $l$-securely derivable.
Case 5. Assume that the rule used at the root is (T-If). Assume that $\Gamma' \parallel L \rhd_m Q_0$ and $\Gamma' \parallel L \rhd_m Q_1$ are the assumptions of the rule instance, where $P = \mathtt{if}\, w\, \mathtt{then}\, Q_0\, \mathtt{else}\, Q_1$ and $\Gamma = \Gamma' \mid w : \mathtt{Bool}^l$. Then, we see that $\Gamma' \parallel L \rhd_m Q_0$ and $\Gamma' \parallel L \rhd_m Q_1$ are $l$-securely derivable. By the induction hypothesis, $\Gamma'[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m Q_0[\tilde{x} \mapsto \tilde{v}]$ and $\Gamma'[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m Q_1[\tilde{x} \mapsto \tilde{v}]$ are $l$-securely derivable. Let $\pi_i$ be an $l$-secure derivation tree of $\Gamma'[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m Q_i[\tilde{x} \mapsto \tilde{v}]$ for each $i = 0, 1$. Then, we have an $l$-secure derivation tree as follows:

$$\dfrac{\begin{array}{c}\vdots\\ \pi_0 \\ \vdots\end{array} \qquad \begin{array}{c}\vdots\\ \pi_1 \\ \vdots\end{array}}{\Gamma'[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m Q_0[\tilde{x} \mapsto \tilde{v}] \qquad \Gamma'[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m Q_1[\tilde{x} \mapsto \tilde{v}]}\ (\text{T-If})}{\Gamma[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P[\tilde{x} \mapsto \tilde{v}]}\ (\text{T-If})$$

Thus, $\Gamma[\tilde{x} \mapsto \tilde{v}] \parallel L \rhd_m P[\tilde{x} \mapsto \tilde{v}]$ is $l$-securely derivable.
Case 6. Assume that the rule used at the root is (T-Out). Assume that $\Gamma_0, y : \langle \tilde{\tau} \rangle^{l_1}/U \parallel L \rhd_{m_1} P'$ is the assumption of the rule instance, where $P = y!\tilde{w}.P'$, $\Gamma = \uparrow^{(t_c+1, t_c+1)} \Gamma_0 \mid \tilde{w} : \uparrow \tilde{\tau} \mid y : \langle \tilde{\tau} \rangle^{l_1}/O^0_{t_c} U$, $l \leq_L l_1$ and $l \leq_L m_1$ and $t_c = \infty$ implies $l_1 \leq_L m_1$. Then, we see that $\Gamma_0, y : \langle \tilde{\tau} \rangle^{l_1}/U \parallel L \rhd_{m_1} P'$ is $l$-securely derivable. By the induction hypothesis, $\Gamma_0[\tilde{x} \mapsto \tilde{v}], y[\tilde{x} \mapsto \tilde{v}] : \langle \tilde{\tau} \rangle^{l_1}/U \parallel L \rhd_{m_1} P'[\tilde{x} \mapsto \tilde{v}]$ is $l$-securely derivable. Let $\pi$ be an $l$-secure derivation tree of $\Gamma_0[\tilde{x} \mapsto \tilde{v}], y[\tilde{x} \mapsto \tilde{v}] : \langle \tilde{\tau} \rangle^{l_1}/U \parallel L \rhd_{m_1} P'[\tilde{x} \mapsto \tilde{v}]$. Then, we have an $l$-secure derivation tree as follows:

$$\frac{\begin{array}{c}\vdots\\ \pi\\ \vdots\end{array}}{\Gamma_0[\tilde{x}\mapsto\tilde{v}], y[\tilde{x}\mapsto\tilde{v}]:\langle\tilde{\tau}\rangle^{l_1}/U \parallel L \rhd_{m_1} P'[\tilde{x}\mapsto\tilde{v}]}{\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_m y[\tilde{x}\mapsto\tilde{v}]!\tilde{w}[\tilde{x}\mapsto\tilde{v}].\, P'[\tilde{x}\mapsto\tilde{v}]}\ (\text{T-Out})$$

Thus, $\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_m P[\tilde{x}\mapsto\tilde{v}]$ is $l$-securely derivable.

Case 7. Assume that the rule used at the root is (T-In). Assume that $\Gamma_0, y:\langle\tilde{\tau}\rangle^{l_1}/U, \tilde{z}:\tilde{\tau} \parallel L \rhd_{m_1} P'$ is the assumption of the rule instance, where $l \leq_L l_1$, $l \leq_L m_1$, $P = y?\tilde{z}.P'$, and $\Gamma = \uparrow^{(t_c+1,t_c+1)}\Gamma_0, y:\langle\tilde{\tau}\rangle^{l_1}/I^0_{t_c}U$, and $t_c = \infty$ implies $l_1 \leq_L m_1$. We can assume $z' \notin \tilde{x}$ and $z' \notin \tilde{v}$ for any $z' \in \tilde{z}$. Since the assumption of the rule instance is $l$-securely derivable, we see that $\Gamma_0, y:\langle\tilde{\tau}\rangle^{l_1}/U, \tilde{z}:\tilde{\tau} \parallel L \rhd_{m_1} P'$ is $l$-securely derivable. Let $\Gamma' = \Gamma_0, y:\langle\tilde{\tau}\rangle^{l_1}/U, \tilde{z}:\tilde{\tau}$. Since we have $z' \notin \tilde{x}$ and $z' \notin \tilde{v}$ for any $z' \in \tilde{z}$, we see that $\Gamma'[\tilde{x}\mapsto\tilde{v}] = \Gamma_0[\tilde{x}\mapsto\tilde{v}], y[\tilde{x}\mapsto\tilde{v}]:\langle\tilde{\tau}\rangle^{l_1}/U, \tilde{z}:\tilde{\tau}$ is well-defined. By the induction hypothesis, we see that $\Gamma'[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_{m_1} P'[\tilde{x}\mapsto\tilde{v}]$ is $l$-securely derivable. Let $\pi$ be an $l$-secure derivation tree of $\Gamma'[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_{m_1} P'[\tilde{x}\mapsto\tilde{v}]$. Then, we have an $l$-secure derivation tree as follows:

$$\frac{\begin{array}{c}\vdots\\ \pi\\ \vdots\end{array}}{\Gamma'[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_{m_1} P'[\tilde{x}\mapsto\tilde{v}]}{\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_{m_1} y[\tilde{x}\mapsto\tilde{v}]?\tilde{z}.\, P'[\tilde{x}\mapsto\tilde{v}]}\ (\text{T-In})$$

Thus, $\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_l P[\tilde{x}\mapsto\tilde{v}]$ is $l$-securely derivable.

Case 8. Assume that the rule used at the root is (T-NewSec). Assume that $\Gamma \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L \rhd_m P'$ is the assumption of the rule instance, where $P = \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)P'$ and $l' \leq_L l_s$ for any $l' \in \tilde{l_1}, \tilde{l_2}$. Then, we see that $\Gamma \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L \rhd_m P'$ is $l$-securely derivable. By the induction hypothesis, we see that $\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L \rhd_m P'[\tilde{x}\mapsto\tilde{v}]$ is $l$-securely derivable. Let $\pi$ be an $l$-secure derivation tree of $\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L \rhd_m P'[\tilde{x}\mapsto\tilde{v}]$. Then, we have an $l$-secure derivation tree as follows:

$$\frac{\begin{array}{c}\vdots\\ \pi\\ \vdots\end{array}}{\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L \rhd_m P'[\tilde{x}\mapsto\tilde{v}]}{\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_m \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)P'[\tilde{x}\mapsto\tilde{v}]}\ (\text{T-NewSec})$$

Thus, $\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_m P[\tilde{x}\mapsto\tilde{v}]$ is $l$-securely derivable.

Case 9. Assume that the rule used at the root is (T-Weak). Assume that $\Gamma' \parallel L \rhd_{m'} P$ is the assumption of the rule instance, where $\Gamma <: \Gamma'$ and $l \leq_L m'$. Then, we see that $\Gamma' \parallel L \rhd_{m'} P$ is $l$-securely derivable. By the induction hypothesis, we see that $\Gamma'[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_{m'} P[\tilde{x}\mapsto\tilde{v}]$ is $l$-securely derivable. By Lemma D.4, $\Gamma'[\tilde{x}\mapsto\tilde{v}]$ is well-defined and $\Gamma[\tilde{x}\mapsto\tilde{v}] <: \Gamma'[\tilde{x}\mapsto\tilde{v}]$. Let $\pi$ be an $l$-secure derivation tree of $\Gamma'[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_{m'} P[\tilde{x}\mapsto\tilde{v}]$. Then, we have an $l$-secure derivation tree as follows:

$$\frac{\begin{array}{c}\vdots\\ \pi\\ \vdots\end{array}}{\Gamma'[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_{m'} P[\tilde{x}\mapsto\tilde{v}]}{\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_m P[\tilde{x}\mapsto\tilde{v}]}\ (\text{T-Weak})$$

Thus, $\Gamma[\tilde{x}\mapsto\tilde{v}] \parallel L \rhd_m P[\tilde{x}\mapsto\tilde{v}]$ is $l$-securely derivable. □

## D.4. Proof of subject reduction

**Lemma D.6.** *For type environments $\Gamma_0$, $\Gamma_0'$, and $\Gamma_1$, if $\Gamma_1 \longrightarrow \Gamma_1'$ and $\Gamma_0 <: \Gamma_1$, then there exists $\Gamma_0'$ such that $\Gamma_0 \longrightarrow \Gamma_0'$ and $\Gamma_0' <: \Gamma_1'$.*

*Proof.* Since $\Gamma_1 \longrightarrow \Gamma_1'$, there exist a name $x$, a core channel type $\xi$, and usages $U_1$, $U_1'$ such that $\Gamma_1(x) = \xi/U_1$, $\Gamma_1'(x) = \xi/U_1'$, and $U_1 \longrightarrow U_1'$. Since $\Gamma_0 <: \Gamma_1$, there exists a core channel type $\xi$, and a usage $U_0$ such that $\Gamma_0(x) = \xi/U_0$ and $U_0 <: U_1$. By Definition 3.7 (b), there exists a usage $U_0'$ such that $U_0 \longrightarrow U_0'$ and $U_0' <: U_1'$. Let $\Gamma_0' = \Gamma_0[x \mapsto \xi/U_0']$. Then $\Gamma_0 \longrightarrow \Gamma_0'$ and $\Gamma_0' <: \Gamma_1'$. □

**Lemma D.7.** *For type environments $\Gamma_0$, $\Gamma_0'$, and $\Gamma_1$, if $\Gamma_0 \longrightarrow \Gamma_0'$, then $\Gamma_0 \,|\, \Gamma_1 \longrightarrow \Gamma_0' \,|\, \Gamma_1$.*

*Proof.* Since $\Gamma_0 \longrightarrow \Gamma_0'$, there exist a name $x$, a core channel type $\xi$, and usages $U_0$, $U_0'$ such that $\Gamma_0(x) = \xi/U_0$, $\Gamma_0'(x) = \xi/U_0'$, and $U_0 \longrightarrow U_0'$.

Then $\Gamma_0 \,|\, \Gamma_1(x) = \xi/U_0$ or $\Gamma_0 \,|\, \Gamma_1(x) = \xi/U_0 \,|\, U_1$ with some usage $U_1$.

If $\Gamma_0 \,|\, \Gamma_1(x) = \xi/U_0$, then we have $\Gamma_0' \,|\, \Gamma_1(x) = \xi/U_0'$. Hence, $\Gamma_0 \,|\, \Gamma_1 \longrightarrow \Gamma_0' \,|\, \Gamma_1$.

If $\Gamma_0 \,|\, \Gamma_1(x) = \xi/U_0 \,|\, U_1$ with some usage $U_1$, then we have $\Gamma_0' \,|\, \Gamma_1(x) = \xi/U_0' \,|\, U_1$. Hence, $\Gamma_0 \,|\, \Gamma_1 \longrightarrow \Gamma_0' \,|\, \Gamma_1$. □

Now, we prove Proposition 4.5.

*Proof of Proposition 4.5.* Let $P$ and $P'$ be processes. Assume that $\Gamma \parallel L \rhd_m P$ is $l$-securely derivable and $(P, L) \longrightarrow (P', L')$. We show that there exist a type environment $\Gamma'$ such that either $\Gamma' = \Gamma$ or $\Gamma \longrightarrow \Gamma'$ and $\Gamma' \parallel L' \rhd_m P'$ is $l$-securely derivable.

We show the statement by induction on the construction of $(P, L) \longrightarrow (P', L')$. We proceed by a case analysis of the last rule used to construct $P \longrightarrow P'$.

Case 1. We consider the case (R-Com). In this case, $P = x!(v_0, \ldots, v_n).P_0 \,|\, x?(y_0, \ldots, y_n).P_1$, $P' = P_0 \,|\, P_1[y_0 \mapsto v_0, \ldots, y_n \mapsto v_n]$, and $L' = L$. Let $\tilde{y} = (y_0, \ldots, y_n)$ and $\tilde{v} = (v_0, \ldots, v_n)$.

By Lemma D.1 (2), there exist two type environments $\Gamma_0'$, $\Gamma_1'$ and $l' \in L$ such that $\Gamma <: \Gamma_0' \,|\, \Gamma_1'$ and $l \leq_L l'$ hold, and that $\Gamma_0' \parallel L \rhd_{m'} x!(v_0, \ldots, v_n).P_0$ and $\Gamma_1' \parallel L \rhd_{m'} x?(y_0, \ldots, y_n).P_1$ are $\check{l}$-securely derivable. By Lemma D.1 (3), there exist a type environments $\Gamma_0''$, $l_{00}'' \in L$, $m_{01}'' \in L$, types $\tilde{\tau}$, a usage $U$ and $t_c \in \mathbb{N} \cup \{\infty\}$ such that $\Gamma_0' <: \left(\uparrow^{(t_c+1, t_c+1)} \Gamma_0'' \,|\, \tilde{v} : \uparrow\tilde{\tau} \,|\, x : \langle\tilde{\tau}\rangle^{l_{00}''}/O^0_{t_c}U\right)$, $l_0 \leq_L l_{00}''$, and $l_0 \leq_L m_{01}''$, $\left(\uparrow^{(t_c+1, t_c+1)} \Gamma_0'' \,|\, \tilde{v} : \uparrow\tilde{\tau} \,|\, x : \langle\tilde{\tau}\rangle^{l_{00}''}/O^0_{t_c}U\right) \parallel L$ is $l$-secure, and $\Gamma_0'', x : \langle\tilde{\tau}\rangle^{l_{00}''}/U \parallel L \rhd_{m_{01}''} P_0$ is $l$-securely derivable, and $t_c = \infty$ implies $l_{00}'' \leq_L m_{01}''$. By Lemma D.1 (4), there exist a type environments $\Gamma_1''$ $l_{10}'' \in L$, $m_{11}'' \in L$, types $\tilde{\tau'}$, a usage $U'$ and $t_c' \in \mathbb{N} \cup \{\infty\}$ such that $\Gamma_1'' <: \left(\uparrow^{(t_c'+1, t_c'+1)} \Gamma_1'', x : \langle\tilde{\tau'}\rangle^{l_{10}''}/I^0_{t_c'}U'\right)$, $l_1 \leq_L l_{10}''$, and $l_1 \leq_L m_{11}''$, $\left(\uparrow^{(t_c'+1, t_c'+1)} \Gamma_1'', x : \langle\tilde{\tau'}\rangle^{l_{10}''}/I^0_{t_c'}U'\right) \parallel L$ is $\check{l}$-secure, $\Gamma_1'', x : \langle\tilde{\tau'}\rangle^{l_{10}''}/U, \tilde{y} : \tilde{\tau'} \parallel L \rhd_{m_{11}''} P_1$ is $l$-securely derivable, and $t_c' = \infty$ implies $l_{10}'' \leq_L m_{11}''$.

Since $\Gamma_0' <: \left(\uparrow^{(t_c+1, t_c+1)} \Gamma_0'' \,|\, \tilde{v} : \uparrow\tilde{\tau} \,|\, x : \langle\tilde{\tau}\rangle^{l_{00}''}/O^0_{t_c}U\right)$, we have $\Gamma_0'(x) \sim \langle\tilde{\tau}\rangle^{l_{00}'''}/O^0_{t_c}U$. Since $\Gamma_1' <: \left(\uparrow^{(t_c'+1, t_c'+1)} \Gamma_1''', x : \langle\tilde{\tau'}\rangle^{l_{10}'''}/I^0_{t_c'}U'\right)$, we have $\Gamma_1'(x) \sim \langle\tilde{\tau'}\rangle^{l_{10}''}/I^0_{t_c'}U'$. Since $\Gamma_0' \,|\, \Gamma_1'$ is defined, $\Gamma_0'(x) \sim \Gamma_1'(x)$. Hence, $\langle\tilde{\tau}\rangle^{l_{00}''}/O^0_{t_c}U \sim \langle\tilde{\tau'}\rangle^{l_{10}''}/I^0_{t_c'}U'$. Therefore, $\tilde{\tau} = \tilde{\tau'}$ and $l_{00}'' = l_{10}''$.

Let $\pi_0$ be an $\check{l}$-secure derivation tree of $\Gamma_0'', x : \langle\tilde{\tau}\rangle^{l_{00}''}/U \parallel L \rhd_{m_{01}''} P_0$, and $\pi_1$ be an $\check{l}$-secure derivation tree of $\Gamma_1'', x : \langle\tilde{\tau}\rangle^{l_{00}''}/U, \tilde{y} : \tilde{\tau} \parallel L \rhd_{m_{11}''} P_1$. We have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\dfrac{\vdots\,\pi_0}{\Gamma_0'', x : \langle\tilde{\tau}\rangle^{l_{00}''}/U \parallel L \rhd_{m_{01}''} P_0}}{\check{\Gamma}_0 \parallel L \rhd_{m_0} x!(v_0, \ldots, v_n).P_0}}{\check{\Gamma}_0 \parallel L \rhd_{m'} x!(v_0, \ldots, v_n).P_0} \quad \dfrac{\dfrac{\dfrac{\vdots\,\pi_1}{\Gamma_1'', x : \langle\tilde{\tau}\rangle^{l_{00}''}/U, \tilde{y} : \tilde{\tau} \parallel L \rhd_{m_{11}''} P_1}}{\check{\Gamma}_1 \parallel L \rhd_{m_1} x?(y_0, \ldots, y_n).P_1}}{\check{\Gamma}_1 \parallel L \rhd_{m'} x?(y_0, \ldots, y_n).P_1}}{\check{\Gamma}_0 \,|\, \check{\Gamma}_1 \parallel L \rhd_{m'} x!(v_0, \ldots, v_n).P_0 \,|\, x?(y_0, \ldots, y_n).P_1},$$

where $\check{\Gamma}_0 = \left(\uparrow^{(t_c+1, t_c+1)} \Gamma_0'' \,|\, \tilde{v} : \uparrow\tilde{\tau} \,|\, x : \langle\tilde{\tau}\rangle^{l_{00}''}/O^0_{t_c}U'\right)$ and $\check{\Gamma}_1 = \left(\uparrow^{(t_c'+1, t_c'+1)} \Gamma_1'', x : \langle\tilde{\tau}\rangle^{l_{00}''}/I^0_{t_c'}U'\right)$. Thus, we see that

$$\left(\uparrow^{(t_c+1, t_c+1)} \Gamma_0'' \,|\, \tilde{v} : \uparrow\tilde{\tau} \,|\, x : \langle\tilde{\tau}\rangle^{l_{00}''}/O^0_{t_c}U\right) \,|\, \left(\uparrow^{(t_c'+1, t_c'+1)} \Gamma_1'', x : \langle\tilde{\tau}\rangle^{l_{00}''}/I^0_{t_c'}U'\right) \parallel L \rhd_{m'} P$$

is $l$-securely derivable. Then

$$\left(\uparrow^{(t_c+1,t_c+1)}\Gamma_0'' \mid \tilde{v}:\uparrow\tilde{\tau} \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/O_{t_c}^0U\right) \mid \left(\uparrow^{(t_c'+1,t_c'+1)}\Gamma_1'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/I_{t_c'}^0U'\right)$$
$$<: \left(\uparrow^{(t_c+1,t_c+1)}\Gamma_0'' \mid \tilde{v}:\uparrow\tilde{\tau}\right) \mid \left(\uparrow^{(t_c'+1,t_c'+1)}\Gamma_1''\right) \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/(O_{t_c}^0U \mid I_{t_c'}^0U').$$

Hence, we have

$$\Gamma <: \left(\uparrow^{(t_c+1,t_c+1)}\Gamma_0'' \mid \tilde{v}:\uparrow\tilde{\tau}\right) \mid \left(\uparrow^{(t_c'+1,t_c'+1)}\Gamma_1''\right) \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/(O_{t_c}^0U \mid I_{t_c'}^0U').$$

Since $y_i \notin \mathrm{Dom}(\Gamma_1'')$, we have $\Gamma_1''[\tilde{y}\mapsto\tilde{v}] = \Gamma_1''$. By Lemma 4.4, we see that

$$\Gamma_1'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U' \mid \tilde{v}:\tilde{\tau} \parallel L \rhd_{m_{11}''} P_1[\tilde{y}\mapsto\tilde{v}]$$

is $l$-securely derivable. Let $\hat{\pi}_0$ be an $l$-secure derivation tree of $\Gamma_0'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U \parallel L \rhd_{m_{01}''} P_0$ and $\hat{\pi}_1$ be an $l$-secure derivation tree of $\Gamma_1'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U' \mid \tilde{v}:\tilde{\tau} \parallel L \rhd_{m_{11}''} P_1[\tilde{y}\mapsto\tilde{v}]$. We have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \hat{\pi}_0\\ \vdots\end{array}}{\Gamma_0'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U \parallel L \rhd_{m_{01}''} P_0} \quad \dfrac{\begin{array}{c}\vdots\\ \hat{\pi}_1\\ \vdots\end{array}}{\Gamma_1'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U' \mid \tilde{v}:\tilde{\tau} \parallel L \rhd_{m_{11}''} P_1[\tilde{y}\mapsto\tilde{v}]}}{\Gamma_0'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U \parallel L \rhd_{m'} P_0} \quad \dfrac{\Gamma_1'', x:\langle\tilde{\tau}'\rangle^{l_{00}''}/U' \mid \tilde{v}:\tilde{\tau} \parallel L \rhd_{m'} P_1[\tilde{y}\mapsto\tilde{v}]}{\left(\Gamma_0'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U\right) \mid \left(\Gamma_1'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U' \mid \tilde{v}:\tilde{\tau}\right) \parallel L \rhd_{m'} P_0 \mid P_1[\tilde{y}\mapsto\tilde{v}]}.$$

Thus, we see that

$$\left(\Gamma_0'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U\right) \mid \left(\Gamma_1'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U' \mid \tilde{v}:\tilde{\tau}\right) \parallel L \rhd_{m'} P'$$

is $l$-securely derivable. Then

$$(\Gamma_0'' \mid \Gamma_1'') \mid \tilde{v}:\tilde{\tau} \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/(U \mid U') <: \left(\Gamma_0'', x:\langle\tilde{\tau}\rangle^{l_{00}''}/U\right) \mid \left(\Gamma_1'', x:\langle\tilde{\tau}'\rangle^{l_{10}''}/U' \mid \tilde{v}:\tilde{\tau}\right).$$

By Proposition C.2 (10) and (11), we have

$$\left(\uparrow^{(t_c+1,t_c+1)}\Gamma_0'' \mid \tilde{v}:\uparrow\tilde{\tau}\right) \mid \left(\uparrow^{(t_c'+1,t_c'+1)}\Gamma_1''\right) \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/(U \mid U')$$
$$<: ((\Gamma_0'') \mid (\Gamma_1'')) \mid \tilde{v}:\tilde{\tau} \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/(U \mid U').$$

Hence,

$$\left(\uparrow^{(t_c+1,t_c+1)}\Gamma_0'' \mid \tilde{v}:\uparrow\tilde{\tau}\right) \mid \left(\uparrow^{(t_c'+1,t_c'+1)}\Gamma_1''\right) \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/(U \mid U') \parallel L \rhd_{m'} P'$$

is $l$-securely derivable.

Now,

$$\left(\uparrow^{(t_c+1,t_c+1)}\Gamma_0'' \mid \tilde{v}:\uparrow\tilde{\tau}\right) \mid \left(\uparrow^{(t_c'+1,t_c'+1)}\Gamma_1''\right) \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/(O_{t_c}^0U \mid I_{t_c'}^0U')$$
$$\longrightarrow \left(\uparrow^{(t_c+1,t_c+1)}\Gamma_0'' \mid \tilde{v}:\uparrow\tilde{\tau}\right) \mid \left(\uparrow^{(t_c'+1,t_c'+1)}\Gamma_1''\right) \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/(U \mid U').$$

By Lemma D.6, there exists $\Gamma'$ such that $\Gamma \longrightarrow \Gamma'$ and

$$\Gamma' <: \left(\uparrow^{(t_c+1,t_c+1)}\Gamma_0'' \mid \tilde{v}:\uparrow\tilde{\tau}\right) \mid \left(\uparrow^{(t_c'+1,t_c'+1)}\Gamma_1''\right) \mid x:\langle\tilde{\tau}\rangle^{l_{00}''}/(U \mid U').$$

Hence, $\Gamma' \parallel L \rhd_m P'$ is $l$-securely derivable.

Case 2. We consider the case (R-NewLev). In this case, $P = \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)P_0$, $P' = P_0$ and $L' = \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L$, where $\tilde{l_1}$, $\tilde{l_2} \subseteq L$ and $\left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L$ is defined.

By Lemma D.1 (7), there exist a type environments $\Gamma'$ and $m' \in L$ such that $m \leq_L m'$, and $\Gamma <: \Gamma'$, $m' \leq_L l''$ for any $l'' \in \tilde{l_1}, \tilde{l_2}$, and $\Gamma' \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L \rhd_{m'} P_0$ is $l$-securely derivable.

Let $\pi$ be an $l$-secure derivation tree of $\Gamma' \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L \rhd_{m'} P_0$. We have an $l$-secure derivation tree as follows:

$$\dfrac{\begin{array}{c}\vdots\\ \pi\\ \vdots\end{array}}{\Gamma' \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right) L \rhd_{m'} P_0}\,(\text{T-Weak})$$

Hence, we have the statement.

Case 3. We consider the case (R-Par). In this case, $P = P_0 \mid P_1$ and $P' = P_0' \mid P_1$ with $(P_0, L) \longrightarrow (P_0', L')$. By Lemma D.1 (2), there exist two type environments $\Gamma_0'$, $\Gamma_1'$ and $m' \in L$ such that $\Gamma <: \Gamma_0' \mid \Gamma_1'$ and $m \leq_L m'$ hold, and that $\Gamma_i' \parallel L \rhd_{m'} P_i$ is $l$-securely derivable for each $i = 0, 1$. Since $m \leq_L m'$ and $\Gamma_i' \parallel L \rhd_{m'} P_i$ is $l$-securely derivable, we see that $\Gamma_i' \parallel L \rhd_m P_i$ is $l$-securely derivable for each $i = 0, 1$. By the induction hypothesis, then there exists a type environment $\Gamma_0'$ such that either $\Gamma_0' = \Gamma_0'$ or $\Gamma_0' \longrightarrow \Gamma_0'$ and $\Gamma_0' \parallel L' \rhd_m P_0'$ is $l$-securely derivable. By Theorem A.6, either $L' = L$ or $L' = \left(\tilde{l_0} < \nu l < \tilde{l_1}\right) L$. By Proposition 3.16, $\Gamma_1' \parallel L' \rhd_m P_1'$ is $l$-securely derivable.

Let $\pi_i$ be a derivation tree of $\Gamma_i' \parallel L \rhd_m P_i$ for each $i = 0, 1$. Then, we have a derivation tree as follows:

$$\dfrac{\begin{array}{c}\vdots\\ \pi_0\\ \vdots\end{array}\qquad\qquad \begin{array}{c}\vdots\\ \pi_1\\ \vdots\end{array}}{\Gamma_0' \parallel L \rhd_m P_0 \qquad \Gamma_1' \parallel L \rhd_m P_1}\,(\text{T-Weak})$$
$$\Gamma_0' \mid \Gamma_1' \parallel L \rhd_m P_0 \mid P_1$$

Let $\hat{\pi}_0$ be an $l$-secure derivation tree of $\Gamma_0' \parallel L' \rhd_m P_0'$ and $\hat{\pi}_1$ be an $\check{l}$-secure derivation tree of $\Gamma_1' \parallel L' \rhd_m P_1'$.

$$\dfrac{\begin{array}{c}\vdots\\ \hat{\pi}_0\\ \vdots\end{array}\qquad\qquad \begin{array}{c}\vdots\\ \hat{\pi}_1\\ \vdots\end{array}}{\Gamma_0' \parallel L' \rhd_m P_0 \qquad \Gamma_1' \parallel L' \rhd_m P_1}\,(\text{T-Weak})$$
$$\Gamma_0' \mid \Gamma_1' \parallel L' \rhd_m P_0 \mid P_1$$

If $\Gamma_0' = \Gamma_0'$, then we have $\Gamma_0' \mid \Gamma_1' = \Gamma_0' \mid \Gamma_1'$. Since $\Gamma <: \Gamma_0' \mid \Gamma_1'$, we see that $\Gamma \parallel L' \rhd_m P_0 \mid P_1$ is $l$-securely derivable.

Assume $\Gamma_0' \longrightarrow \Gamma_0'$. By Lemma D.7, we have $\Gamma_0' \mid \Gamma_1' \longrightarrow \Gamma_0' \mid \Gamma_1'$. By Lemma D.6, there exists $\Gamma'$ such that $\Gamma \longrightarrow \Gamma'$ and $\Gamma' <: \Gamma_0' \mid \Gamma_1'$. Since $\Gamma' <: \Gamma_0' \mid \Gamma_1'$, we see that $\Gamma' \parallel L' \rhd_m P_0 \mid P_1$ is $l$-securely derivable.

Case 4. We consider the case (R-New). In this case, $P = ((\nu x : \xi) P_0, L)$ and $P' = ((\nu x : \xi) P_0', L')$, where $(P_0, L) \longrightarrow (P_0', L')$. By Lemma D.1 (6), there exist a type environments $\Gamma'$, a usage $U$, and $m' \in L'$ such that $m \leq_L m'$, $\mathrm{rel}(U)$ and $\Gamma <: \Gamma'$, and $\Gamma', x : \xi/U \parallel L \rhd_{m'} P_0$ is $l$-securely derivable. By the induction hypothesis, there exist a type environment $\Gamma''$ such that $\Gamma'' \parallel L' \rhd_{m'} P_0'$ is $l$-securely derivable, where either $\Gamma'' = \Gamma', x : \xi/U$ or $\Gamma', x : \xi/U \longrightarrow \Gamma''$.

Let $\pi$ be an $l$-secure derivation tree of $\Gamma'' \parallel L' \rhd_{m'} P_0'$.

If $\Gamma'' = \Gamma', x : \xi/U$, then we have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \pi\\ \vdots\end{array}}{\Gamma', x : \xi/U \parallel L' \rhd_{m'} P_0'}\,(\text{T-New})}{\Gamma' \parallel L' \rhd_{m'} (\nu x : \xi) P_0'}\,(\text{T-Weak})$$
$$\Gamma \parallel L' \rhd_m (\nu x : \xi) P_0'$$

Assume $\Gamma', x : \xi/U \longrightarrow \Gamma''$.

Assume $\Gamma'(y) \longrightarrow \Gamma''(y)$ with $y \in \mathrm{Dom}(\Gamma')$. Then, there exists a type environment $\Gamma''_0$ such that $\Gamma'' = \Gamma''_0, x : \xi/U$ and $\Gamma' \longrightarrow \Gamma''_0$. Since $\Gamma'' = \Gamma''_0, x : \xi/U$, we have an $l$-secure derivation tree as follows:

$$\dfrac{\begin{array}{c}\vdots\\ \pi\\ \vdots\end{array}}{\Gamma''_0, x : \xi/U \parallel L' \rhd_{m'} P_0'}\,(\text{T-New})$$
$$\Gamma''_0 \parallel L' \rhd_m (\nu x : \xi) P_0'$$

Since $\Gamma' \longrightarrow {\Gamma''}_0$, Lemma D.6 implies that there exists $\Gamma'_0$ such that $\Gamma \longrightarrow \Gamma'$ and $\Gamma' <: {\Gamma''}_0$. Hence, $\Gamma' \parallel L' \rhd_m (\nu x : \xi) P'_0$ is $l$-securely derivable.

Assume $\xi/U \longrightarrow \xi/U'$ with some usage $U'$. Then $\Gamma'' = \Gamma', x : \xi/U'$. Hence, we have an $l$-secure derivation tree as follows:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \pi \\ \vdots\end{array}}{\dfrac{\Gamma', x : \xi/U' \parallel L' \rhd_{m'} P'_0}{\Gamma' \parallel L' \rhd_{m'} (\nu x : \xi) P'_0}\,(\text{T-New})}}{\Gamma \parallel L' \rhd_m (\nu x : \xi) P'_0}\,(\text{T-Weak})}\ .$$

Therefore, we have the statement.

Case 5. We consider the case (R-SP). In this case, $P = P_0$ and $P' = P_1$, where $(P_0, L) \preceq (P'_0, L)$, $(P'_0, L) \longrightarrow (P'_1, L')$, and $(P'_1, L') \preceq (P_1, L')$. By Lemma 4.2, $\Gamma \parallel L \rhd_m P'_0$ is $l$-securely derivable. By the induction hypothesis, there exist a type environment $\Gamma'$ such that either $\Gamma' = \Gamma$ or $\Gamma \longrightarrow \Gamma'$ and $\Gamma' \parallel L' \rhd_m P'_1$ is $l$-securely derivable. By Lemma 4.2, $\Gamma' \parallel L' \rhd_m P'$ is $l$-securely derivable. Thus, we have the statement. □

# Appendix E. Lemmata for lock-freedom and the details of its proof

## E.1. Properties of $\longrightarrow_l^\Gamma$

**Lemma E.1.** *For type environments $\Gamma$ and $\Gamma'$, a lattice of secrecy levels $L$, a secrecy level $l \in L$ and a process $P$, if $\Gamma(x) \sim \Gamma'(x)$ for any value $x$ belonging to the domain of $\Gamma$, the domain of $\Gamma$ is a subset of the domain of $\Gamma'$, and $(P, L) \longrightarrow_l^\Gamma (P', L')$, then $(P, L) \longrightarrow_l^{\Gamma'} (P', L')$.*

*Proof.* Straightforward. □

**Lemma E.2.** *For type environments $\Gamma$ and $\Gamma'$, a lattice of secrecy levels $L$, a secrecy level $l \in L$ and a process $P$, if $\Gamma(x) \sim \Gamma'(x)$ for any value $x$ occurring in $P$, and $(P, L) \longrightarrow_l^\Gamma (P', L')$, then $(P, L) \longrightarrow_l^{\Gamma'} (P', L')$.*

*Proof.* Straightforward. □

## E.2. Proof of Lemma 4.8

We show Lemma 4.8.

Assume that $\Gamma \parallel L \rhd_l P$ and $\Delta \parallel L \rhd_l Q$ are $k$-securely derivable, $\Gamma \mid \Delta$ are reliable, $\Gamma \mid \Delta \parallel L$ is $k$-secure, and $\mathrm{ob}_\alpha(\Gamma(x))$ is finite, where either $\alpha = I$ or $\alpha = O$.

Let $n$ be $\mathrm{ob}_\alpha(\Gamma(x))$, and $l_P$ be the length of $P$. By induction on $(n, l_P)$, we prove that there exists $R$ such that $(P \mid Q, L) \longrightarrow\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R, \hat{L}\right)$ and $x \in \mathrm{SBarbs}_\alpha(R)$. Let $\Gamma(x) = \xi/U_x$ and $\Delta(x) = \xi/U'_x$.

Assume $\mathrm{con}_{\overline{\alpha}}(U_x)$ does not hold. Then $\mathrm{ob}_\alpha(U_x) > \mathrm{cap}_{\overline{\alpha}}(U_x)$. Because $\Gamma \mid \Delta$ is reliable, we have $\mathrm{ob}_\alpha(U_x \mid U'_x) \leq \mathrm{cap}_{\overline{\alpha}}(U_x \mid U'_x)$. Hence, $\min\left(\mathrm{ob}_\alpha^\emptyset(U_x), \mathrm{ob}_\alpha^\emptyset(U'_x)\right) \leq \min(\mathrm{cap}_{\overline{\alpha}}(U_x), \mathrm{cap}_{\overline{\alpha}}(U'_x))$. Then $\mathrm{ob}_\alpha(U_x) > \mathrm{cap}_{\overline{\alpha}}(U_x) \geq \min(\mathrm{cap}_{\overline{\alpha}}(U_x), \mathrm{cap}_{\overline{\alpha}}(U'_x)) \geq \min\left(\mathrm{ob}_\alpha^\emptyset(U_x), \mathrm{ob}_\alpha^\emptyset(U'_x)\right)$. Hence, $n > \mathrm{ob}_\alpha(U'_x)$. By the induction hypothesis, there exists $R$ such that $(Q \mid P, L) \longrightarrow\!\!\!\!\rightarrow_k^{\Delta|\Gamma} \left(R, \hat{L}\right)$ and $x \in \mathrm{SBarbs}_\alpha(R)$. Since $P \mid Q \preceq Q \mid P$, we have $(P \mid Q, L) \longrightarrow\!\!\!\!\rightarrow_k^{\Delta|\Gamma} (R, k)$. By Lemma E.1, $(P \mid Q, L) \longrightarrow\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R, \hat{L}\right)$.

Assume $\mathrm{con}_{\overline{\alpha}}(U_x)$. We consider cases according to the form of $P$.

Case 1. Since $\mathrm{ob}_\alpha(\Gamma(x))$ is finite, we have $P \neq \mathsf{0}$.

Case 2. $P = (P_0 \mid P_1)$. By Lemma D.1 (2), there exist two type environments $\Gamma'_0$, $\Gamma'_1$, and $l' \in L'$ such that $\Gamma <: \Gamma'_0 \mid \Gamma'_1$ and $l \leq_L l'$, and $\Gamma'_i \parallel L \rhd_{l'} P_i$ is $k$-securely derivable for each $i = 0, 1$. By Proposition C.2 (4), $\Gamma \mid \Delta <: \Gamma'_0 \mid \Gamma'_1 \mid \Delta$. By Proposition C.3, $\Gamma'_0 \mid \Gamma'_1 \mid \Delta$ is reliable. Because $\Gamma <: \Gamma'_0 \mid \Gamma'_1$ and $\mathrm{ob}_\alpha(\Gamma(x))$ is finite, we have $x \in \mathrm{Dom}(\Gamma'_0 \mid \Gamma'_1)$. By Definition 3.7 (d), we have $n \geq \mathrm{ob}_\alpha(\Gamma'_0 \mid \Gamma'_1(x))$. Hence, either $n \geq \mathrm{ob}_\alpha(\Gamma'_0(x))$ or $n \geq \mathrm{ob}_\alpha(\Gamma'_1(x))$.

Assume $n \geq \mathrm{ob}_\alpha(\Gamma'_0(x))$. The length of $P_0$ is less then $l_P$. By the induction hypothesis, we see that there exist $R_0$ and $\hat{L}_0$ such that $(P_0 \mid Q, L) \longrightarrow\!\!\!\!\rightarrow_k^{\Gamma'_0|\Delta} \left(R_0, \hat{L}_0\right)$ and $x \in \mathrm{SBarbs}_\alpha(R_0)$. By Lemma E.1, $(P_0 \mid Q, L) \longrightarrow\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R_0, \hat{L}_0\right)$.

Then $(P_0 \mid Q \mid P_1, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R_0 \mid P_1, \hat{L}_0\right)$. Since $P_0 \mid P_1 \mid Q \preceq P_0 \mid Q \mid P_1$, we have $(P \mid Q, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R_0 \mid P_1, \hat{L}_0\right)$. By $x \in \mathrm{SBarbs}_\alpha(R_0)$, we see $x \in \mathrm{SBarbs}_\alpha(R_0 \mid P_1)$.

In the similar way to the case $n \geq \mathrm{ob}_\alpha(\Gamma_0'(x))$, under the assumption that $n \geq \mathrm{ob}_\alpha(\Gamma_1'(x))$, we can show that there exists $R$ such that $(P \mid Q, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R, \hat{L}\right)$ and $x \in \mathrm{SBarbs}_\alpha(R)$.

Case 3. $P = y!\tilde{v}.P_0$.

Assume $y = x$. Let $R = P \mid Q$ and $\hat{L} = L$. Then $(P \mid Q, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R, \hat{L}\right)$ and $x \in \mathrm{SBarbs}_\alpha(R)$.

Assume $y \neq x$. By Lemma D.1 (3), there exist a type environments $\Gamma'$, secrecy levels $l_0, l_1 \in L$, types $\tilde{\tau}$, a usage $U$ and $t_c \in \mathbb{N} \cup \{\infty\}$ such that $\Gamma <: \Gamma''$, $l \leq_L l_0$, and $l \leq_L l_1$, $\Gamma', y : \langle\tilde{\tau}\rangle^{l_0}/U_y \parallel L \rhd_k l_1 P_0$ is $k$-securely derivable, $\Gamma'' \parallel L$ is $k$-secure, and $t_c = \infty$ implies $l_0 \leq_L l_1$, where $\Gamma'' = \uparrow^{(t_c+1,t_c+1)} \Gamma' \mid \tilde{v} : \uparrow\tilde{\tau} \mid y : \langle\tilde{\tau}\rangle^{l_0}/O^0_{t_c}U_y$. Since $\Gamma <: \Gamma''$, we have $t_c < t_c + 1 \leq \mathrm{ob}_\alpha(\Gamma''(x)) \leq n$. Since $\Gamma'' \parallel L$ is $k$-secure, we have $l_0 \not\leq_L k$. By Proposition C.2 (4), $\Gamma \mid \Delta <: \Gamma'' \mid \Delta$. By Proposition C.3, $\Gamma'' \mid \Delta$ is reliable. Then, we see that $\langle\tilde{\tau}\rangle^{l_0}/O^0_{t_c}U_y \mid \Delta(y)$ is reliable. Let $\Delta(y) = \langle\tilde{\tau}\rangle^{l_0}/U'_y$. Then, we have $\mathrm{ob}_I\left(O^0_{t_c}U_y \mid U'_y\right) \leq \mathrm{cap}_O\left(O^0_{t_c}U_y \mid U'_y\right)$. Then $\mathrm{ob}_I\left(U'_y\right) \leq \mathrm{cap}_O\left(O^0_{t_c}U_y \mid U'_y\right) \leq t_c < n$. By the induction hypothesis, there exist $R_0$ and $\hat{L}_0$ such that $(Q \mid \mathtt{0}, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Delta|\emptyset} \left(R_0, \hat{L}_0\right)$ and $y \in \mathrm{SBarbs}_I(R_0)$. Hence, $(Q, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Delta|\emptyset} \left((\nu\tilde{w})y?\tilde{z}.Q_0 \mid Q_1, \hat{L}_0\right)$ and $y \notin \tilde{w}$ for some $Q_0$ and $Q_1$. By Proposition 4.5, there exists a type environment $\hat{\Delta}$ such that $\Delta \longrightarrow\!\!\!\!\!\rightarrow \hat{\Delta}$ and $\hat{\Delta} \parallel \hat{L}_0 \rhd_l (\nu\tilde{w})y?\tilde{z}.Q_0 \mid Q_1$ is $k$-securely derivable. By Lemma D.1 there exist type environments $\Delta_0$ and $\Delta_1$ and $l_0, l_1 \in \hat{L}_0$ such that $\Delta_0, y : \langle\tilde{\tau}\rangle^{l_0}/V, \tilde{z} : \tilde{\tau} \parallel \hat{L}_0 \rhd_k l_1 Q_0$ and $\Delta_1 \parallel \hat{L}_0 \rhd_{l'} Q_1$ are $k$-securely derivable, and $\hat{\Delta}, \tilde{w} : \tilde{\tau}' <: \left(\uparrow^{(t'_c+1,t'_c+1)} \Delta_0, y : \langle\tilde{\tau}\rangle^{l_0}/I^0_{t'_c}V\right) \mid \Delta_1$, $l \leq_L l_0$, $l \leq_L l_1$ and $l \leq_L l'$. By Lemma 4.4, $\left(\Delta_0, y : \langle\tilde{\tau}\rangle^{l_0}/V, \tilde{z} : \tilde{\tau}\right)[\tilde{z} \mapsto \tilde{v}] \parallel \hat{L}_0 \rhd_{l_1} Q_0[\tilde{z} \mapsto \tilde{v}]$ is $k$-securely derivable. By Theorem A.6 and Proposition 3.16, $\Gamma', y : \langle\tilde{\tau}\rangle^{l_0}/U_y \parallel \hat{L}_0 \rhd_{l_1} P_0$ is $k$-securely derivable. Then, we see that

$$\left(\Gamma', y : \langle\tilde{\tau}\rangle^{l_0}/U_y \mid \left(\Delta_0, y : \langle\tilde{\tau}\rangle^{l_0}/V, \tilde{z} : \tilde{\tau}\right) \mid \Delta_1\right)[\tilde{z} \mapsto \tilde{v}] \parallel \hat{L}_0 \rhd_{l_1} (P_0 \mid Q_0 \mid Q_1)[\tilde{z} \mapsto \tilde{v}]$$

is $k$-securely derivable. By Proposition C.3, $\Gamma', y : \langle\tilde{\tau}\rangle^{l_0}/U_y \mid \left(\Delta_0, y : \langle\tilde{\tau}\rangle^{l_0}/V, \tilde{z} : \tilde{\tau}\right)[\tilde{z} \mapsto \tilde{v}] \mid \Delta_1$ is reliable.

Because $\Gamma <: \Gamma''$ and $\mathrm{con}_{\overline{\alpha}}(U_x)$, we have

$$\mathrm{ob}_\alpha\left(\Gamma', y : \langle\tilde{\tau}\rangle^{l_0}/U_y(x)\right) \leq \mathrm{ob}_\alpha\left(\left(\uparrow^{(t_c+1,t_c+1)} \Gamma' \mid \tilde{v} : \uparrow\tilde{\tau} \mid y : \langle\tilde{\tau}\rangle^{l_0}/O^0_{t_c}U_y\right)(x)\right) \leq \mathrm{ob}_\alpha(\Gamma(x)) = n.$$

Since the length of $P_0$ is less then $l_P$, we see that there exist $R$ and $k$ such that

$$(P_0 \mid Q_0[\tilde{z} \mapsto \tilde{v}] \mid Q_1, L) \longrightarrow\!\!\!\!\!\rightarrow_{(R,\hat{L})}^{\Gamma', y:\langle\tilde{\tau}\rangle^{l_0}/U_y \mid \left(\Delta_0, y:\langle\tilde{\tau}\rangle^{l_0}/V, \tilde{z}:\tilde{\tau}\right)[\tilde{z}\mapsto\tilde{v}] \mid \Delta_1}$$

and $x \in \mathrm{SBarbs}_\alpha(R)$. Then, we have the claimed result.

Case 4. $P = y?\tilde{z}.P_0$. Straightforward.

Case 5. $P = *P_0$. Straightforward.

Case 6. $P = (\nu y : \xi)P_0$. Straightforward.

Case 7. $P = \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)P_0$. By Lemma D.1 (7), $l'' \not\leq_L k$ for some $l'' \in \tilde{l_1}, \tilde{l_2}$ and there exist a type environments $\Gamma'$, and $l' \in L$ such that $l \leq_L l'$ and $\Gamma <: \Gamma'$, $l' \leq_L l''$ for any $l'' \in \tilde{l_1}, \tilde{l_2}$, and $\Gamma' \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L \rhd_{l'} P_0$ is $k$-securely derivable. By Proposition 3.16, $\Delta \parallel \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L \rhd_l Q$ is $k$-securely derivable. Because $\Gamma <: \Gamma'$ and $\mathrm{con}_{\overline{\alpha}}(U_x)$, we have $\mathrm{ob}_\alpha(\Gamma'(x)) \leq \mathrm{ob}_\alpha(\Gamma(x))$. Since the length of $P_0$ is less then $l_P$, we see that there exist $R$ and $k$ such that $\left(P_0 \mid Q, \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L\right) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma'|\Delta} \left(R, \hat{L}\right)$ and $x \in \mathrm{SBarbs}_\alpha(R)$. By Lemma E.1, $\left(P_0 \mid Q, \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L\right) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R, \hat{L}\right)$. Hence,

$$(P \mid Q, L) \longrightarrow_k^{\Gamma|\Delta} \left(P_0 \mid Q, \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L\right) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma|\Delta} \left(R, \hat{L}\right).$$

Case 8. $P = \mathtt{if}\ v\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1$. Straightforward. □

# Appendix F. Proof of non-interference theorems

## F.1. Basic properties for bisimulation

**Lemma F.1.** *For processes $P$, $P'$ and a lattice of secrecy levels $L$, if $P \simeq P'$, then* $\mathrm{Barbs}(P, L) = \mathrm{Barbs}(P', L)$.

*Proof.* Assume $P \preceq P'$. We show $\mathrm{Barbs}(P, L) = \mathrm{Barbs}(P', L)$.

We show $\mathrm{Barbs}(P, L) \subseteq \mathrm{Barbs}(P', L)$. Assume $x \in \mathrm{Barbs}(P, L)$. We show $x \in \mathrm{Barbs}(P', L)$.

Assume $(P, L) \longrightarrow\!\!\!\!\!\rightarrow (P'', L')$, $P'' = (\nu\tilde{y})x!\tilde{v}.P_0 \mid P_1$ and $x \notin \tilde{y}$. Since $P' \preceq P$, we have $(P', L) \longrightarrow\!\!\!\!\!\rightarrow (P'', L')$. Hence, $x \in \mathrm{Barbs}(P', L)$.

In the similar way to the case $P'' = (\nu\tilde{y})x!\tilde{v}.P_0 \mid P_1$, we have $x \in \mathrm{Barbs}(P', L)$ if $(P, L) \longrightarrow\!\!\!\!\!\rightarrow (P'', L')$, $P'' \preceq (\nu\tilde{y})x?\tilde{z}.P_0 \mid P_1$ and $x \notin \tilde{y}$.

In the same way to the case $\mathrm{Barbs}(P, L) \subseteq \mathrm{Barbs}(P', L)$, we have $\mathrm{Barbs}(P', L) \subseteq \mathrm{Barbs}(P, L)$. □

**Lemma F.2.** *$\overset{\bullet}{\approx}$ is transitive i.e. if $(P_0, L_0) \overset{\bullet}{\approx} (P_1, L_1)$ and $(P_1, L_1) \overset{\bullet}{\approx} (P_2, L_2)$, then $(P_0, L_0) \overset{\bullet}{\approx} (P_2, L_2)$.*

*Proof.* Easy. □

**Lemma F.3.** *For processes $P$, $P'$, $Q$, $Q'$ and a lattice of secrecy level $L$, if $(P, L) \overset{\bullet}{\approx} (Q, L)$, $P' \simeq P$, and $Q \simeq Q'$, then $(P', L) \overset{\bullet}{\approx} (Q', L)$.*

*Proof.* Assume $(P, L) \overset{\bullet}{\approx} (Q, L)$, $P' \simeq P$, and $Q \simeq Q'$. Since $(P, L) \overset{\bullet}{\approx} (Q, L)$, there exists a barbed bisimulation $\mathcal{R}$ such that $((P, L), (Q, L)) \in \mathcal{R}$. Let

$$\mathcal{R}' = \{((P', L), (Q', L')) \mid ((P, L), (Q, L')) \in \mathcal{R}, P' \simeq P, \text{ and } Q \simeq Q', \}.$$

We show that $\mathcal{R}'$ is a barbed bisimulation. Let $((P'_0, L_0), (P'_1, L_1)) \in \mathcal{R}'$. Then, there exist processes $P_0$ and $P_1$ such that $((P_0, L_0), (P_1, L_1)) \in \mathcal{R}$, $P'_0 \simeq P_0$, and $P_1 \simeq P'_1$. We note $\mathcal{R} \subseteq \mathcal{R}'$.

(1) Assume $(P'_0, L_0) \longrightarrow (P''_0, L'_0)$. We show that there exists $(P''_1, L'_1)$ such that $(P'_1, L_1) \longrightarrow\!\!\!\!\!\rightarrow (P''_1, L'_1)$ and $((P''_0, L'_0), (P''_1, L'_1)) \in \mathcal{R}'$. Since $P'_0 \simeq P_0$, we have $(P_0, L_0) \longrightarrow (P''_0, L'_0)$. Since $((P_0, L_0), (P_1, L_1)) \in \mathcal{R}$, there exists $(P''_1, L'_1)$ such that $(P_1, L_1) \longrightarrow\!\!\!\!\!\rightarrow (P''_1, L'_1)$ and $((P''_0, L'_0), (P''_1, L'_1)) \in \mathcal{R}$. By $P_1 \simeq P'_1$, we have $(P'_1, L_1) \longrightarrow\!\!\!\!\!\rightarrow (P''_1, L'_1)$. By $\mathcal{R} \subseteq \mathcal{R}'$, we see $((P''_0, L'_0), (P''_1, L'_1)) \in \mathcal{R}'$.

(2) In the same way to (1).

(3) By Lemma F.1, we have $\mathrm{Barbs}(P'_0, L) = \mathrm{Barbs}(P_0, L)$ and $\mathrm{Barbs}(P_1, L) = \mathrm{Barbs}(P'_1, L)$. Since $((P_0, L_0), (P_1, L_1)) \in \mathcal{R}$, we have $\mathrm{Barbs}(P_0, L) = \mathrm{Barbs}(P_1, L)$. Hence, we have $\mathrm{Barbs}(P'_0, L) = \mathrm{Barbs}(P'_1, L)$.

Now, we see that $\mathcal{R}'$ is a barbed bisimulation. By definition of $\mathcal{R}'$, we have $((P', L), (Q', L)) \in \mathcal{R}'$. Thus, $(P', L) \overset{\bullet}{\approx} (Q', L)$. □

**Lemma F.4.** *(1) If $P_0 \preceq P_1$, then $\mathrm{FN}(C[P_0]) \supseteq \mathrm{FN}(C[P_1])$ for any context $C$.*
*(2) If $P_0 \simeq P_1$, then $\mathrm{FN}(C[P_0]) = \mathrm{FN}(C[P_1])$ for any context $C$.*

*Proof.* It suffices to show (1). We see (1) by induction on the construction of $C$. □

**Lemma F.5.** *For processes $P_0$ and $P_1$, if $P_0 \simeq P_1$ and $C[P_0] \preceq P'_0$, then there exists a context $C'$ such that $P'_0 = C'[P_0]$ and $C[P_1] \preceq C'[P_1]$.*

*Proof.* Assume $P_0 \simeq P_1$ and $C[P_0] \preceq P'_0$. We show that there exists a context $C'$ such that $P'_0 = C'[P_0]$ and $C[P_1] \preceq C'[P_1]$. We proceed by induction on the construction of $C[P_0] \preceq P'_0$. We consider cases according to the form of $C$.

If $[\,]$ does not occur in $C$, then the required condition holds obviously.

Assume $C = [\,]$. Let $C' = [\,]$. Then, the required condition holds.

Assume $C \neq [\,]$. We consider cases according to the last rule of the construction of $C[P_0] \preceq P'_0$.

Case 1. Assume $P'_0 = C[P_0]$. Let $C' = C$. Then, the required condition holds.

Case 2. Assume that there exists a process $Q$ such that $C[P_0] \preceq Q$ and $Q \preceq P'_0$. By the induction hypothesis, we see that there exists a context $C''$ such that $Q = C''[P_0]$ and $C[P_1] \preceq C''[P_1]$. Then, we have $C''[P_0] \preceq P'_0$. By the induction hypothesis, we see that there exists a context $C'$ such that $C''[P_0] = C'[P_0]$ and $C''[P_1] \preceq C'[P_1]$. Since $C[P_1] \preceq C''[P_1]$ and $C''[P_1] \preceq C'[P_1]$, we have $C[P_1] \preceq C'[P_1]$.

Case 3. (SP-Zero1). Assume $P'_0 = C[P_0] \mid \mathsf{0}$. Let $C' = C \mid \mathsf{0}$. Then $C[P_1] \preceq C'[P_1]$.

Assume $C = C_0 \mid [\,]$ and $P_0 = \mathsf{0}$ for some context $C_0$. Then $P'_0 = C_0[P_0]$. Let $C' = C_0$. Then, we have $P'_0 = C'[P_0]$. By Proposition A.3, we have $C[P_1] = C_0[P_1] \mid P_1 \preceq C_0[P_1] \mid \mathsf{0}$. Hence, $C[P_1] \preceq C'[P_1]$.

Assume $C = C_0 \mid \mathsf{0}$ for some context $C_0$. Then $P'_0 = C_0[P_0]$. Let $C' = C_0$. Then, we have $P'_0 = C'[P_0]$. By (SP-Zero1), $C[P_1] = C'[P_1] \mid \mathsf{0} \preceq C'[P_1]$.

Case 4. (SP-Zero2). Assume $C = (\nu x : \xi)[\,]$ and $P_0 = \mathsf{0}$. Then $P'_0 = \mathsf{0}$. Let $C' = \mathsf{0}$. Then, we have $P'_0 = C'[P_0]$. By (SP-CNew), $C[P_1] = (\nu x : \xi)P_1 \preceq (\nu x : \xi)\mathsf{0}$. Then $C[P_1] \preceq \mathsf{0} = C'[P_1]$.

Case 5. (SP-Commut). Assume $C = C_0 \mid C_1$ for some contexts $C_0$ and $C_1$. Then $P'_0 = C_1[P_0] \mid C_0[P_0]$. Let $C' = C_1 \mid C_0$. Then, we have $P'_0 = C'[P_0]$. By (SP-Commut), $C[P_1] = C_0[P_1] \mid C_1[P_1] \preceq C_1[P_1] \mid C_0[P_1]$.

Case 6. (SP-Assoc). Assume $C = [\,] \mid C_2$ and $P_0 = Q_0 \mid Q_1$ for some context $C_2$ and processes $Q_0$ and $Q_1$. Then $P_0' = Q_0 \mid (Q_1 \mid C_2[P_0])$. Let $C' = Q_0 \mid (Q_1 \mid C_2)$. Then, we have $P_0' = C'[P_0]$. By (SP-Par), we have $C[P_1] = P_1 \mid C_2[P_1] \preceq P_0 \mid C_2[P_1] = (Q_0 \mid Q_1) \mid C_2[P_1]$. By (SP-Assoc), $C[P_1] \preceq Q_0 \mid (Q_1 \mid C_2[P_1]) = C'[P_1]$.

Assume $C = (C_0 \mid C_1) \mid C_2$ for some contexts $C_0$, $C_1$, and $C_2$. Then $P_0' = C_0[P_0] \mid (C_1[P_0] \mid C_2[P_0])$. Let $C' = C_0 \mid (C_1 \mid C_2)$. Then, we have $P_0' = C'[P_0]$. By (SP-Assoc), $C[P_1] \preceq C_0[P_1] \mid (C_1[P_1] \mid C_2[P_1]) = C'[P_1]$.

Case 7. (SP-New). Assume $C = [\,] \mid C_1$, $P_0 = (\nu x : \xi)Q$, and $x \notin \mathrm{FN}(C_1[P_0])$ for some context $C_1$. Then $P_0' = (\nu x : \xi)Q \mid C_1[P_0]$. Let $C' = (\nu x : \xi)Q \mid C_1$. By (SP-Par), we have $C[P_1] = P_1 \mid C_1[P_1] \preceq P_0 \mid C_1[P_1] = (\nu x : \xi)Q \mid C_1[P_1]$. By Lemma F.4 (2) and (SP-New), $C[P_1] \preceq (\nu x : \xi)Q \mid C_1[P_1] = C'[P_1]$.

Assume $C = (\nu x : \xi)C_0 \mid C_1$ and $x \notin \mathrm{FN}(C_1[P_0])$ for some contexts $C_0$ and $C_1$. Then $P_0' = (\nu x : \xi)C_0[P_0] \mid C_1[P_0]$. Let $C' = (\nu x : \xi)C_0 \mid C_1$. By Lemma F.4 (2) and (SP-New), $C[P_1] \preceq (\nu x : \xi)C_0[P_1] \mid C_1[P_1] = C'[P_1]$.

Case 8. (SP-IfT). Assume $C = \mathtt{if}\ [\,]\ \mathtt{then}\ C_0\ \mathtt{else}\ C_1$ and $P_0 = \mathrm{true}^l$ for some contexts $C_0$ and $C_1$. Then $P_0' = C_0[P_0]$. Let $C' = C_0$. Since $P_0 \simeq P_1$, we have $P_1 = \mathrm{true}^l$. By (SP-IfT), $C[P_1] = \mathtt{if}\ \mathrm{true}^l\ \mathtt{then}\ C_0[P_1]\ \mathtt{else}\ C_1[P_1] \preceq C_0[P_1] = C'[P_1]$.

Assume $C = \mathtt{if}\ \mathrm{true}^l\ \mathtt{then}\ C_0\ \mathtt{else}\ C_1$ for some contexts $C_0$ and $C_1$. Then $P_0' = C_0[P_0]$. Let $C' = C_0$. By (SP-IfT), $C[P_1] = \mathtt{if}\ \mathrm{true}^l\ \mathtt{then}\ C_0[P_1]\ \mathtt{else}\ C_1[P_1] \preceq C_0[P_1] = C'[P_1]$.

Case 9. (SP-IfF). In the similar way to (SP-IfT).

Case 10. (SP-Rep). Assume $C = *C_0$ for some context $C_0$. Then $P_0' = *C_0[P_0] \mid C_0[P_0]$. Let $C' = *C_0 \mid C_0$. Then, we have $P_0' = C'[P_0]$. By (SP-Rep), $C[P_1] = *C_0[P_1] \preceq *C_0[P_1] \mid C_0[P_1] = C'[P_1]$.

Case 11. (SP-Par). Assume $C = C_0 \mid C_1$ and $C_0[P_0] \preceq Q_0$ for some contexts $C_0$ and $C_1$, and a process $Q_0$. Then $P_0' = Q_0 \mid C_1[P_0]$. By the induction hypothesis, we see that there exists a context $C_0'$ such that $Q_0 = C_0'[P_0]$ and $C_0[P_1] \preceq C_0'[P_1]$. Let $C' = C_0' \mid C_1$. Then, we have $P_0' = C'[P_0]$. By (SP-Par), $C[P_1] = C_0[P_1] \mid C_1[P_1] \preceq C_0'[P_1] \mid C_1[P_1] = C'[P_1]$.

Case 12. (SP-CNew). Assume $C = (\nu x : \xi)C_0$ and $C_0[P_0] \preceq Q_0$ for some context $C_0$ and a process $Q_0$. Then $P_0' = (\nu x : \xi)Q_0$. By the induction hypothesis, we see that there exists a context $C_0'$ such that $Q_0 = C_0'[P_0]$ and $C_0[P_1] \preceq C_0'[P_1]$. Let $C' = (\nu x : \xi)C_0'$. Then, we have $P_0' = C'[P_0]$. By (SP-CNew), $C[P_1] = (\nu x : \xi)C_0[P_1] \preceq (\nu x : \xi)C_0'[P_1] = C'[P_1]$. □

**Lemma F.6.** *For processes $P_0$ and $P_1$, if $P_0 \simeq P_1$ and $(C[P_0], L) \longrightarrow (P_0', L')$, then there exists a context $C'$ such that $P_0' = C'[P_0]$ and $(C[P_1], L) \longrightarrow (C'[P_1], L')$.*

*Proof.* Assume $P_0 \simeq P_1$ and $(C[P_0], L) \longrightarrow (P_0', L')$.

Assume $C = [\,]$. In this case, $C[P_i] = P_i$ for $i = 0, 1$. Assume $(P_0, L) \longrightarrow (P_0', L')$. Since $P_1 \preceq P_0$, we have $(P_1, L) \longrightarrow (P_0', L')$. Let $C' = P_0'$. Then $P_0' = C'[P_0]$ and $C[P_1] \longrightarrow C'[P_1]$.

Assume $C \neq [\,]$. The proof proceeds by induction on the construction of $(C[P_0], L) \longrightarrow (P_0', L')$. We consider cases according to the last rule of the construction of $(C[P_0], L) \longrightarrow (P_0', L')$.

Case 1. (R-Com). Assume $C = C_0 \mid C_1$ with contexts $C_0$ and $C_1$ and $L' = L$.

Assume $C_0 = [\,]$, $C_1 = x?(y_0, \ldots, y_n).C_1'$, and $P_0 = x!(v_0, \ldots, v_n).P$. Then $P_0' = P \mid C_1'[P_0]$. By Definition 2.6, we see $P_1 = x!(v_0, \ldots, v_n).P$. Then, we have $C[P_1] = x!(v_0, \ldots, v_n).P \mid x?(y_0, \ldots, y_n).C_1'[P_1]$. Let $C' = P \mid C_1'$. Then $P_0' = C'[P_0]$. By (R-Com), $(C[P_1], L) \longrightarrow (C'[P_1], L)$.

In the similar way, we can show the case $C_0 = x!(v_0, \ldots, v_n).C_0'$, $C_1 = [\,]$, and $P_0 = x?(y_0, \ldots, y_n).P$.

Assume $C_0 = x!(v_0, \ldots, v_n).C_0'$ and $C_1 = x?(y_0, \ldots, y_n).C_1'$. Then $P_0' = C_0'[P_0] \mid C_1'[P_0]$. Let $C' = C_0' \mid C_1'$. Then $P_0' = C'[P_0]$. By (R-Com), $(C[P_1], L) \longrightarrow (C'[P_1], L)$.

Case 2. (R-NewLev). Assume $C = \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)C_0'$, $L' = \left(\tilde{l_0} < \nu l < \tilde{l_1}\right)L$, $\tilde{l_0}$ and $\tilde{l_1} \subseteq L$ with a context $C_0$. Then $P_0' = C_0'[P_0]$. Let $C' = C_0'$. Then $P_0' = C'[P_0]$. By (R-NewLev), $(C[P_1], L) \longrightarrow (C'[P_1], L')$.

Case 3. (R-Par). Assume $C = C_0 \mid C_1$ with contexts $C_0$ and $C_1$.

Assume $C_0 = [\,]$. Then, there exists a process $Q$ such that $P_0' = Q \mid C_1[P_0]$ and $(P_0, L) \longrightarrow (Q, L')$. Since $P_1 \preceq P_0$, we have $(P_1, L) \longrightarrow (Q, L')$. Let $C' = Q \mid C_1$. Then $P_0' = C'[P_0]$. By (R-Par), $(C[P_1], L) \longrightarrow (C'[P_1], L)$.

Assume $C_0 \neq [\,]$. Then, there exists a process $Q_0$ such that $P_0' = Q_0 \mid C_1[P_0]$ and $(C_0[P_0], L) \longrightarrow (Q_0, L')$. By the induction hypothesis, there exists a context $C_0'$ such that $Q_0 = C_0'[P_0]$ and $C_0[P_1] \longrightarrow C_0'[P_1]$. Let $C' = C_0' \mid C_1$. Then $P_0' = C'[P_0]$. Since $(C_0[P_1], L) \longrightarrow (C_0'[P_1], L')$ and (R-Par), we have $(C[P_1], L) \longrightarrow (C'[P_1], L')$.

Case 4. (R-New). Assume that $C = (\nu x : \xi)C_0$ with a context $C_0$, and there exists a process $Q_0$ such that $(C_0[P_0], L) \longrightarrow (Q_0, L')$ and $P_0' = (\nu x : \xi)Q_0$. By the induction hypothesis, there exists a context $C_0'$ such that $Q_0 = C_0'[P_0]$ and $C_0[P_1] \longrightarrow C_0'[P_1]$. Let $C' = (\nu x : \xi)C_0'$. Then $P_0' = C'[P_0]$. Since $(C_0[P_1], L) \longrightarrow (C_0'[P_1], L')$ and (R-New), we have $(C[P_1], L) \longrightarrow (C'[P_1], L')$.

Case 5. (R-SP). Assume that there exist processes $Q_0$ and $Q_0'$ such that $C[P_0] \preceq Q_0$, $(Q_0, L) \longrightarrow (Q_0', L')$, and $Q_0' \preceq P_0'$. By Lemma F.5, there exists a context $C''$ such that $Q_0 = C''[P_0]$ and $C[P_1] \preceq C''[P_1]$. By the induction hypothesis, there exists a context $C'''$ such that $Q_0' = C'''[P_0]$ and $(C''[P_1], L) \longrightarrow (C'''[P_1], L')$. By Lemma F.5, there

exists a context $C'$ such that $P_0' = C'[P_0]$ and $C'''[P_1] \preceq C'[P_1]$. Since $C[P_1] \preceq C''[P_1]$, $(C''[P_1], L) \longrightarrow (C'''[P_1], L')$, $C'''[P_1] \preceq C'[P_1]$ and (R-SP), we have $(C[P_1], L) \longrightarrow (C'[P_1], L')$. □

**Lemma F.7.** *For processes $P_0$ and $P_1$, and a lattices for secrecy levels $L$, if $P_0 \simeq P_1$, then $(C[P_0], L) \overset{\bullet}{\approx} (C[P_1], L)$ with any context $C$.*

*Proof.* Let

$$\mathcal{R} = \{((C[P_0], L), (C[P_1], L)) \mid P_0 \simeq P_1, C \text{ is a context}, L \text{ is a lattice of secrecy levels}\}$$

To show the claim, it suffices to show that $\mathcal{R}$ is a barbed bisimulation.

Fix $C$ be a context, and processes $P_0$ and $P_1$ with $P_0 \simeq P_1$. Then $((C[P_0], L), (C[P_1], L)) \in \mathcal{R}$. We show that the conditions in Definition 4.15 hold.

(1) and (2) By Lemma F.6.

(3) We show $\mathrm{Barbs}(C[P_0], L) = \mathrm{Barbs}(C[P_1], L)$. To show the claim, we show $\mathrm{Barbs}(C[P_0], L) \subseteq \mathrm{Barbs}(C[P_1], L)$. Let $x \in \mathrm{Barbs}(C[P_0], L)$.

Assume $(C[P_0], L) \longrightarrow\!\!\!\!\!\rightarrow (Q, L'), Q = (\nu\tilde{y})x!\tilde{v}.Q_0 \mid Q_1$ with $x \notin \tilde{y}$. By Lemma F.5 and Lemma F.6, there exists a context $C'$ such that $(\nu\tilde{y})x!\tilde{v}.Q_0 \mid Q_1 = C'[P_0]$, $(C[P_1], L) \longrightarrow\!\!\!\!\!\rightarrow (Q', L')$, and $Q' \preceq C'[P_1]$.

Assume $C' = [\,]$ and $P_0 = (\nu\tilde{y})x!\tilde{v}.Q_0 \mid Q_1$. In this case, $(C[P_1], L) \longrightarrow\!\!\!\!\!\rightarrow (P_1, L')$. Since $P_1 \preceq P_0$, we have $(C[P_1], L) \longrightarrow\!\!\!\!\!\rightarrow ((\nu\tilde{y})x!\tilde{v}.Q_0 \mid Q_1, L')$. Hence, $x \in \mathrm{Barbs}(C[P_1], L)$.

Assume $C' = (\nu\tilde{y})[\,]$ and $P_0 = x!\tilde{v}.Q_0 \mid Q_1$. In this case, $(C[P_1], L) \longrightarrow\!\!\!\!\!\rightarrow ((\nu\tilde{y})P_1, L')$. Since $P_1 \preceq P_0$, we have $(\nu\tilde{y})P_1 \preceq (\nu\tilde{y})P_1$. Hence, we have $(C[P_1], L) \longrightarrow\!\!\!\!\!\rightarrow ((\nu\tilde{y})x!\tilde{v}.Q_0 \mid Q_1, L')$. Therefore, $x \in \mathrm{Barbs}(C[P_1], L)$.

Assume $C' = (\nu\tilde{y})[\,] \mid C_1$ and $P_0 = x!\tilde{v}.Q_0$ for some context $C_1$. In this case, $(C[P_1], L) \longrightarrow\!\!\!\!\!\rightarrow ((\nu\tilde{y})P_1 \mid C_1[P_1], L')$. Since $P_1 \preceq P_0$, we have $(\nu\tilde{y})P_1 \mid C_1[P_1] \preceq (\nu\tilde{y})x!\tilde{v}.Q_0 \mid C_1[P_1]$. Hence, we have $(C[P_1], L) \longrightarrow\!\!\!\!\!\rightarrow ((\nu\tilde{y})x!\tilde{v}.Q_0 \mid C_1[P_1], L')$. Therefore, $x \in \mathrm{Barbs}(C[P_1], L)$.

Assume $C' = (\nu\tilde{y})x!\tilde{v}.C_1 \mid C_1$ for some contexts $C_0$ and $C_1$. In this case, $(C[P_1], L) \longrightarrow\!\!\!\!\!\rightarrow ((\nu\tilde{y})x!\tilde{v}.C_0[P_1] \mid C_1[P_1], L')$. Hence, $x \in \mathrm{Barbs}(C[P_1], L)$.

In the similar way to the case $(C[P_0], L) \longrightarrow\!\!\!\!\!\rightarrow (Q, L'), Q = (\nu\tilde{y})x!\tilde{v}.Q_0 \mid Q_1$, we have $x \in \mathrm{Barbs}(C[P_1], L)$ if $(C[P_0], L) \longrightarrow\!\!\!\!\!\rightarrow (Q, L'), Q = (\nu\tilde{y})x?\tilde{z}.Q_0 \mid Q_1$ with $x \notin \tilde{y}$. Therefore, $\mathrm{Barbs}(C[P_0], L) \subseteq \mathrm{Barbs}(C[P_1], L)$.

In the same way to the case $\mathrm{Barbs}(C[P_0], L) \subseteq \mathrm{Barbs}(C[P_1], L)$, we have $\mathrm{Barbs}(C[P_1], L) \subseteq \mathrm{Barbs}(C[P_0], L)$. Thus, $\mathrm{Barbs}(C[P_0], L) = \mathrm{Barbs}(C[P_1], L)$. □

**Lemma F.8.** *For processes $P$, $P'$, $Q$, $Q'$ and a lattice of secrecy level $L$, if $P \underset{(\Gamma \| L, l)}{\approx} Q$, $P' \simeq P$, and $Q \simeq Q'$, then $P' \underset{(\Gamma \| L, l)}{\approx} Q'$.*

*Proof.* Assume $P \underset{(\Gamma \| L, l)}{\approx} Q$, $P' \simeq P$, and $Q \simeq Q'$. We show that the conditions in Definition 4.17 hold.

(1) By Lemma D.4.

(2) Fix $C$ be an $(\Gamma \parallel L, l)$-$(\Delta \parallel L', l')$-context. Then, we have $(C[P], L') \overset{\bullet}{\approx} (C[Q], L')$. Since $P' \simeq P$, and $Q \simeq Q'$, Lemma F.7 implies $(C[P'], L') \overset{\bullet}{\approx} (C[P], L')$ and $(C[Q], L') \overset{\bullet}{\approx} (C[Q'], L')$. By Lemma F.2, we have $(C[P'], L') \overset{\bullet}{\approx} (C[Q'], L')$. □

## F.2. Definition of Er

**Definition F.9** (Er)**.** For a type environment $\Gamma$, a lattice of secrecy levels $L$, and a secrecy level $l \in L$, we inductively define $\mathrm{Er}_\Gamma^{L,l}(P)$ as follows:

$$\mathrm{Er}_\Gamma^{L,l}(\mathsf{0}) = \mathsf{0} \qquad \text{if } P = \mathsf{0},$$

$$\mathrm{Er}_\Gamma^{L,l}(v) = \mathrm{unit} \qquad \text{if } P = v,\ v \text{ is a value, and } \Gamma(v) \text{ is not } l \text{ and not lower than } l \text{ in } L,$$

$$\mathrm{Er}_\Gamma^{L,l}(v) = v \qquad \text{if } P = v,\ v \text{ is a value, and } \Gamma(v) \text{ is } l \text{ or lower than } l \text{ in } L,$$

$$\mathrm{Er}_\Gamma^{L,l}(P_0 \mid P_1) = \mathrm{Er}_\Gamma^{L,l}(P_0) \mid \mathrm{Er}_\Gamma^{L,l}(P_1) \qquad \text{if } P = P_0 \mid P_1 \text{ for processes } P_0 \text{ and } P_1,$$

$$\mathrm{Er}^{L,l}_{\Gamma}(*P') = \mathsf{0}$$
if $P = *P'$ and $\mathrm{Er}^{L,l}_{\Gamma}(P') \simeq \mathsf{0}$ for a process $P'$,

$$\mathrm{Er}^{L,l}_{\Gamma}(*P') = *\mathrm{Er}^{L,l}_{\Gamma}(P')$$
if $P = *P'$ and $\mathrm{Er}^{L,l}_{\Gamma}(P') \not\simeq \mathsf{0}$ for a process $P'$,

$$\mathrm{Er}^{L,l}_{\Gamma}(x!(v_0,\ldots,v_n).P') = x!v'_0,\ldots,v'_n.\,\mathrm{Er}^{L,l}_{\Gamma}(P')$$
if $P = x!(v_0,\ldots,v_n).P'$ for a process $P'$, $\Gamma(x)$ is the form $\langle \tau_0,\ldots,\tau_n\rangle^{l'}/U$ with $l' \leq_L l$, and $v'_i = \mathrm{Er}^{L}_{\Gamma}(v_i)$ for all $i = 0,\ldots,n$,

$$\mathrm{Er}^{L,l}_{\Gamma}(x!(v_0,\ldots,v_n).P') = \mathrm{Er}^{L,l}_{\Gamma}(P')$$
if $P = x!(v_0,\ldots,v_n).P'$ for a process $P'$, and $\Gamma(x)$ is *not* the form $\langle \tau_0,\ldots,\tau_n\rangle^{l'}/U$ with $l' \leq_L l$,

$$\mathrm{Er}^{L,l}_{\Gamma}(x?(y_0,\ldots,y_n).P') = x?y_0,\ldots,y_n.\,\mathrm{Er}^{L,l}_{\Gamma,y_0:\tau_0,\ldots,y_n:\tau_n}(P')$$
if $P = x?(y_0,\ldots,y_n).P'$ for a program $P'$, and $\Gamma(x)$ is the form $\langle \tau_0,\ldots,\tau_n\rangle^{l'}/U$ with $l' \leq_L l$,

$$\mathrm{Er}^{L,l}_{\Gamma}(x?(y_0,\ldots,y_n).P') = \mathrm{Er}^{L,l}_{\Gamma,y_0:\tau_0,\ldots,y_n:\tau_n}(P')$$
if $P = x?(y_0,\ldots,y_n).P'$ for a process $P'$, and $\Gamma(x)$ is the form $\langle \tau_0,\ldots,\tau_n\rangle^{l'}/U$ with $l' \not\leq_L l$,

$$\mathrm{Er}^{L,l}_{\Gamma}(x?(y_0,\ldots,y_n).P') = \mathrm{Er}^{L,l}_{\Gamma,y_0:\mathtt{Unit},\ldots,y_n:\mathtt{Unit}}(P')$$
if $P = x?(y_0,\ldots,y_n).P'$ for a process $P'$, and $\Gamma(x)$ is *not* the form $\langle \tau_0,\ldots,\tau_n\rangle^{l'}/U$,

$$\mathrm{Er}^{L,l}_{\Gamma}((\nu x:\xi)P') = (\nu x:\xi)\mathrm{Er}^{L,l}_{\Gamma,x:\xi/\mathsf{0}}(P')$$
if $P = (\nu x:\xi)P'$ for a process $P'$, and $\xi$ is the form $\langle \tau_0,\ldots,\tau_n\rangle^{l'}$ with $l' \leq_L l$,

$$\mathrm{Er}^{L,l}_{\Gamma}((\nu x:\xi)P') = \mathrm{Er}^{L,l}_{\Gamma,x:\xi/\mathsf{0}}(P')$$
if $P = (\nu x:\xi)P'$ for a process $P'$, and $\xi$ is *not* the form $\langle \tau_1,\ldots,\tau_n\rangle^{l'}$ with $l' \leq_L l$,

$$\mathrm{Er}^{L,l}_{\Gamma}\Big(\Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big)P'\Big) = \Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big)\mathrm{Er}^{(\tilde{l_1}<\nu l_0<\tilde{l_2})L,l}_{\Gamma}(P') \quad \begin{array}{l}\text{if } P = \Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big)P' \\ \text{for a process } P', \text{ and} \\ l' \leq_L l \text{ for any } l' \in \tilde{l_1}, \tilde{l_2},\end{array}$$

$$\mathrm{Er}^{L,l}_{\Gamma}\Big(\Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big)P'\Big) = \mathrm{Er}^{(\tilde{l_1}<\nu l_0<\tilde{l_2})L,l}_{\Gamma}(P') \quad \begin{array}{l}\text{if } P = \Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big)P' \\ \text{for a process } P', \text{ and} \\ l' \not\leq_L l \text{ for some } l' \in \tilde{l_1}, \tilde{l_2},\end{array}$$

$$\mathrm{Er}^{L,l}_{\Gamma}(\mathtt{if}\ v\ \mathtt{then}\ P'\ \mathtt{else}\ P'') = \mathtt{if}\ v\ \mathtt{then}\ \mathrm{Er}^{L,l}_{\Gamma}(P')\ \mathtt{else}\ \mathrm{Er}^{L,l}_{\Gamma}(P'') \quad \begin{array}{l}\text{if } P = \mathtt{if}\ v\ \mathtt{then}\ P'\ \mathtt{else}\ P'' \\ \text{for processes } P', P'', \text{ and} \\ \Gamma(v) = \mathtt{Bool}^{l'} \text{ with } l' \leq_L l,\end{array}$$

$$\mathrm{Er}^{L,l}_{\Gamma}(\mathtt{if}\ v\ \mathtt{then}\ P'\ \mathtt{else}\ P'') = \mathtt{0} \quad \begin{array}{l}\text{if } P = \mathtt{if}\ v\ \mathtt{then}\ P'\ \mathtt{else}\ P'' \\ \text{for processes } P', P'', \text{ and} \\ \Gamma(v) = \mathtt{Bool}^{l'} \text{ does } \textit{not} \text{ hold} \\ \text{with } l' \leq_L l.\end{array}$$

**Definition F.10** (The order of occurrences of $(- < \nu - < -)$'s in a process $P$)**.** For a process $P$, we define the order $\succ_P$ of occurrences of $(- < \nu - < -)$'s in $P$ as follows:

$\Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big) \succ_P \Big(\tilde{l'_1} < \nu l'_0 < \tilde{l'_2}\Big)$ if and only if $\Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big)P'$ is a subexpression of $P$, and $\Big(\tilde{l'_1} < \nu l'_0 < \tilde{l'_2}\Big)$ occurs in $P'$.

**Definition F.11** ($\mathrm{Er}^{L,l}_{\Gamma}(P)$-sublattice)**.** We say that a sublattice $L'$ of $L$ is an $\mathrm{Er}^{L,l}_{\Gamma}(P)$-sublattice if the following conditions hold:

(1) For occurrences of $\Big(\tilde{l_{1_0}} < \nu l_{0_0} < \tilde{l_{2_0}}\Big), \ldots, \Big(\tilde{l_{1_n}} < \nu l_{0_n} < \tilde{l_{2_n}}\Big)$ in $P$, where $\Big(\tilde{l_{1_i}} < \nu l_{0_i} < \tilde{l_{2_i}}\Big) \not\succ_P \Big(\tilde{l_{1_j}} < \nu l_{0_j} < \tilde{l_{2_j}}\Big)$ for $i < j$, if $\Big(\tilde{l_{1_0}} < \nu l_{0_0} < \tilde{l_{2_0}}\Big)\ldots\Big(\Big(\tilde{l_{1_n}} < \nu l_{0_n} < \tilde{l_{2_n}}\Big)L$ is defined, then there exist $j_0 < \cdots < j_m$ such that $\Big(\tilde{l_{1_{j_0}}} < \nu l_{0_{j_0}} < \tilde{l_{2_{j_0}}}\Big)\ldots\Big(\Big(\tilde{l_{1_{j_m}}} < \nu l_{0_{j_m}} < \tilde{l_{2_{j_m}}}\Big)L'$ is defined,

$$\Big\{\Big(\tilde{l_{1_{j_0}}} < \nu l_{0_{j_0}} < \tilde{l_{2_{j_0 0}}}\Big), \ldots, \Big(\tilde{l_{1_{j_m}}} < \nu l_{0_{j_m}} < \tilde{l_{2_{j_m}}}\Big)\Big\} = \Big\{\Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big) \;\Big|\; \Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big) \text{ occurs in } \mathrm{Er}^{L,l}_{\Gamma}(P)\Big\} \cap \Big\{\Big(\tilde{l_{1_0}} < \nu l_{0_0} < \tilde{l_{2_0}}\Big), \ldots, \Big(\tilde{l_{1_n}} < \nu l_{0_n} < \tilde{l_{2_n}}\Big)\Big\}.$$

(2) For occurrences of $\Big(\tilde{l'_{1_0}} < \nu l'_{0_0} < \tilde{l'_{2_0}}\Big), \ldots, \Big(\tilde{l'_{1_m}} < \nu l'_{0_m} < \tilde{l'_{2_m}}\Big)$ in $\mathrm{Er}^{L,l}_{\Gamma}(P)$, where $\Big(\tilde{l'_{1_i}} < \nu l'_{0_i} < \tilde{l'_{2_i}}\Big) \not\succ_{\mathrm{Er}^{L,l}_{\Gamma}(P)} \Big(\tilde{l'_{1_j}} < \nu l'_{0_j} < \tilde{l'_{2_j}}\Big)$ for $i < j$, if $\Big(\tilde{l'_{1_0}} < \nu l'_{0_0} < \tilde{l'_{2_0}}\Big)\ldots\Big(\Big(\tilde{l'_{1_m}} < \nu l'_{0_m} < \tilde{l'_{2_m}}\Big)L'$ is defined, then there exist $\Big(\tilde{l_{1_0}} < \nu l_{0_0} < \tilde{l_{2_0}}\Big), \ldots, \Big(\tilde{l_{1_n}} < \nu l_{0_n} < \tilde{l_{2_n}}\Big)$ such that $\Big(\tilde{l_{1_0}} < \nu l_{0_0} < \tilde{l_{2_0}}\Big)\ldots\Big(\Big(\tilde{l_{1_n}} < \nu l_{0_n} < \tilde{l_{2_n}}\Big)L$ is defined,

$$\Big\{\Big(\tilde{l_{1_0}} < \nu l_{0_0} < \tilde{l_{2_0}}\Big), \ldots, \Big(\tilde{l_{1_n}} < \nu l_{0_n} < \tilde{l_{2_n}}\Big)\Big\} = \Big\{\Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big) \;\Big|\; \Big(\tilde{l_1} < \nu l_0 < \tilde{l_2}\Big) \succ_P \Big(\tilde{l'_{1_i}} < \nu l'_{0_i} < \tilde{l'_{2_i}}\Big) \text{ for some } i = 0, \ldots, m\Big\},$$

and $\Big(\tilde{l_{1_i}} < \nu l_{0_i} < \tilde{l_{2_i}}\Big) \not\succ_P \Big(\tilde{l_{1_j}} < \nu l_{0_j} < \tilde{l_{2_j}}\Big)$ for $i < j$.

We note that $\Gamma(v)$ is lower than $l$ in $L$ for any value $v$ freely occurring in $\mathrm{Er}^{L,l}_{\Gamma}(P)$.

### F.3. Basic properties of Er

**Lemma F.12.** *For a type environments $\Gamma$, a lattice for secrecy levels $L$, a secrecy level $l \in L$ and a process $P$, if $\Gamma(x)$ is not lower than $l$ in $L$, then $x$ does not occur in $\mathrm{Er}^{L,l}_{\Gamma}(P)$.*

*Proof.* By induction on the construction of $P$. □

**Lemma F.13.** *For type environments $\Gamma$ and $\Gamma'$, a lattice for secrecy levels $L$, a secrecy level $l \in L$ and a process $P$, if $\Gamma(x) \sim \Gamma'(x)$ for any value $x$ occurring in $P$, then $\mathrm{Er}_{\Gamma}^{L,l}(P) \equiv \mathrm{Er}_{\Gamma'}^{L,l}(P)$.*

*Proof.* By induction on the construction of $P$. □

**Lemma F.14.** *For a type environments $\Gamma$, lattices for secrecy levels $L, L'$, a secrecy level $l \in L$, and a process $P$, if $L' \sqsubseteq L$ and $\mathrm{Er}_{\Gamma}^{L',l}(P) \simeq \mathsf{0}$, then $\mathrm{Er}_{\Gamma}^{L,l}(P) \simeq \mathsf{0}$.*

*Proof.* By induction on the construction of $P$. □

**Lemma F.15.** *For a type environment $\Gamma$,a lattice for secrecy levels $L$, secrecy levels $l, l' \in L$, and a process $P$, if $l \leq_L l'$ and $\mathrm{Er}_{\Gamma}^{L,l'}(P) \simeq \mathsf{0}$, then $\mathrm{Er}_{\Gamma}^{L,l}(P) \simeq \mathsf{0}$.*

*Proof.* By induction on the construction of $P$. □

**Lemma F.16.** *If $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, then $\mathrm{Er}_{\Gamma}^{L,l}(P) \simeq \mathsf{0}$ for any secrecy level $l \not\geq_L m$.*

*Proof.* Assume that $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable. We show $\mathrm{Er}_{\Gamma}^{L,l}(P) \equiv \mathsf{0}$ by induction on $k$-secure derivation tree of $\Gamma \parallel L \rhd_l P$. We proceed by a case analysis of the rule used at the root.
Case 1. In case the rule used at the root is (T-Zero), the claimed result holds obviously.
Case 2. Assume that the rule used at the root is (T-New). In this case, there exists a process $P'$ such that $P \equiv (\nu x : \xi)P'$. Then $\Gamma, x : \xi/U \parallel L \rhd_m P'$ is derivable. Let $l \not\geq_L m$. By the induction hypothesis, $\mathrm{Er}_{\Gamma, x:\xi/U}^{L,l}(P') \simeq \mathsf{0}$.

Assume that $\xi$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l''}$ for $l'' \leq_L l$. Then $\mathrm{Er}_{\Gamma}^{L,l}((\nu x : \xi)P') \equiv (\nu x : \xi)\mathrm{Er}_{\Gamma, x:\xi/\mathsf{0}}^{L,l}(P')$. By Lemma F.13, we have $(\nu x : \xi)\mathrm{Er}_{\Gamma, x:\xi/\mathsf{0}}^{L,l}(P') \simeq (\nu x : \xi)\mathsf{0} \simeq \mathsf{0}$. Hence, we see $\mathrm{Er}_{\Gamma}^{L,l}(P) \simeq \mathsf{0}$.

Assume that $\xi$ is not the form $\langle \tau_1, \ldots, \tau_n \rangle^{l''}$ with $l'' \leq_L l$. Then $\mathrm{Er}_{\Gamma}^{L,l}((\nu x : \xi)P') \equiv \mathrm{Er}_{\Gamma, x:\xi/\mathsf{0}}^{L,l}(P')$. By Lemma F.13, $\mathrm{Er}_{\Gamma, x:\xi/U}^{L,l}(P') \simeq \mathsf{0}$. Hence, we have $\mathrm{Er}_{\Gamma}^{L,l}(P) \simeq \mathsf{0}$.
Case 3. Assume that the rule used at the root is (T-Rep). In this case, there exist a process $P'$ and a type environment $\Gamma'$ such that $P \equiv *P'$ and $\Gamma = *\Gamma'$. Then $\Gamma' \parallel L \rhd_m P'$ is derivable. Let $l \not\geq_L m$. By the induction hypothesis, $\mathrm{Er}_{\Gamma'}^{L,l}(P') \simeq \mathsf{0}$. By Lemma F.13, $\mathrm{Er}_{\Gamma}^{L,l}(P') \simeq \mathsf{0}$. Hence, $\mathrm{Er}_{\Gamma}^{L,l}(P) \equiv \mathsf{0}$.
Case 4. Assume that the rule used at the root is (T-Par). In this case, there exist processes $P_0$ and $P_1$ such that $P \equiv P_0 \mid P_1$. Then, there exist type environments $\Gamma_0$ and $\Gamma_1$ such that $\Gamma \equiv \Gamma_0 \mid \Gamma_1$ and $\Gamma_i \parallel L \rhd_m P_i$ is derivable for $i = 0, 1$. Let $l \not\geq_L m$. By the induction hypothesis, $\mathrm{Er}_{\Gamma_i}^{L,l}(P_i) \simeq \mathsf{0}$ for $i = 0, 1$. By Lemma F.13, we have $\mathrm{Er}_{\Gamma_i}^{L,l}(P_i) \equiv \mathrm{Er}_{\Gamma}^{L,l}(P_i)$ for $i = 0, 1$. Then $\mathrm{Er}_{\Gamma}^{L,l}(P_0 \mid P_1) \simeq \mathsf{0} \mid \mathsf{0} \simeq \mathsf{0}$.
Case 5. Assume that the rule used at the root is (T-If). In this case, there exist a type environment $\Gamma'$ and processes $P_0$ and $P_1$ such that $\Gamma \equiv \Gamma' \mid v : \mathtt{Bool}^l$ and $P \equiv \mathtt{if}\ v\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1$ hold and $\Gamma' \parallel L \rhd_m P_i$ is derivable for $i = 0, 1$. Let $l \not\geq_L m$. Since $\Gamma(v) = \mathtt{Bool}^l$, we see $\mathrm{Er}_{\Gamma}^{L,l}(\mathtt{if}\ v\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1) \equiv \mathsf{0}$.
Case 6. Assume that the rule used at the root is (T-Out). In this case, there exist a process $P'$, a type environments $\Gamma'$, secrecy levels $l'_0, l'_1 \in L$, types $\tilde{\tau}$, a usage $U$ and $t_c \in \mathbb{N} \cup \{\infty\}$ such that $P \equiv x!\tilde{v}.P'$, $m \leq_L l'_1$ and $\Gamma \equiv \uparrow^{(t_c+1,t_c+1)} \Gamma' \mid \tilde{v} : \uparrow\tilde{\tau} \mid x : \langle\tilde{\tau}\rangle^{l'_0}/O^0_{t_c}U$ with $m \leq_L l'_0$, $t_c = \infty$ implies $l'_0 \leq_L l'_1$, and $\Gamma', x : \langle\tilde{\tau}\rangle^{l'_0}/U \parallel L \rhd_{l'_1} P'$ is derivable. Let $l \not\geq_L m$. Since $m \leq_L l'_1$, we have $l \not\geq_L l'_1$. By the induction hypothesis, $\mathrm{Er}^{L,l}_{\Gamma', x:\langle\tilde{\tau}\rangle^{l'_0}/U}(P') \simeq \mathsf{0}$. Since $l \not\geq_L m$ and $m \leq_L l'_0$, we have $l'_0 \not\leq_L l$. Since $l'_0 \not\leq_L l$, we have

$$\mathrm{Er}^{L,l}_{\uparrow^{(t_c+1,t_c+1)}\Gamma' \mid \tilde{v}:\uparrow\tilde{\tau} \mid x:\langle\tilde{\tau}\rangle^{l'_0}/O^0_{t_c}U}(x!\tilde{v}.P') \equiv \mathrm{Er}^{L,l}_{\uparrow^{(t_c+1,t_c+1)}\Gamma' \mid \tilde{v}:\uparrow\tilde{\tau} \mid x:\langle\tilde{\tau}\rangle^{l'_0}/O^0_{t_c}U}(P').$$

By Lemma F.13, we have

$$\mathrm{Er}^{L,l}_{\uparrow^{(t_c+1,t_c+1)}\Gamma' \mid \tilde{v}:\uparrow\tilde{\tau} \mid x:\langle\tilde{\tau}\rangle^{l'_0}/O^0_{t_c}U}(x!\tilde{v}.P') \equiv \mathrm{Er}^{L,l}_{\Gamma', x:\langle\tilde{\tau}\rangle^{l'_0}/U}(P') \simeq \mathsf{0}.$$

Case 7. Assume that the rule used at the root is (T-In). In this case, there exist a process $P'$, a type environments $\Gamma'$, secrecy levels $l'_0, l'_1 \in L$, types $\tilde{\tau}$, a usage $U$ and $t_c \in \mathbb{N} \cup \{\infty\}$ such that $P \equiv x?(\tilde{y}).P'$, $\Gamma \equiv \left(\uparrow^{(t_c+1,t_c+1)}\Gamma', x : \langle\tilde{\tau}\rangle^{l'_0}/I^0_{t_c}U\right)$, $m \leq_L l'_0$, and $m \leq_L l'_1$ hold, $t_c = \infty$ implies $l'_0 \leq_L l'_1$, and $\Gamma', x : \langle\tilde{\tau}\rangle^{l'_0}/U, \tilde{y} : \tilde{\tau} \parallel L \rhd_{l'_1} P'$ is derivable. Let $l \not\geq_L m$. Since $m \leq_L l'_1$, we have $l \not\geq_L l'_1$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma', x:\langle\tilde{\tau}\rangle^{l'_0}/U, \tilde{y}:\tilde{\tau}}(P') \simeq \mathsf{0}$. Since $l \not\geq_L m$ and $m \leq_L l'_0$, we have $l'_0 \not\leq_L l$. Since $l'_0 \not\leq_L l$, we have

$$\mathrm{Er}^{L,l}_{\left(\uparrow^{(t_c+1,t_c+1)}\Gamma', x:\langle\tilde{\tau}\rangle^{l'_0}/I^0_{t_c}U\right)}(x?(\tilde{y}).P') \equiv \mathrm{Er}^{L,l}_{\left(\uparrow^{(t_c+1,t_c+1)}\Gamma', x:\langle\tilde{\tau}\rangle^{l'_0}/I^0_{t_c}U\right), \tilde{y}:\tilde{\tau}}(P').$$

By Lemma F.13, we have

$$\mathrm{Er}^{L,l}_{\left(\uparrow^{(t_c+1,t_c+1)}\,\Gamma',x:\langle\tilde{\tau}\rangle^{l'_0}/I^0_{t_c}U\right)}(x?(\tilde{y}).P') \equiv \mathrm{Er}^{L,l}_{\left(\uparrow^{(t_c+1,t_c+1)}\,\Gamma',x:\langle\tilde{\tau}\rangle^{l'_0}/I^0_{t_c}U\right),\tilde{y}:\tilde{\tau}}(P') \simeq 0.$$

Case 8. Assume that the rule used at the root is (T-NewSec). In this case, $m \leq_L l'$ for any $l'' \in \tilde{l_2}, \tilde{l_3}$, and there exist a process $P'$ such that $P \equiv \left(\tilde{l_2} < \nu l_1 < \tilde{l_3}\right)P'$. Then, the assumption of the rule instance $\Gamma \parallel \left(\tilde{l_2} < \nu l_1 < \tilde{l_3}\right)L \rhd_m P'$ is derivable. Let $l \not\geq_L m$. By the induction hypothesis, we have $\mathrm{Er}^{\left(\tilde{l_2}<\nu l_1<\tilde{l_3}\right)L,l}_{\Gamma}(P') \simeq 0$. For any $l' \in \tilde{l_2}$ and $\tilde{l_3}$, because of $m \leq_L l'$, we have $l' \not\leq_L l$. Then $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv \mathrm{Er}^{\left(\tilde{l_2}<\nu l_1<\tilde{l_3}\right)L,l}_{\Gamma}(P') \simeq 0$.
Case 9. Assume that the rule used at the root is (T-Weak). In this case, there exist a type environments $\Gamma'$, a lattice for secrecy levels $L'$, a secrecy level $l' \in L'$ such that $\Gamma <: \Gamma'$, $L' \sqsubseteq L$, and $l \leq_L l'$, and $\Gamma' \parallel L' \rhd_{l'} P$ is derivable. Let $l \not\geq_L m$. By the induction hypothesis, we have $\mathrm{Er}^{L',l'}_{\Gamma'}(P) \simeq 0$. By Lemma F.13, Theorem F.14, and Theorem F.15, we see $\mathrm{Er}^{L,l}_{\Gamma}(P) \simeq 0$. □

## F.4. $\mathrm{Er}^{L,l}_{\Gamma}(P)$ can simulate $P$

**Lemma F.17.** *If $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, the secrecy level of $\Gamma \parallel L$ is $l_1$, and $P \preceq P'$, then $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$ for any secrecy level $l \not\leq_L l_1$.*

*Proof.* Assume that $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable and $P \preceq P'$. Let $l_1$ be the secrecy level of $\Gamma \parallel L$. Fix $l \not\leq_L l_1$. We show $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$ by induction on the construction of $P \preceq P'$. We consider cases according to the last rule of the construction of $P \preceq P'$.

Case 1. If $P' \equiv P$, then $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$ obviously.

Case 2. Assume that there exists a process $Q$ such that $P \preceq Q$ and $Q \preceq P'$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(Q)$ and $\mathrm{Er}^{L,l}_{\Gamma}(Q) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$. Hence, $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$.

Case 3. (SP-Zero1). Assume $P' \equiv P \mid 0$. Then $\mathrm{Er}^{L,l}_{\Gamma}(P') \equiv \mathrm{Er}^{L,l}_{\Gamma}(P) \mid \mathrm{Er}^{L,l}_{\Gamma}(0) \equiv \mathrm{Er}^{L,l}_{\Gamma}(P) \mid 0$. Hence, $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P) \mid 0 \equiv \mathrm{Er}^{L,l}_{\Gamma}(P')$.

In the same way, we can show $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$ in case $P \equiv P' \mid 0$.

Case 4. (SP-Zero2). Assume $P \equiv 0$ and $P' \equiv (\nu x : \xi)0$. Then $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv 0$. If $\xi$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}$ with $l' \leq_L l$, then $\mathrm{Er}^{L,l}_{\Gamma}(P') \equiv (\nu x : \xi)\mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(0) \equiv (\nu x : \xi)0$. If $\xi$ is not the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}$ with $l' \leq_L l$, then $\mathrm{Er}^{L,l}_{\Gamma}(P') \equiv 0$. In both cases, we have $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$.

In the same way, we can show $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$ in case $P \equiv (\nu x : \xi)0$ and $P' \equiv 0$.

Case 5. (SP-Commut). Assume $P \equiv P_0 \mid P_1$ and $P' \equiv P_1 \mid P_0$ with processes $P_0$ and $P_1$. Then $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv \mathrm{Er}^{L,l}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,l}_{\Gamma}(P_1)$ and $\mathrm{Er}^{L,l}_{\Gamma}(P') \equiv \mathrm{Er}^{L,l}_{\Gamma}(P_1) \mid \mathrm{Er}^{L,l}_{\Gamma}(P_0)$. We have $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$.

Case 6. (SP-Assoc). Assume $P \equiv (P_0 \mid P_1) \mid P_2$ and $P' \equiv P_0 \mid (P_1 \mid P_2)$ with processes $P_0$, $P_1$, and $P_2$. Then $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,l}_{\Gamma}(P_1)\right) \mid \mathrm{Er}^{L,l}_{\Gamma}(P_2)$ and $\mathrm{Er}^{L,l}_{\Gamma}(P') \equiv \mathrm{Er}^{L,l}_{\Gamma}(P_0) \mid \left(\mathrm{Er}^{L,l}_{\Gamma}(P_1) \mid \mathrm{Er}^{L,l}_{\Gamma}(P_2)\right)$. We have $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$.

Case 7. (SP-New). Assume $P \equiv (\nu x : \xi)P_0 \mid P_1$ and $P' \equiv (\nu x : \xi)P_0 \mid P_1$ with processes $P_0$, $P_1$, and $x \notin \mathrm{FN}(P_1)$. If $\xi$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}$ with $l' \leq_L l$, then $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv (\nu x : \xi)\mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_0) \mid \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_1)$ and $\mathrm{Er}^{L,l}_{\Gamma}(P') \equiv (\nu x : \xi)\mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_0) \mid \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_1)$. If $\xi$ is not the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}$ with $l' \leq_L l$, then $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_0) \mid \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_1)$ and $\mathrm{Er}^{L,l}_{\Gamma}(P') \equiv \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_0) \mid \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_1)$. In both cases, we have $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$.

Case 8. (SP-IfT). Assume $P \equiv \mathtt{if}\ \mathrm{true}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1$ and $P' \equiv P_0$ with processes $P_0$ and $P_1$. By Lemma D.1 (8), there exist a type environments $\Gamma'$, a lattice for secrecy levels $L'$, and $l'' \in L'$ such that $L' \sqsubseteq L$, $m \leq_L l''$, and $\Gamma <: \left(\Gamma' \mid \mathrm{true}^{l'} : \mathtt{Bool}^{l''}\right)$, and both $\Gamma' \parallel L' \rhd_{l''} P_0$ and $\Gamma' \parallel L' \rhd_{l''} P_1$ are derivable. Then $l' = l''$. We consider cases according to $l'$.

Assume $l' \leq_L l$. Then $\mathrm{Er}^{L,l}_{\Gamma}\left(\mathtt{if}\ \mathrm{true}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1\right) \equiv \mathtt{if}\ \mathrm{true}^{l'}\ \mathtt{then}\ \mathrm{Er}^{L,l}_{\Gamma}(P_0)\ \mathtt{else}\ \mathrm{Er}^{L,l}_{\Gamma}(P_1)$. Hence, $\mathrm{Er}^{L,l}_{\Gamma}\left(\mathtt{if}\ \mathrm{true}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1\right) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P_0)$.

Assume $l' \not\leq_L l$. Then $\mathrm{Er}^{L,l}_{\Gamma}\left(\mathtt{if}\ \mathrm{true}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1\right) \equiv 0$. By Theorem F.16, we have $\mathrm{Er}^{L',l}_{\Gamma'}(P_0) \simeq 0$. By Lemma F.13 and Theorem F.14, we have $\mathrm{Er}^{L,l}_{\Gamma}(P_0) \simeq 0$. Hence, $\mathrm{Er}^{L,l}_{\Gamma}\left(\mathtt{if}\ \mathrm{true}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1\right) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P_0)$.

Case 9. (SP-IfF). Assume $P \equiv \mathtt{if}\ \mathrm{false}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1$ and $P' \equiv P_1$ with processes $P_0$ and $P_1$. By Lemma D.1 (8), there exist a type environments $\Gamma'$, a lattice for secrecy levels $L'$, and $l'' \in L'$ such that $L' \sqsubseteq L$, $m \leq_L l''$, and $\Gamma <: \left(\Gamma' \mid \mathrm{false}^{l'} : \mathtt{Bool}^{l''}\right)$, and both $\Gamma' \parallel L' \rhd_{l''} P_0$ and $\Gamma' \parallel L' \rhd_{l''} P_1$ are derivable. Then $l' = l''$. We consider cases according to $l'$.

Assume $l' \leq_L l$. Then $\mathrm{Er}^{L,l}_{\Gamma}\left(\mathtt{if}\ \mathrm{false}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1\right) \equiv \mathtt{if}\ \mathrm{false}^{l'}\ \mathtt{then}\ \mathrm{Er}^{L,l}_{\Gamma}(P_0)\ \mathtt{else}\ \mathrm{Er}^{L,l}_{\Gamma}(P_1)$. Hence, $\mathrm{Er}^{L,l}_{\Gamma}\left(\mathtt{if}\ \mathrm{false}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1\right) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P_1)$.

Assume $l' \not\leq_L l$. Then $\mathrm{Er}^{L,l}_{\Gamma}\left(\mathtt{if}\ \mathrm{false}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1\right) \equiv 0$. By Theorem F.16, we have $\mathrm{Er}^{L',l}_{\Gamma'}(P_1) \simeq 0$. By Lemma F.13 and Theorem F.14, we have $\mathrm{Er}^{L,l}_{\Gamma}(P_1) \simeq 0$. Hence, $\mathrm{Er}^{L,l}_{\Gamma}\left(\mathtt{if}\ \mathrm{false}^{l'}\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1\right) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P_1)$.

Case 10. (SP-Rep). Assume $P \equiv *P_0$ and $P' \equiv *P_0 \mid P_0$ with a process $P_0$. We consider cases according to $\mathrm{Er}^{L,l}_{\Gamma}(P_0)$.

Assume $\mathrm{Er}^{L,l}_{\Gamma}(P_0) \simeq 0$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(*P_0) \equiv 0$. We also have $\mathrm{Er}^{L,l}_{\Gamma}(*P_0 \mid P_0) \equiv 0 \mid \mathrm{Er}^{L,l}_{\Gamma}(P_0)$. By (SP-Zero1) and Lemma A.5 (1), we have $\mathrm{Er}^{L,l}_{\Gamma}(*P_0) \equiv 0 \preceq 0 \mid 0 \preceq 0 \mid \mathrm{Er}^{L,l}_{\Gamma}(P_0) \equiv \mathrm{Er}^{L,l}_{\Gamma}(*P_0 \mid P_0)$.

Assume $\mathrm{Er}^{L,l}_{\Gamma}(P_0) \not\simeq 0$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(*P_0) \equiv *\mathrm{Er}^{L,l}_{\Gamma}(P_0)$. Hence, we have $\mathrm{Er}^{L,l}_{\Gamma}(*P_0) \equiv *\mathrm{Er}^{L,l}_{\Gamma}(P_0) \preceq *\mathrm{Er}^{L,l}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,l}_{\Gamma}(P_0) \preceq \mathrm{Er}^{L,l}_{\Gamma}(*P_0 \mid P_0)$.

Case 11. (SP-Par). Assume $P \equiv P_0 \mid P_1$ and $P' \equiv P'_0 \mid P_1$ with $P_0 \preceq P'_0$ for process $P_0$, $P_1$, and $P'_0$. Then $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv \mathrm{Er}^{L,l}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,l}_{\Gamma}(P_1)$ and $\mathrm{Er}^{L,l}_{\Gamma}(P') \equiv \mathrm{Er}^{L,l}_{\Gamma}(P'_0) \mid \mathrm{Er}^{L,l}_{\Gamma}(P_1)$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma}(P_0) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P'_0)$. We have $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$.

Case 12. (SP-CNew). Assume $P \equiv (\nu x : \xi)P_0$ and $P' \equiv (\nu x : \xi)P'_0$ with $P_0 \preceq P'_0$ for process $P_0$ and $P'_0$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_0) \preceq \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P'_0)$. If $\xi$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}$ with $l' \leq_L l$, then $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv (\nu x : \xi)\mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_0)$ and $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv (\nu x : \xi)\mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P'_0)$. If $\xi$ is not the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}$ with $l' \leq_L l$, then $\mathrm{Er}^{L,l}_{\Gamma}(P) \equiv \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P_0)$ and $\mathrm{Er}^{L,l}_{\Gamma}(P') \equiv \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P'_0)$. In both cases, we have $\mathrm{Er}^{L,l}_{\Gamma}(P) \preceq \mathrm{Er}^{L,l}_{\Gamma}(P')$. □

**Lemma F.18.** *Let $y_0, \ldots, y_n$ be channel names, $v_0, \ldots, v_n$ be values and $v'_i$ be $\mathrm{Er}^{L,l}_{\Gamma}(v_i)$. Let $\tilde{y} = (y_0, \ldots, y_n)$, $\tilde{v} = (v_0, \ldots, v_n)$, and $\tilde{v'} = (v'_0, \ldots, v'_n)$.*

*$\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$ with $\tilde{\tau} = (\Gamma(v_0), \ldots, \Gamma(v_n))$ for a value or process $P$.*

*Proof.* We show $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$ by induction on the construction of $P$. We consider cases according to the form of $P$.

Case 1. Assume $P \equiv w$ for a value $w$.

Assume $w \not\equiv y_i$ for $i = 0, \ldots, n$. Then $\mathrm{Er}^{L,l}_{\Gamma}(w[\tilde{y} \mapsto \tilde{v}]) \equiv \mathrm{Er}^{L,l}_{\Gamma}(w)$. By Lemma F.13, $\mathrm{Er}^{L,l}_{\Gamma}(w) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(w)\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$.

Assume $w \equiv y_i$ for $i = 0, \ldots, n$. Then $\mathrm{Er}^{L,l}_{\Gamma}(y_i[\tilde{y} \mapsto \tilde{v}]) \equiv \mathrm{Er}^{L,l}_{\Gamma}(v_i)$.

We consider the case where $\Gamma(v_i)$ is not lower than $l$ in $L$. In this case, $\mathrm{Er}^{L,l}_{\Gamma}(v_i) \equiv \mathrm{unit}$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(y_i) \equiv \mathrm{unit}$. Hence, we have $\mathrm{Er}^{L,l}_{\Gamma}(v_i) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(y_i)\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$.

We consider the case where $\Gamma(v_i)$ is lower than $l$ in $L$. In this case, $\mathrm{Er}^{L,l}_{\Gamma}(v_i) \equiv v_i \equiv v'_i$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(y_i) \equiv y_i$. Hence, we have $\mathrm{Er}^{L,l}_{\Gamma}(v_i) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(y_i)\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$.

Case 2. Assume $P \equiv 0$. In this case, $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv 0$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv 0$. Hence, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$.

Case 3. Assume $P \equiv P_0 \mid P_1$. In this case, $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \mathrm{Er}^{L,l}_{\Gamma}(P_0[\tilde{y} \mapsto \tilde{v}]) \mid \mathrm{Er}^{L,l}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv \mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_0) \mid \mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_1)$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma}(P_i[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_i)\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$ for $i = 0, 1$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$.

Case 4. Assume $P \equiv *P'$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$. We consider cases according to the form of $\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}])$.

Assume $\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}]) \simeq 0$. Then $\mathrm{Er}^{L,l}_{\Gamma}(*P'[\tilde{y} \mapsto \tilde{v}]) \equiv 0$. Since $\left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\right)\left[\tilde{y} \mapsto \tilde{v'}\right] \simeq 0$, we have $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P') \simeq 0$. Hence, $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(*P') \equiv 0$. Then, we have $\left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(*P')\right)\left[\tilde{y} \mapsto \tilde{v'}\right] \equiv 0$. Thus, $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)\left[\tilde{y} \mapsto \tilde{v'}\right]$.

Assume $\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}]) \not\equiv \mathsf{0}$. Then $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv *\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv *\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')$. We have

$$\begin{aligned}\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) &\equiv *\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}]) \\ &\equiv \Big(*\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big] \\ &\equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\Big)\big[\tilde{y} \mapsto \tilde{v'}\big].\end{aligned}$$

Thus, $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]$.

Case 5. Assume $P \equiv x!\tilde{w}.P'$. Let $x' \equiv x\big[\tilde{y} \mapsto \tilde{v'}\big]$ and $\tilde{w'} \equiv \tilde{w}\big[\tilde{y} \mapsto \tilde{v'}\big]$. We consider cases according to the form of $\Gamma(x)$.

Assume that $\Gamma(x)$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}/U$ with $l' \leq_L l$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv x'!\tilde{w'}.\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv x!\tilde{w}.\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}]) \equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]$. Then, we have

$$\begin{aligned}\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) &\equiv x'!\tilde{w'}.\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}]) \\ &\equiv x'!\tilde{w'}.\Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big] \\ &\equiv \Big(x!\tilde{w}.\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big] \\ &\equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\Big)\big[\tilde{y} \mapsto \tilde{v'}\big].\end{aligned}$$

Assume that $\Gamma(x)$ is *not* the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}/U$ with $l' \leq_L l$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv \mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}]) \equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]$.

Case 6. Assume $P \equiv x?\tilde{z}.P'$. Let $x' \equiv x\big[\tilde{y} \mapsto \tilde{v'}\big]$. We consider cases according to the form of $\Gamma(x)$.

Assume that $\Gamma(x)$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}/U$ with $l' \leq_L l$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv x'?\tilde{z}.\mathrm{Er}^{L,l}_{\Gamma,\tilde{z}:\tilde{\tau'}}(P'[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv x?\tilde{z}.\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},\tilde{z}:\tilde{\tau'}}(P')$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma,\tilde{z}:\tilde{\tau'}}(P'[\tilde{y} \mapsto \tilde{v}]) \equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},\tilde{z}:\tilde{\tau'}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]$. Then, we have

$$\begin{aligned}\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) &\equiv x'?\tilde{z}.\mathrm{Er}^{L,l}_{\Gamma,\tilde{z}:\tilde{\tau'}}(P'[\tilde{y} \mapsto \tilde{v}]) \\ &\equiv x'?\tilde{z}.\Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},\tilde{z}:\tilde{\tau'}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big] \\ &\equiv \Big(x?\tilde{z}.\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big] \\ &\equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\Big)\big[\tilde{y} \mapsto \tilde{v'}\big].\end{aligned}$$

Assume that $\Gamma(x)$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}/U$ with $l' \not\leq_L l$. Then $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \mathrm{Er}^{L,l}_{\Gamma,\tilde{z}:\tilde{\tau'}}(P'[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv \mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},\tilde{z}:\tilde{\tau'}}(P')$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma,\tilde{z}:\tilde{\tau'}}(P'[\tilde{y} \mapsto \tilde{v}]) \equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},\tilde{z}:\tilde{\tau'}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]$.

In case that $\Gamma(x)$ is not the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}/U$ for any $l'$, we can show $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]$ in the similar way to the case that $\Gamma(x)$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}/U$ with $l' \not\leq_L l$.

Case 7. Assume $P \equiv (\nu x : \xi)P'$. We consider cases according to the form of $\xi$.

Assume that $\xi$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}$ with $l' \leq_L l$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv (\nu x : \xi)\mathrm{Er}^{L,l}_{\Gamma,x:\xi/\mathsf{0}}(P'[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv (\nu x : \xi)\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},x:\xi/\mathsf{0}}(P')$. By the induction hypothesis, we have $\mathrm{Er}^{L,l}_{\Gamma,x:\xi/\mathsf{0}}(P'[\tilde{y} \mapsto \tilde{v}]) \equiv \Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},x:\xi/\mathsf{0}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]$. Then, we have

$$\begin{aligned}\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) &\equiv (\nu x : \xi)\mathrm{Er}^{L,l}_{\Gamma,x:\xi/\mathsf{0}}(P'[\tilde{y} \mapsto \tilde{v}]) \\ &\equiv (\nu x : \xi)\Big(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},x:\xi/\mathsf{0}}(P')\Big)\big[\tilde{y} \mapsto \tilde{v'}\big]\end{aligned}$$

$$\equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)[\tilde{y} \mapsto \tilde{v'}].$$

Assume that $\xi$ is not the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}$ with $l' \leq_L l$. Then $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P'[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv \mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},x:\xi/0}(P')$. By the induction hypothesis, we have

$$\mathrm{Er}^{L,l}_{\Gamma,x:\xi/0}(P'[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau},x:\xi/0}(P')\right)[\tilde{y} \mapsto \tilde{v'}].$$

Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)[\tilde{y} \mapsto \tilde{v'}]$.

Case 8. Assume $P \equiv \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)P'$. Let $L' = \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)L$ We consider cases according to $l$.

Assume $l' \leq_L l$ for any $l' \in \tilde{l_1}, \tilde{l_2}$. In this case, $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)\mathrm{Er}^{L',l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv \left(\tilde{l_1} < \nu l_0 < \tilde{l_2}\right)\mathrm{Er}^{L',l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')$. By the induction hypothesis, we have $\mathrm{Er}^{L',l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L',l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\right)[\tilde{y} \mapsto \tilde{v'}]$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)[\tilde{y} \mapsto \tilde{v'}]$.

Assume $l' \not\leq_L l$ for some $l' \in \tilde{l_1}, \tilde{l_2}$. In this case, $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \mathrm{Er}^{L',l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv \mathrm{Er}^{L',l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')$. By the induction hypothesis, we have $\mathrm{Er}^{L',l}_{\Gamma}(P'[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L',l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P')\right)[\tilde{y} \mapsto \tilde{v'}]$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)[\tilde{y} \mapsto \tilde{v'}]$.

Case 9. Assume $P \equiv \mathtt{if}\ w\ \mathtt{then}\ P_0\ \mathtt{else}\ P_1$. Let $\tilde{w'} \equiv \tilde{w}[\tilde{y} \mapsto \tilde{v'}]$. We consider cases according to the form of $\Gamma(w)$.

Assume that $\Gamma(w)$ is the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}/U$ with $l' \leq_L l$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \mathtt{if}\ w'\ \mathtt{then}\ \mathrm{Er}^{L,l}_{\Gamma}(P_0[\tilde{y} \mapsto \tilde{v}])\ \mathtt{else}\ \mathrm{Er}^{L,l}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}])$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv \mathtt{if}\ w\ \mathtt{then}\ \mathrm{Er}^{L,l}_{\Gamma}(P_0)\ \mathtt{else}\ \mathrm{Er}^{L,l}_{\Gamma}(P_1)$. By the induction hypothesis, we have $\mathrm{Er}^{(\tilde{l_1}<\nu l_0<\tilde{l_2})L,l}_{\Gamma}(P_i[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_i)\right)[\tilde{y} \mapsto \tilde{v'}]$ for $i = 0, 1$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)[\tilde{y} \mapsto \tilde{v'}]$.

Assume that $\Gamma(w)$ is not the form $\langle \tau_1, \ldots, \tau_n \rangle^{l'}/U$ with $l' \leq_L l$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \mathtt{0}$ and $\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P) \equiv \mathtt{0}$. Then, we have $\mathrm{Er}^{L,l}_{\Gamma}(P[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,l}_{\Gamma,\tilde{y}:\tilde{\tau}}(P)\right)[\tilde{y} \mapsto \tilde{v'}]$. □

**Lemma F.19.** *(1) If $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, and $(P, L) \longrightarrow^{\Gamma}_{\hat{l}} \left(\hat{P}, \hat{L}\right)$, then $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \preceq \mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$.*

*(2) If $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, and $(P, L) \not\longrightarrow^{\Gamma}_{\hat{l}} \left(\hat{P}, \hat{L}\right)$ but $(P, L) \longrightarrow \left(\hat{P}, \hat{L}\right)$, then, for any $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P)$-sublattice $L'$ of $L$, there exists a lattice for secrecy levels $\hat{L}'$ such that $\left(\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P), L'\right) \longrightarrow \left(\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right), \hat{L}'\right)$ and $\hat{L}'$ is an $\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$-sublattice of $\hat{L}$.*

*Proof.* We show each statements

(1) Assume that $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, and $(P, L) \longrightarrow^{\Gamma}_{\hat{l}} \left(\hat{P}, \hat{L}\right)$. By induction on the construction of $(P, L) \longrightarrow \left(\hat{P}, \hat{L}\right)$, we prove $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \preceq \mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$. We consider cases according to the last rule of the construction of $(P, L) \longrightarrow^{\Gamma}_{\hat{l}} \left(\hat{P}, \hat{L}\right)$.

Case (1). In this case, $P \equiv x!\tilde{v}.P_0 \mid x?\tilde{y}.P_1$ and $\hat{P} \equiv P_0 \mid P_1[\tilde{y} \mapsto \tilde{v}]$ with $\tilde{y} = (y_0, \ldots, y_n)$ and $\tilde{v} = (v_0, \ldots, v_n)$. We also have $\hat{L} = L$. Then $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(x!\tilde{v}.P_0) \mid \mathrm{Er}^{L,\hat{l}}_{\Gamma}(x?\tilde{y}.P_1)$ and $\mathrm{Er}^{L,\hat{l}}_{\Gamma}\left(\hat{P}\right) \equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}])$. By Lemma D.1, $\Gamma(x)$ is the form $\langle \tau_0, \ldots, \tau_n \rangle^{l'}/U$, where $\tau_i \sim \Gamma(v_i)$ for $i = 0, \ldots, n$. Since $(P, L) \longrightarrow^{\Gamma}_{\hat{l}} \left(\hat{P}, \hat{L}\right)$, we have $l' \not\leq_L \hat{l}$. Then, we see $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,\hat{l}}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_1)$ and $\mathrm{Er}^{L,\hat{l}}_{\Gamma}\left(\hat{P}\right) \equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}])$. By Theorem F.18, we have

$$\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,\hat{l}}_{\Gamma,y_0:\Gamma(v_n),\ldots,y_n:\Gamma(v_n)}(P_1)\right)[\tilde{y} \mapsto \tilde{v'}].$$

Because $\Gamma \parallel L$ is secure, $l' \leq_L l''$ for any secrecy type $l''$ occurring in $\tau_i$ with $i = 0, 1, \ldots$. Hence, $\tau_i$ is not lower than $\hat{l}$ for any $i = 0, \ldots, n$. Therefore, $\Gamma(v_i)$ is not lower than $\hat{l}$ for any $i = 0, \ldots, n$. By Lemma F.12, $y_i$ does not occur in $\mathrm{Er}^{L,\hat{l}}_{\Gamma,y_0:\Gamma(v_n),\ldots,y_n:\Gamma(v_n)}(P_1)$ for any $i = 0, \ldots, n$. Hence,

$$\left(\mathrm{Er}^{L,\hat{l}}_{\Gamma,y_0:\Gamma(v_n),\ldots,y_n:\Gamma(v_n)}(P_1)\right)[\tilde{y} \mapsto \tilde{v'}] \equiv \left(\mathrm{Er}^{L,\hat{l}}_{\Gamma,y_0:\Gamma(v_n),\ldots,y_n:\Gamma(v_n)}(P_1)\right).$$

By Lemma F.13, we have $\left(\mathrm{Er}^{L,\hat{l}}_{\Gamma,y_0:\Gamma(v_n),\ldots,y_n:\Gamma(v_n)}(P_1)\right) \equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_1)$. Thus, $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \preceq \mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$. Then $L'$ is an $\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$-sublattice of $\hat{L}$.

Case (2). Let $\tilde{l_0}$, $\tilde{l_1} \subseteq L$. Let $P \equiv \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)P'$. Assume that $\left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)L$ is defined. Then $\hat{P} \equiv P'$ and $\hat{L} = \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)L$. Since $(P, L) \longrightarrow^{\Gamma}_{\hat{l}} \left(\hat{P}, \hat{L}\right)$, we have $l' \not\leq_L \hat{l}$ for some $l' \in \tilde{l_0}, \tilde{l_1}$. Then $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \equiv \mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$. Hence, $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \preceq \mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$, and $L'$ is an $\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$-sublattice of $\hat{L}$.

Case (3). Straightforward.

Case (4). Straightforward.

Case (5). Straightforward.

(2) Assume that $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, and $(P, L) \not\longrightarrow^{\Gamma}_{\hat{l}} \left(\hat{P}, \hat{L}\right)$ but $(P, L) \longrightarrow \left(\hat{P}, \hat{L}\right)$. Let $L'$ be an $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P)$-sublattice of $L$. By induction on the construction of $(P, L) \longrightarrow \left(\hat{P}, \hat{L}\right)$, we prove that there exists a lattice for secrecy levels $\hat{L}'$ such that $\left(\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P), L'\right) \longrightarrow \left(\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right), \hat{L}'\right)$ and $\hat{L}'$ is an $\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$-sublattice of $\hat{L}$. We consider cases according to the last rule of the construction of $(P, L) \longrightarrow \left(\hat{P}, \hat{L}\right)$.

Case 1. (R-Com). In this case, $P \equiv x!\tilde{v}.P_0 \mid x?\tilde{y}.P_1$ and $\hat{P} \equiv P_0 \mid P_1[\tilde{y} \mapsto \tilde{v}]$ with $\tilde{y} = (y_0, \ldots, y_n)$ and $\tilde{v} = (v_0, \ldots, v_n)$. We also have $\hat{L} = L$. Then $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(x!\tilde{v}.P_0) \mid \mathrm{Er}^{L,\hat{l}}_{\Gamma}(x?\tilde{y}.P_1)$ and $\mathrm{Er}^{L,\hat{l}}_{\Gamma}\left(\hat{P}\right) \equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}])$. By Lemma D.1, $\Gamma(x)$ is the form $\langle \tau_0, \ldots, \tau_n \rangle^{l'}/U$, where $\tau_i \sim \Gamma(v_i)$ for $i = 0, \ldots, n$. We consider cases according to $l'$. Since $(P, L) \not\longrightarrow^{\Gamma}_{\hat{l}} \left(\hat{P}, \hat{L}\right)$, we have $l' \leq_L \hat{l}$. Let $v'_i \equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(v_i)$ for all $i = 0, \ldots, n$. Let $\tilde{v'} = (v'_0, \ldots, v'_n)$, and $\tilde{\tau} = \langle \tau_0, \ldots, \tau_n \rangle$. Then, we have $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \equiv x!\tilde{v'}.\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_0) \mid x?\tilde{y}.\mathrm{Er}^{L,\hat{l}}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_1)$ and $\mathrm{Er}^{L,\hat{l}}_{\Gamma}\left(\hat{P}\right) \equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}])$. By Theorem F.18, we have

$$\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,\hat{l}}_{\Gamma,y_0:\Gamma(v_n),\ldots,y_n:\Gamma(v_n)}(P_1)\right)[\tilde{y} \mapsto \tilde{v'}].$$

By Lemma F.13, $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}]) \equiv \left(\mathrm{Er}^{L,\hat{l}}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_1)\right)[\tilde{y} \mapsto \tilde{v'}]$. Hence, we have $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \equiv x!\tilde{v'}.\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_0) \mid x?\tilde{y}.\mathrm{Er}^{L,\hat{l}}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_1)$ and

$$\begin{aligned}\mathrm{Er}^{L,\hat{l}}_{\Gamma}\left(\hat{P}\right) &\equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_0) \mid \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_1[\tilde{y} \mapsto \tilde{v}]) \\ &\equiv \mathrm{Er}^{L,\hat{l}}_{\Gamma}(P_0) \mid \left(\mathrm{Er}^{L,\hat{l}}_{\Gamma,\tilde{y}:\tilde{\tau}}(P_1)\right)[\tilde{y} \mapsto \tilde{v'}].\end{aligned}$$

Therefore, we have $\left(\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P), L'\right) \longrightarrow \left(\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right), L'\right)$ for any lattice for secrecy levels $L'$, where $L'$ is an $\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$-sublattice of $L$.

Case 2. (R-NewLev). Let $\tilde{l_0}$, $\tilde{l_1} \subseteq L$. Let $P \equiv \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)P'$. Assume that $\left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)L$ is defined. Then $\hat{P} \equiv P'$ and $\hat{L} = \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)L$. Since $(P, L) \not\longrightarrow^{\Gamma}_{\hat{l}} \left(\hat{P}, \hat{L}\right)$, we have $l' \leq_L \hat{l}$ for any $l' \in \tilde{l_0}, \tilde{l_1}$. Then $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P) \equiv \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$. Let $L'$ be an $\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P)$-sublattice of $L$. Then $\left(\mathrm{Er}^{L,\hat{l}}_{\Gamma}(P), L'\right) \longrightarrow \left(\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right), \left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)L'\right)$. Then $\left(\tilde{l_0} < \nu l' < \tilde{l_1}\right)L'$ is an $\mathrm{Er}^{\hat{L},\hat{l}}_{\Gamma}\left(\hat{P}\right)$-sublattice of $\hat{L}$.

Case 3. (R-Par). Straightforward.

Case 4. (R-New). Straightforward.

Case 5. (R-SP). Straightforward. □

## F.5. $P$ can simulate $\mathrm{Er}^{L,l}_{\Gamma}(P)$

**Lemma F.20.** *For a reliable type environment $\Gamma$, if $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, $P' \preceq \mathrm{Er}^{L,k}_{\Gamma}(P)$ and $P' \preceq \bar{P}'$, then there exist $\bar{P}$, $\bar{L}$ and $\bar{\Gamma}$ such that $(P, L) \longrightarrow\!\!\!\!\!\rightarrow (\bar{P}, \bar{L})$, $\Gamma \longrightarrow\!\!\!\!\!\rightarrow \bar{\Gamma}$ and $\bar{P}' \preceq \mathrm{Er}^{\bar{L},k}_{\bar{\Gamma}}(\bar{P})$.*

*Proof.* Assume that $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, $P' \preceq \mathrm{Er}^{L,k}_{\Gamma}(P)$ and $P' \preceq \bar{P}'$. By induction on the construction of $P' \preceq \bar{P}'$, we show that there exist $\bar{P}$, $\bar{L}$, and $\bar{\Gamma}$ such that $(P, L) \longrightarrow\!\!\!\!\!\rightarrow (\bar{P}, \bar{L})$, $\Gamma \longrightarrow\!\!\!\!\!\rightarrow \bar{\Gamma}$ and $\bar{P}' \preceq \mathrm{Er}^{\bar{L},k}_{\bar{\Gamma}}(\bar{P})$. We consider cases according to the last rule of the construction of $P' \preceq \bar{P}'$.

Case 1. Assume $\bar{P}' \equiv P'$. Let $\bar{P} \equiv P$, $\bar{L} \equiv L$ and $\bar{\Gamma} \equiv \Gamma$. Then, we have the claimed result.

Case 2. Assume tbar there exists a process $P_0$ such that $P' \preceq P_0$ and $P_0 \preceq \bar{P}'$. By the induction hypothesis, we see tbar there exist $\bar{P}_0$, $\bar{L}_0$ and $\bar{\Gamma}_0$ such tbar $(P, L) \longrightarrow\!\!\!\!\!\rightarrow (\bar{P}_0, \bar{L}_0)$, $\Gamma \longrightarrow\!\!\!\!\!\rightarrow \bar{\Gamma}_0$ and $P_0 \preceq \mathrm{Er}_{\bar{\Gamma}_0}^{\bar{L}_0,k}(\bar{P}_0)$. By $P_0 \preceq \mathrm{Er}_{\bar{\Gamma}_0}^{\bar{L}_0,k}(\bar{P}_0)$ and the induction hypothesis, we see tbar there exist $\bar{P}$, $\bar{L}$ and $\bar{\Gamma}$ such that $(\bar{P}_0, \bar{L}_0) \longrightarrow\!\!\!\!\!\rightarrow (\bar{P}, \bar{L})$, $\bar{\Gamma}_0 \longrightarrow\!\!\!\!\!\rightarrow \bar{\Gamma}$ and $\bar{P}' \preceq \mathrm{Er}_{\bar{\Gamma}}^{\bar{L},k}(\bar{P})$. Therefore, we have $(P, L) \longrightarrow\!\!\!\!\!\rightarrow (\bar{P}, \bar{L})$, $\Gamma \longrightarrow\!\!\!\!\!\rightarrow \bar{\Gamma}$ and $\bar{P}' \preceq \mathrm{Er}_{\Gamma}^{\bar{L},k}(\bar{P})$.

Case 3. (SP-Zero1). Straightforward.

Case 4. (SP-Zero2). Straightforward.

Case 5. (SP-Commut). Straightforward.

Case 6. (SP-Assoc). Straightforward.

Case 7. (SP-New). Straightforward.

Case 8. (SP-IfT). Let $P' \equiv \mathtt{if}\,\mathrm{true}^{l'}\,\mathtt{then}\,Q_0\,\mathtt{else}\,Q_1$ and $\bar{P}' \equiv Q_0$. Then, we have either $\mathrm{Er}_{\Gamma}^{L,k}(P) \equiv P'$ or $Q_0 \preceq \mathrm{Er}_{\Gamma}^{L,k}(P)$.

Assume $\mathrm{Er}_{\Gamma}^{L,k}(P) \equiv P'$. Then $l' \leq_L k$. By Definition F.9, $P \equiv C[P']$ for some finite level context, where $\Gamma(x) = \langle\tilde{\tau}\rangle^{l'}/U$ implies $l' \not\leq_L k$ for all $x \in \mathrm{FN}(C)$ and, for all occurrence $(\nu x : \xi)$- in $C$, the type of $\xi$ is not less than $k$ in $L$. From Lemma 4.13, there exists an evaluation context $E$ and a lattice for secrecy levels $\hat{L}$ such that $(C, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma} \left(E, \hat{L}\right)$. Hence, $(C[P'], L) \longrightarrow\!\!\!\!\!\rightarrow \left(E[P'], \hat{L}\right)$ and $(C[Q_0], L) \longrightarrow\!\!\!\!\!\rightarrow \left(E[Q_0], \hat{L}\right)$. Since $E[P'] \preceq E[Q_0]$, we have $(C[P'], L) \longrightarrow\!\!\!\!\!\rightarrow \left(E[Q_0], \hat{L}\right)$. We see $\mathrm{Er}_{\Gamma}^{\hat{L},k}(E[Q_0]) \equiv Q_0$. Let $\bar{P} \equiv E[Q_0]$, $\bar{L} \equiv \hat{L}$, $\bar{\Gamma} \equiv \Gamma$. Then, we have the claimed result.

Assume $Q_0 \preceq \mathrm{Er}_{\Gamma}^{L,k}(P)$. Then $\bar{P}' \preceq \mathrm{Er}_{\Gamma}^{L,k}(P)$. Let $\bar{P} \equiv P$, $\bar{L} \equiv L$ and $\bar{\Gamma} \equiv \Gamma$. Then, we have the claimed result.

Case 9. (SP-IfF). In the similar way to the case (SP-IfT).

Case 10. (SP-Rep). Straightforward.

Case 11. (SP-Par). Straightforward.

Case 12. (SP-CNew). Straightforward. □

**Lemma F.21.** *For type environments $\Gamma$, $\Delta$, lattices for secrecy levels $L$, $L'$ and a $k$-$(\Gamma \parallel L, m)$-$(\Delta \parallel L', m')$-context $C$, if $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, then $\mathrm{Er}_{\Delta}^{L',m'}(C[P]) \equiv \mathrm{Er}_{\Delta}^{L',m'}(C)\left[\mathrm{Er}_{\Gamma}^{L,m}(P)\right]$.*

*Proof.* By induction on $k$-secure derivation tree of $\Delta \parallel L' \rhd_{m'} C$ from $\Gamma \parallel L \rhd_m [\,]$. □

**Lemma F.22.** *For a reliable type environment $\Gamma$, if $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, $P' \preceq \mathrm{Er}_{\Gamma}^{L,k}(P)$, $L'$ is an $\mathrm{Er}_{\Gamma}^{L,k}(P)$-sublattice of $L$, and $(P', L') \longrightarrow (\bar{P}', \bar{L}')$, then there exist $\bar{P}$ and $\bar{L}$ such that $(P, L) \longrightarrow\!\!\!\!\!\rightarrow (\bar{P}, \bar{L})$, and $\bar{P}' \preceq \mathrm{Er}_{\Gamma}^{\bar{L},k}(\bar{P})$, $\bar{L}'$ is an $\mathrm{Er}_{\Gamma}^{\bar{L},k}(P)$-sublattice of $\bar{L}$.*

*Proof.* Assume that $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, $P' \preceq \mathrm{Er}_{\Gamma}^{L,\hat{l}}(P)$, $L'$ is an $\mathrm{Er}_{\Gamma}^{\hat{L},\hat{l}}(P)$-sublattice of $L$, and $(P', L') \longrightarrow (\bar{P}', \bar{L}')$. By Theorem A.6, either

(1) $P' \preceq \left(\nu\tilde{x} : \tilde{\xi}\right) z!\tilde{v}.P_0' \mid z?\tilde{y}.P_1' \mid P_2'$, $\left(\nu\tilde{x} : \tilde{\xi}\right) P_0' \mid P_1'[\tilde{y} \mapsto \tilde{v}] \mid P_2' \preceq \bar{P}'$ and $\bar{L}' = L'$, or

(2) $P' \preceq \left(\nu\tilde{x} : \tilde{\xi}\right)\left(\tilde{l_0} < \nu l < \tilde{l_1}\right) P_0' \mid P_1'$, $\left(\nu\tilde{x} : \tilde{\xi}\right) P_0' \mid P_1' \preceq \bar{P}'$ and $\bar{L}' = \left(\tilde{l_0} < \nu l < \tilde{l_1}\right) L'$.

We consider the case (1). By Lemma F.20, there exist $\bar{P}_0$, $\bar{L}_0$ and $\bar{\Gamma}_0$ such that $(P, L) \longrightarrow\!\!\!\!\!\rightarrow (\bar{P}_0, \bar{L}_0)$, $\Gamma \longrightarrow\!\!\!\!\!\rightarrow \bar{\Gamma}_0$ and $\left(\nu\tilde{x} : \tilde{\xi}\right) z!\tilde{v}.P_0' \mid z?\tilde{y}.P_1' \mid P_2' \preceq \mathrm{Er}_{\bar{\Gamma}_0}^{\bar{L}_0,k}(\bar{P}_0)$, and $\bar{\Gamma}_0 \parallel L \rhd_m \bar{P}_0$ is $k$-securely derivable. Then, there exists an evaluation context with two holes $E$ such that $\mathrm{Er}_{\bar{\Gamma}_0}^{\bar{L}_0,k}(\bar{P}_0) \equiv E\,[z!\tilde{v}.P_0']^{(1)}[z?\tilde{y}.P_1']^{(2)}$ and $\left(\nu\tilde{x} : \tilde{\xi}\right)[\,]^{(1)} \mid [\,]^{(2)} \mid P_2' \preceq E$. Since $\bar{\Gamma}_0 \parallel L \rhd_m \bar{P}_0$ is $k$-securely derivable, there exists a finite level context with two holes $C$, process $P_0$, $P_1$ and type environments $\Delta_0$, $\Delta_1$ such that $\bar{P}_0 \equiv C\,[z!\tilde{v}.P_0]^{(1)}[z?\tilde{y}.P_1]^{(2)}$, $\mathrm{Er}_{\bar{\Gamma}_0}^{\bar{L}_0,k}(C) \equiv E$, $\mathrm{Er}_{\Delta_0}^{\bar{L}_0,k}(P_0) \equiv z!\tilde{v}.P_0'$, $\mathrm{Er}_{\Delta_1}^{\bar{L}_0,k}(P_0) \equiv z?\tilde{y}.P_1'$, and $\bar{\Gamma}_0 \parallel L \rhd_m C$ is $k$-securely derivable from $\Delta_0 \parallel L_1' \rhd_{l_0'} [\,]^{(1)}$ and $\Delta_1 \parallel L_1' \rhd_{l_1'} [\,]^{(2)}$, where $l_i' \geq m$ for $i = 0, 1$. By Lemma 4.13, there exists an evaluation context $\bar{E}$ and a lattice for secrecy levels $\bar{L}$ such that $(C, L) \longrightarrow\!\!\!\!\!\rightarrow_k^{\Gamma} (\bar{E}, \bar{L})$. Hence, $(\bar{P}_0, \bar{L}_0) \longrightarrow\!\!\!\!\!\rightarrow \left(\bar{E}\,[P_0]^{(1)}[P_1[\tilde{y} \mapsto \tilde{v}]]^{(2)}, \bar{L}\right)$. By Lemma F.19, we have $\left(\nu\tilde{x} : \tilde{\xi}\right)[P_0']^{(1)} \mid [P_1'[\tilde{y} \mapsto \tilde{v}]]^{(2)} \mid P_2' \preceq E\,[P_0']^{(1)}[P_1'[\tilde{y} \mapsto \tilde{v}]]^{(2)} \equiv \mathrm{Er}_{\bar{\Gamma}_0}^{\bar{L}_0,k}(C)\,[P_0']^{(1)}[P_1'[\tilde{y} \mapsto \tilde{v}]]^{(2)} \preceq \mathrm{Er}_{\bar{\Gamma}_0}^{\bar{L}_0,k}(\bar{E})\,[P_0']^{(1)}[P_1'[\tilde{y} \mapsto \tilde{v}]]^{(2)}$. By Lemma F.20, there exist $\bar{P}$, $\bar{L}$, such that $(\bar{P}_0, \bar{L}_0) \longrightarrow\!\!\!\!\!\rightarrow (\bar{P}, \bar{L})$, and $\left(\nu\tilde{x} : \tilde{\xi}\right) P_0' \mid P_1'[\tilde{y} \mapsto \tilde{v}] \mid P_2' \preceq \mathrm{Er}_{\bar{\Gamma}_0}^{\bar{L}_0,k}(\bar{P})$. Therefore, $(P, L) \longrightarrow\!\!\!\!\!\rightarrow (\bar{P}, \bar{L})$.

The case (2) is obvious. □

**Lemma F.23.** *Define*

$$\mathcal{R} = \left\{ ((P,L),(P',L')) \;\middle|\; \begin{array}{c} \Gamma \parallel L \rhd_m P \text{ is } k\text{-securely derivable} \\ \text{for a reliable type environment } \Gamma, \\ P' \preceq \mathrm{Er}_\Gamma^{L,k}(P), \text{ and} \\ L' \text{ is an } \mathrm{Er}_\Gamma^{L,\hat{l}}(P)\text{-sublattice of } L. \end{array} \right\}.$$

*$\mathcal{R}$ is a barbed bisimulation.*

*Proof.* It suffices to show that $\mathcal{R}$ satisfies all the conditions of Definition 4.15.

Assume $((P,L),(P',L')) \in R$. Then, we see that $\Gamma \parallel L \rhd_m P$ is derivable for a reliable type environment $\Gamma$, the secrecy level of $\Gamma \parallel L$ is $l_1$, and $P' \preceq \mathrm{Er}_\Gamma^{L,\hat{l}}(P)$.

(1) Assume $(P,L) \longrightarrow \left(\hat{P},\hat{L}\right)$. By Proposition 4.5, there exists a type environment $\hat{\Gamma}$ such that either $\hat{\Gamma} \equiv \Gamma$ or $\Gamma \longrightarrow \hat{\Gamma}$ and $\hat{\Gamma} \parallel \hat{L} \rhd_m \hat{P}$ is derivable. By Lemma F.19, either $\mathrm{Er}_\Gamma^{L,\hat{l}}(P) \preceq \mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right)$ and $L'$ is an $\mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right)$-sublattice of $\hat{L}$, or there exists a lattice for secrecy levels $\hat{L}'$ such that $\left(\mathrm{Er}_\Gamma^{L,\hat{l}}(P),L'\right) \longrightarrow \left(\mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right),\hat{L}'\right)$ and $\hat{L}'$ is an $\mathrm{Er}_\Gamma^{\hat{L},\hat{l}}(P)$-sublattice of $\hat{L}$.

Assume $\mathrm{Er}_\Gamma^{L,\hat{l}}(P) \preceq \mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right)$. Since $P' \preceq \mathrm{Er}_\Gamma^{L,\hat{l}}(P)$, we have $P' \preceq \mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right)$. Hence, $(P',L') \longrightarrow\!\!\!\!\!\rightarrow \left(\mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right),L'\right)$. By Lemma F.13, we have $\mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right) \equiv \mathrm{Er}_{\hat{\Gamma}}^{\hat{L},\hat{l}}\left(\hat{P}\right)$. Since $L'$ is an $\mathrm{Er}_{\hat{\Gamma}}^{\hat{L},\hat{l}}\left(\hat{P}\right)$-sublattice of $\hat{L}$, we have $\left(\left(\hat{P},\hat{L}\right),\left(\mathrm{Er}_{\hat{\Gamma}}^{\hat{L},\hat{l}}\left(\hat{P}\right),L'\right)\right) \in R$.

Assume $\mathrm{Er}_\Gamma^{L,\hat{l}}(P) \not\preceq \mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right)$. Then, there exists a lattice for secrecy levels $\hat{L}'$ such that $\left(\mathrm{Er}_\Gamma^{L,\hat{l}}(P),L'\right) \longrightarrow \left(\mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right),\hat{L}'\right)$ and $\hat{L}'$ is an $\mathrm{Er}_\Gamma^{\hat{L},\hat{l}}(P)$-sublattice of $\hat{L}$. Since $P' \preceq \mathrm{Er}_\Gamma^{L,\hat{l}}(P)$, we have $(P',L') \longrightarrow \left(\mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right),\hat{L}'\right)$. By Lemma F.13, we have $\mathrm{Er}_\Gamma^{\hat{L},\hat{l}}\left(\hat{P}\right) \equiv \mathrm{Er}_{\hat{\Gamma}}^{\hat{L},\hat{l}}\left(\hat{P}\right)$. Hence, $(P',L') \longrightarrow\!\!\!\!\!\rightarrow \left(\mathrm{Er}_{\hat{\Gamma}}^{\hat{L},\hat{l}}\left(\hat{P}\right),L'\right)$. We also have $\left(\left(\hat{P},\hat{L}\right),\left(\mathrm{Er}_{\hat{\Gamma}}^{\hat{L},\hat{l}}\left(\hat{P}\right),\hat{L}'\right)\right) \in R$.

(2) By Lemma F.22.

(3) Straightforward. □

**Lemma F.24.** *For a reliable type environment $\Gamma$, a lattice for secrecy levels $L$ and a process $P$, if $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, then $(P,L) \mathrel{\dot{\approx}} \left(\mathrm{Er}_\Gamma^{L,l}(P),L\right)$.*

*Proof.* Assume that $\Gamma \parallel L \rhd_m P$ is $k$-securely derivable, where $m \not\leq_L l$. By Lemma F.23, we have $(P,L) \mathrel{\dot{\approx}} \left(\mathrm{Er}_\Gamma^{L,l}(P),L\right)$. □

**Definition F.25.** We write $\mathbf{lower}_L^l(\Gamma)$ for the type environment obtained from a type environment $\Gamma$ by replacing all the secrecy annotations $l' \not\leq_L l$ with the infimum of $\{l,l'\}$ and all the capability level annotations with $\infty$.

We also write $\mathbf{lower}_L^l(C)$ for the context obtained from a context $C$ by replacing every secrecy annotation $l' \not\leq_L l$ in a type or a constant value with the infimum of $\{l,l'\}$.

We note that, for a closed type environment $\Gamma$, $\mathbf{lower}_L^l(\Gamma)$ is a reliable type environment whose secrecy level is $l$.

**Lemma F.26.** *For type environments $\Gamma$, $\Delta$, lattices for secrecy levels $L$, $L'$ and a $(\Gamma \parallel L,m)$-$(\Delta \parallel L',m')$-context $C$, if the secrecy level of $\Gamma \parallel L$ is $l_0$, then $\mathbf{lower}_{L'}^{l_0}(C)$ is a $k$-$(\Gamma \parallel L,m)$-$\left(\mathbf{lower}_{L'}^{l_0}(\Delta) \parallel L',\hat{m}\right)$-context, where $\hat{m}$ is the infimum of $\{l_0,l'\}$ in $L'$.*

*Proof.* Straightforward. □

**Lemma F.27.** *For a type environment $\Gamma$, a lattice for secrecy levels $L$, a process $P$, and secrecy levels $m$, $l_1$, if $\Gamma \parallel L \rhd_m P\left[x \mapsto \mathrm{true}^{l_1}\right]$ is $k$-securely derivable, then $\Gamma \parallel L \rhd_m P\left[x \mapsto \mathrm{false}^{l_1}\right]$ is $k$-securely derivable.*

*Proof.* By induction on derivation tree of $\Gamma \parallel L \rhd_m P\left[x \mapsto \mathrm{true}^{l_1}\right]$. □

**Lemma F.28.** *For a type environment $\Gamma$, a lattice for secrecy levels $L$, a process $P$, and secrecy levels $l_0$, $l_1$, if $\Gamma \parallel L \rhd_m P\left[x \mapsto \mathrm{true}^{l_1}\right]$ is $k$-securely derivable, then $\mathrm{Er}_\Gamma^{L,m}\left(P\left[x \mapsto \mathrm{true}^{l_1}\right]\right) \equiv \mathrm{Er}_\Gamma^{L,m}\left(P\left[x \mapsto \mathrm{false}^{l_1}\right]\right)$.*

*Proof.* By induction on the construction of $P$. □

**Lemma F.29.** *For type environments $\Gamma$ and $\Delta$, lattices for secrecy levels $L$, processes $P$, $Q$, $(\Gamma \parallel L, m)$-$(\Delta \parallel L', m')$-context $C$, if $\Delta$ is closed and $\left(\mathbf{lower}^{l''}_{L'}(C)[P], L\right) \overset{\bullet}{\approx} \left(\mathbf{lower}^{l''}_{L'}(C)[Q], L\right)$, then $(C[P], L) \overset{\bullet}{\approx} (C[Q], L)$.*

*Proof.* Straightforward. □

## F.6. Proof of Theorem 4.18

For a type environment $\Gamma$, a lattice for secrecy levels $L$, a process $P$, and secrecy levels $l$, $l'$, Assume that $l' \not\leq_L l$, the secrecy level of $\Gamma \parallel L$ is $l$ and $\Gamma \parallel L \rhd_m P\left[x \mapsto \mathrm{true}^{l'}\right]$ is $k$-securely derivable. We show $P\left[x \mapsto \mathrm{true}^{l'}\right] \underset{(\Gamma \parallel L, m)}{\approx} P\left[x \mapsto \mathrm{false}^{l'}\right]$. By Theorem F.27, we see that $\Gamma \parallel L \rhd_m P\left[x \mapsto \mathrm{false}^{l'}\right]$ is $k$-securely derivable. Then, it suffices to show that, for any closed $\Delta$, a lattice for secrecy levels $L'$, and a secrecy level $m'$, $\left(C\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right], L'\right) \overset{\bullet}{\approx} \left(C\left[P\left[x \mapsto \mathrm{false}^{l'}\right], L'\right]\right)$ with any $(\Gamma \parallel L, l)$-$(\Delta \parallel L', m')$-context $C$.

Let $\Delta$ be a closed type environment, and $C$ be a $(\Gamma \parallel L, m)$-$(\Delta \parallel L', m')$-context. Then $\mathbf{lower}^l_L(\Delta)$ is a reliable type environment whose secrecy level is $l$. Let $C' \equiv \mathbf{lower}^l_L(C)$.

By Theorem F.26, $C'$ is a $(\Gamma \parallel L, m)$-$\left(\mathbf{lower}^l_L(\Delta) \parallel L, l\right)$-context. From Theorem F.24, we have

$$\left(C'\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right], L\right) \overset{\bullet}{\approx} \left(\mathrm{Er}^{L,l}_{\mathbf{lower}^l_L(\Delta)}\left(C'\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right]\right), L\right) \text{ and}$$
$$\left(C'\left[P\left[x \mapsto \mathrm{false}^{l'}\right]\right], L\right) \overset{\bullet}{\approx} \left(\mathrm{Er}^{L,l}_{\mathbf{lower}^l_L(\Delta)}\left(C'\left[P\left[x \mapsto \mathrm{false}^{l'}\right]\right]\right), L\right).$$

Theorem F.21 implies

$$\mathrm{Er}^{L',l}_{\mathbf{lower}^l_{L'}(\Delta)}\left(C'\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right]\right) \equiv \mathrm{Er}^{L',l}_{\mathbf{lower}^l_{L'}(\Delta)}(C')\left[\mathrm{Er}^{L,m}_{\Gamma}\left(P\left[x \mapsto \mathrm{true}^{l'}\right]\right)\right].$$

Since $\Gamma \parallel L \rhd_m P\left[x \mapsto \mathrm{true}^{l'}\right]$ and $\Gamma \parallel L \rhd_m P\left[x \mapsto \mathrm{false}^{l'}\right]$ are derivable, Theorem F.28 implies

$$\mathrm{Er}^{L,m}_{\Gamma}\left(P\left[x \mapsto \mathrm{true}^{l'}\right]\right) \equiv \mathrm{Er}^{L,m}_{\Gamma}\left(P\left[x \mapsto \mathrm{false}^{l'}\right]\right).$$

Then, we have

$$\begin{aligned}
\mathrm{Er}^{L',l}_{\mathbf{lower}^l_{L'}(\Delta)}\left(C'\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right]\right) &\equiv \mathrm{Er}^{L',l}_{\mathbf{lower}^l_{L'}(\Delta)}(C')\left[\mathrm{Er}^{L,m}_{\Gamma}\left(P\left[x \mapsto \mathrm{true}^{l'}\right]\right)\right] \\
&\equiv \mathrm{Er}^{L',l}_{\mathbf{lower}^l_{L'}(\Delta)}(C')\left[\mathrm{Er}^{L,m}_{\Gamma}\left(P\left[x \mapsto \mathrm{false}^{l'}\right]\right)\right] \\
&\equiv \mathrm{Er}^{L',l}_{\mathbf{lower}^l_{L'}(\Delta)}\left(C'\left[P\left[x \mapsto \mathrm{false}^{l'}\right]\right]\right).
\end{aligned}$$

By Lemma F.2, we have

$$\left(C'\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right], L\right) \overset{\bullet}{\approx} \left(C'\left[P\left[x \mapsto \mathrm{false}^{l'}\right]\right], L\right).$$

Theorem F.29 implies

$$\left(C\left[P\left[x \mapsto \mathrm{true}^{l'}\right]\right], L\right) \overset{\bullet}{\approx} \left(C\left[P\left[x \mapsto \mathrm{false}^{l'}\right]\right], L\right).$$

□

## F.7. Proof of Theorem 4.19

For type environments $\Gamma$, $\Delta$, lattices for secrecy levels $L$, $L'$, processes $P_0$, $P_1$, and a $(\Delta \parallel L', m')$-$(\Gamma \parallel L, m)$-context $\hat{C}$, assume that $m'' \in L$ and $m' \not\leq_L m''$, the secrecy level of $\Gamma \parallel L$ is $m''$, and $\Delta \parallel L' \rhd_{m'} P_i$ is derivable for $i = 0, 1$. We show $\hat{C}[P_0] \underset{(\Gamma \parallel L, m)}{\approx} \hat{C}[P_1]$.

Since $\Delta \parallel L' \rhd_{m'} P_i$ is $k$-securely derivable for $i = 0, 1$, we see that $\Delta \parallel L' \rhd_{m'} \hat{C}[P_i]$ is $k$-securely derivable for $i = 0, 1$.

Let $\Pi$ be a closed type environment, and $C$ be $(\Gamma \parallel L, m)$-$(\Pi \parallel L', m''')$-context. Then $\mathbf{lower}^{m''}_{L'}(\Pi)$ is a reliable type environment whose secrecy level is $m''$. Let $C' \equiv \mathbf{lower}^{m''}_{L'}(C)$.

By Theorem F.26, $C'$ is a $(\Gamma \parallel L, m)$-$\left(\mathbf{lower}_{L'}^{m''}(\Pi) \parallel L', m''\right)$-context. From Theorem F.24, we have $\left(C'\left[\hat{C}[P_i]\right], L\right) \overset{\bullet}{\approx} \left(\mathrm{Er}^{L,m''}_{\mathbf{lower}_{L'}^{m''}(\Pi)}\left(C'\left[\hat{C}[P_i]\right]\right), L'\right)$ for $i = 0, 1$. Since $C'\left[\hat{C}\right]$ is a $(\Delta \parallel L', m')$-$\left(\mathbf{lower}_{L}^{m''}(\Pi) \parallel L', m''\right)$-context, Theorem F.21 implies

$$\mathrm{Er}^{L,m''}_{\mathbf{lower}_{L'}^{m''}(\Pi)}\left(C'\left[\hat{C}\right][P_i]\right) \equiv \mathrm{Er}^{L,m''}_{\mathbf{lower}_{L'}^{m''}(\Pi)}\left(C'\left[\hat{C}\right]\right)\left[\mathrm{Er}^{L',m'}_{\Delta}(P_i)\right].$$

for $i = 0, 1$. By Lemma F.7 and Theorem F.16, we have

$$\mathrm{Er}^{L,m''}_{\mathbf{lower}_{L'}^{m''}(\Pi)}\left(C'\left[\hat{C}\right]\right)\left[\mathrm{Er}^{L',m'}_{\Delta}(P_0)\right] \overset{\bullet}{\approx} \mathrm{Er}^{L,m''}_{\mathbf{lower}_{L'}^{m''}(\Pi)}\left(C'\left[\hat{C}\right]\right)[\mathsf{0}] \overset{\bullet}{\approx} \mathrm{Er}^{L,m''}_{\mathbf{lower}_{L'}^{m''}(\Pi)}\left(C'\left[\hat{C}\right]\right)\left[\mathrm{Er}^{L',m'}_{\Delta}(P_1)\right].$$

Hence, we have $\left(C'\left[\hat{C}[P_0]\right], L\right) \overset{\bullet}{\approx} \left(C'\left[\hat{C}[P_1]\right], L\right)$. Thus, we see $\hat{C}[P_0] \underset{(\Gamma \parallel L, m)}{\approx} \hat{C}[P_1]$.

□