Addendum for the Paper
“Taming Message-passing Communication in Compositional Reasoning about Confidentiality”

Ximeng Li  Heiko Mantel  Markus Tasch

Department of Computer Science, TU-Darmstadt, Germany
{li, mantel, tasch}@mais.informatik.tu-darmstadt.de

In this document, we provide the supplementary material for the paper “Taming Message-passing Communication in Compositional Reasoning about Confidentiality” [1]. In Sect. 1 we provide the complete structural operational semantics for our programming language, and the complete instrumented semantics supporting our definition of “sound use of assumptions”. In Sect. 2 we provide the proofs for Theorem 1 and Theorem 2 from the paper. In Sect. 3 we present an information-flow type system for local security that does not contain semantic side conditions. In Sect. 4 we discuss the typability of the authentication example and the auction example from the paper, outlining the differences between the type system from the paper and the variant from Sect. 3 of this addendum.

1  Operational Semantics of Message-passing Language

1.1  Basic Semantics

Below we present the rules defining the operational semantics of our message-passing language.

\[
\begin{align*}
\text{mem'} & = \text{mem}[x \mapsto [e]_{\text{mem}}] \\
\langle \text{skip}; \text{mem} \rangle ; \sigma & \rightarrow \langle \text{stop}; \text{mem} \rangle ; \sigma \\
\langle x := e; \text{mem} \rangle ; \sigma & \rightarrow \langle \text{stop}; \text{mem}' \rangle ; \sigma \\
b \in \{\text{tt, ff} \} & \quad [e]_{\text{mem}} = b \\
\langle \text{if} \ e \ \text{then} \ prog_1 \ \text{else} \ prog_2 \ \text{fi}; \text{mem} \rangle ; \sigma & \rightarrow \langle \text{prog}_b; \text{mem} \rangle ; \sigma \\
[e]_{\text{mem}} & = \text{tt} \\
\langle \text{while} \ e \ \text{do} \ prog \ \text{od}; \text{mem} \rangle ; \sigma & \rightarrow \langle \text{prog}; \text{while} \ e \ \text{do} \ prog \ \text{od}; \text{mem} \rangle ; \sigma \\
[e]_{\text{mem}} & = \text{ff} \\
\langle \text{prog}_1; \text{mem} \rangle ; \sigma & \rightarrow \langle \text{prog}_1'; \text{mem}' ; \sigma' \rangle \\
\text{prog}_1 & \neq \text{stop} \\
\langle \text{prog}_1; \text{mem} \rangle ; \sigma & \rightarrow \langle \text{prog}_1'; \text{mem}' ; \sigma' \rangle \\
\langle \text{prog}_1; \text{prog}_2; \text{mem} \rangle ; \sigma & \rightarrow \langle \text{prog}_1'; \text{prog}_2'; \text{mem}' ; \sigma' \rangle \\
\langle \text{prog}_1; \text{prog}_2; \text{mem} \rangle ; \sigma & \rightarrow \langle \text{prog}_2'; \text{mem}' ; \sigma' \rangle \\
\sigma(ch) & = v \cdot \gamma \quad \text{mem'} = \text{mem}[x \mapsto v] \quad \sigma' = \sigma[ch \mapsto \gamma] \\
\langle \text{recv}(ch, x); \text{mem} \rangle ; \sigma & \rightarrow \langle \text{stop}; \text{mem}' ; \sigma' \rangle \\
\sigma(ch) & = v \cdot \gamma \quad \text{mem'} = \text{mem}[x \mapsto v][x_b \mapsto \text{tt}] \quad \sigma' = \sigma[ch \mapsto \gamma] \\
\langle \text{if-recv}(ch, x, x_b); \text{mem} \rangle ; \sigma & \rightarrow \langle \text{stop}; \text{mem}' ; \sigma' \rangle \\
\sigma(ch) & = \epsilon \quad \text{mem'} = \text{mem}[x_b \mapsto \text{ff}] \\
\langle \text{if-recv}(ch, x, x_b); \text{mem} \rangle ; \sigma & \rightarrow \langle \text{stop}; \text{mem}' ; \sigma' \rangle \\
[e]_{\text{mem}} & = v \quad \sigma' = \sigma[ch \mapsto \sigma(ch) \cdot v] \\
\langle \text{send}(ch, e); \text{mem} \rangle ; \sigma & \rightarrow \langle \text{stop}; \text{mem} ; \sigma' \rangle
\end{align*}
\]
1.2 Instrumented Semantics

Below we present a calculus defining the judgment \( pcnf; \sigma; \mu \rightarrow chs \ (pcnf'; \sigma'; \mu') \). This judgment says: A process with the process configuration \( pcnf \) and the set \( chs \) of channels used in the continuation executes one step from the channel state \( \sigma \), resulting in the process configuration \( pcnf' \) and channel state \( \sigma' \), updating the instrumentation state from \( \mu \) to \( \mu' \).

In the calculus to be presented, we write \( \mu^* \) for \( \lambda ch:ICH.\mu(ch) \downarrow_1 \), and \( \mu^\circ \) for \( \lambda ch:ICH.\mu(ch) \downarrow_2 \). We use the function \( ichs-of : Prog \rightarrow 2^{ICH} \) to obtain the set of internal channels syntactically occurring in a program. This function is inductively defined by \( ichs-of(\text{send}(ch, e)) = ichs-of(\text{\textit{"a"}recv}(ch, x)) = \{ ch \} \), \( ichs-of(\text{if } e \text{ then } prog_1 \text{ else } prog_2 \) fi\( \) = \( ichs-of(prog_1) \cup ichs-of(prog_2) \), \( ichs-of(\text{while } e \text{ do } prog \) od\( \) = \( ichs-of(prog) \), and \( ichs-of(prog) = \emptyset \) otherwise.

\[
\begin{align*}
\langle \text{skip; mem}; \sigma; \mu \rangle & \rightarrow_{chs} \langle \text{stop; mem}; \sigma; \mu \rangle \\
\langle \text{skip; mem} \rangle & \rightarrow_{chs} \langle \text{stop; mem} \rangle
\end{align*}
\]

\[
\begin{align*}
\text{lev}(e) &= \mathbb{H} \quad b \in \{ tt, ff \} \quad [e]_{mem} = b \\
chs' &= ichs-of(prog_\mu) \cup ichs-of(prog_f) \cup chs \\
\mu' &= (\mu^*[chs' \mapsto \mathbb{H}^{[\mu^*]'[chs']}] \cdot \mu^{\circ}[chs' \mapsto \mathbb{H}])
\end{align*}
\]

\[
\langle \text{if } e \text{ then } prog_1 \text{ else } prog_2 \text{ fi; mem}; \sigma; \mu \rangle \rightarrow_{chs} \langle \text{prog}_1; \text{mem}; \sigma; \mu' \rangle
\]

\[
\begin{align*}
\text{lev}(e) &= \mathbb{H} \\
[chs' &= ichs-of(prog_\mu) \cup chs \quad \mu' = (\mu^*[chs' \mapsto \mathbb{H}^{[\mu^*]'[chs']}] \cdot \mu^{\circ}[chs' \mapsto \mathbb{H}])
\end{align*}
\]

\[
\langle \text{while } e \text{ do } prog \text{ od; mem}; \sigma; \mu \rangle \rightarrow_{chs} \langle \text{prog; while } e \text{ do } prog \text{ od; mem}; \sigma; \mu' \rangle
\]

\[
\begin{align*}
\text{lev}(e) &= \mathbb{H} \\
[chs' &= ichs-of(prog_\mu) \cup chs \quad \mu' = (\mu^*[chs' \mapsto \mathbb{H}^{[\mu^*]'[chs']}] \cdot \mu^{\circ}[chs' \mapsto \mathbb{H}])
\end{align*}
\]

\[
\langle \text{while } e \text{ do } prog \text{ od; mem}; \sigma; \mu \rangle \rightarrow_{chs} \langle \text{prog; while } e \text{ do } prog \text{ od; mem}; \sigma; \mu' \rangle
\]

\[
\begin{align*}
\text{lev}(e) &= \mathbb{L} \\
[chs' &= ichs-of(prog_\mu) \cup chs \quad \mu' = (\mu^*[chs' \mapsto \mathbb{L}^{[\mu^*]'[chs']}] \cdot \mu^{\circ}[chs' \mapsto \mathbb{L}])
\end{align*}
\]

\[
\langle \text{while } e \text{ do } prog \text{ od; mem}; \sigma; \mu \rangle \rightarrow_{chs} \langle \text{prog; while } e \text{ do } prog \text{ od; mem}; \sigma; \mu' \rangle
\]
In the above, we obtain the trace underlying a rich trace using the function \( \text{trace} \).

Given a distributed program \( \text{dprog} \), we use the judgment \( \mu \).

We define this judgment on the basis of the judgment \( \langle \cdot \rangle \).

Our semantic instrumentation—i.e., neither forbids any local computation steps, nor enables any additional ones. This result will be formalized in Sect. \( \xi \).

We use the judgment \( \langle \text{pcnf}; \sigma; \mu \rangle \rightarrow \langle \text{pcnf}'; \sigma'; \mu' \rangle \) to say that a process with the process configuration \( \text{pcnf} \) executes one step from the channel state \( \sigma \), resulting in the process configuration \( \text{pcnf}' \) and channel state \( \sigma' \), updating the instrumentation state from \( \mu \) to \( \mu' \). We define this judgment by \( \langle \text{pcnf}; \sigma; \mu \rangle \rightarrow \langle \text{pcnf}'; \sigma'; \mu' \rangle \) if and only if \( \langle \text{pcnf}; \sigma; \mu \rangle \rightarrow_{\phi} \langle \text{pcnf}'; \sigma'; \mu' \rangle \). Our semantic instrumentation is transparent wrt. the basic semantics—it neither forbids any local computation steps, nor enables any additional ones. This result will be formalized in Sect. \( \xi \).

We use the judgment \( rtr \rightarrow_{\xi} rtr' \) to state that the rich trace \( rtr' \) is extended into the rich trace \( rtr' \) after one step of a distributed program, or of the environment, under the strategy \( \xi \). We define this judgment on the basis of the judgment \( \langle \text{pcnf}; \sigma; \mu \rangle \rightarrow \langle \text{pcnf}'; \sigma'; \mu' \rangle \) for the process-local instrumented semantics.
2 Proofs

We define a subset of high conditional programs by the following syntax. We denote the set of all high conditional programs by $HCond$.

$$hcond ::= \text{if } e \text{ then } prog_1 \text{ else } prog_2 \text{ fi } (\text{lev}(e) = \mathbb{H}) \mid \text{while } e \text{ do } prog \text{ od } (\text{lev}(e) = \mathbb{H}) \mid hcond; prog$$

**Lemma 1.** If $\langle\langle prog; mem_1\rangle; \sigma_1; \mu_1 \rangle \rightarrow \text{chs}_1 \langle\langle prog'_1; mem'_1\rangle; \sigma'_1; \mu'_1 \rangle$, $\langle\langle prog; mem_2\rangle; \sigma_2; \mu_2 \rangle \rightarrow \text{chs}_2 \langle\langle prog'_2; mem'_2\rangle; \sigma'_2; \mu'_2 \rangle$, $\text{lev}_1 = \text{lev}_2$, and $prog'_1 \neq prog'_2$, then $prog \in HCond$.

**Proof.** We proceed with a structural induction on $prog \in Prog$.

**Case if $e$ then $prog_1$ else $prog_2$ fi:** From $mem_1 = \text{lev}_2 mem_2$ and $prog'_1 \neq prog'_2$, it is not difficult to see that $\text{lev}(e) = \mathbb{H}$. Thus, $prog \in HCond$.

**Case while $e$ do $prog_1$ od:** Analogous to the previous case.

**Case $prog_1; prog_2$:** Without loss of generality, we first show $prog_1 \in HCond$ by the following case analysis on $prog'_1$ and $prog'_2$ in the lemma statement.

**Sub-case $prog'_1 \neq prog'_2 \land prog''_1 \neq prog''_2$:** There exist $prog'$ and $prog''$ such that $prog' \neq prog''$, $prog'_1 = prog'; prog_2$, $prog''_2 = prog''_2$, and

$$\langle\langle prog_1; mem_1\rangle; \sigma_1; \mu_1 \rangle \rightarrow \text{chs}_1 \langle\langle prog'_1; mem'_1\rangle; \sigma'_1; \mu'_1 \rangle$$

$$\langle\langle prog_1; mem_2\rangle; \sigma_2; \mu_2 \rangle \rightarrow \text{chs}_2 \langle\langle prog''_1; mem''_1\rangle; \sigma''_1; \mu''_1 \rangle$$

Using the induction hypothesis, we can derive $prog_1 \in HCond$.

**Sub-case $prog'_1 = prog'_2 \land prog''_1 \neq prog''_2$:** There exists some $prog''_1 \neq \text{stop}$ such that $prog'_1 = prog''_1; prog_2$, and

$$\langle\langle prog_1; mem_1\rangle; \sigma_1; \mu_1 \rangle \rightarrow \text{chs}_1 \langle\langle \text{stop}; mem'_1\rangle; \sigma'_1; \mu'_1 \rangle$$

$$\langle\langle prog_1; mem_2\rangle; \sigma_2; \mu_2 \rangle \rightarrow \text{chs}_2 \langle\langle \text{stop}; mem''_1\rangle; \sigma''_1; \mu''_1 \rangle$$

Using the induction hypothesis, we can derive $prog_1 \in HCond$.

**Sub-case $prog'_1 \neq prog'_2 \land prog''_1 = prog''_2$:** Contradiction with $prog'_1 \neq prog'_2$.

Since $prog_1 \in HCond$, $prog_2 \in Prog$, we have $prog_1; prog_2 \in HCond$.

In the remaining cases, the statement of the lemma vacuously holds. □

**Lemma 2.** If $prog \in HCond$, and $\langle\langle prog; mem\rangle; \sigma; \mu \rangle \rightarrow \text{chs} \langle\langle prog'; mem'\rangle; \sigma'; \mu' \rangle$, then $\forall ch \in \text{ichs-of}(prog) \cup \text{chs} : \exists \text{lst} \in \text{Lev}^*: \mu'(ch) = (\text{lst}, \mathbb{H})$.

**Proof.** It is sufficient to prove

If $hcond \rightarrow^* prog$, and $\langle\langle prog; mem\rangle; \sigma; \mu \rangle \rightarrow \text{chs} \langle\langle prog'; mem'\rangle; \sigma'; \mu' \rangle$, then $\forall ch \in \text{ichs-of}(prog) \cup \text{chs} : \exists \text{lst} \in \text{Lev}^*: \mu'(ch) = (\text{lst}, \mathbb{H})$.

We proceed with an induction on the derivation of $prog$.

- Suppose $hcond \rightarrow$ if $e$ then $prog_1$ else $prog_2$ fi, $\text{lev}(e) = \mathbb{H}$, and $prog = \text{if } e \text{ then } prog_1 \text{ else } prog_2$ fi. It is straightforward to derive the conclusion of the lemma by inspection of the rules of the instrumented semantics.

- Suppose $hcond \rightarrow$ while $e$ do $prog_1$ od, $\text{lev}(e) = \mathbb{H}$, and $prog = \text{while } e \text{ do } prog_1$ od. It is straightforward to derive the conclusion of the lemma by inspection of the rules of the instrumented semantics.
Proposition 1. If \( \forall ch \in \text{ICH} : |\sigma_1(ch)|_{\mu_1(ch)} = |\sigma_2(ch)|_{\mu_2(ch)}, (\sigma_1, \mu_1) \models \text{acs}_1 \), and \((\sigma_2, \mu_2) \models \text{acs}_2\), then \( |\sigma_1|_{\text{ICS}} = |\sigma_2|_{\text{ICS}}\).

Proof. Under the hypotheses of the proposition, we show

\[
\forall ch \in \text{ICH} : (|\sigma_1(ch)| > 0 \land |\sigma_2(ch)| > 0) \Rightarrow \text{first}(\sigma_1(ch)) = \text{first}(\sigma_2(ch))
\]

\[
\forall ch \in \text{ICH} : (|\sigma_1(ch)| > 0 \Rightarrow |\sigma_2(ch)| > 0)
\]

Pick an arbitrary \( ch \in \text{ICH} \).

Suppose \( |\sigma_1(ch)|_{\text{ICS}} = |\sigma_2(ch)|_{\text{ICS}}\). Without loss of generality, we assume \( |\sigma_1(ch)|_{\text{ICS}} > |\sigma_2(ch)|_{\text{ICS}}\). From \((\sigma_1, \mu_1) \models \text{acs}_1\), we have \( |\mu_1(ch)|_{\text{ICS}} > |\mu_2(ch)|_{\text{ICS}}\). Hence \( |\sigma_1(ch)|_{\text{ICS}} > |\sigma_2(ch)|_{\text{ICS}}\). Thus we have if \( |\sigma_1(ch)|_{\text{ICS}} > 0 \) then \( \text{first}(\sigma_1(ch)) = \text{first}(\sigma_2(ch))\), by Lemma 4 and \( |\sigma_1(ch)|_{\text{ICS}} = |\sigma_2(ch)|_{\text{ICS}}\).

Suppose \( |\sigma_1(ch)|_{\text{ICS}} \neq |\sigma_2(ch)|_{\text{ICS}}\). Without loss of generality, we assume \( |\sigma_1(ch)|_{\text{ICS}} > |\sigma_2(ch)|_{\text{ICS}}\). From \((\sigma_1, \mu_1) \models \text{acs}_1\), we have \( |\mu_1(ch)|_{\text{ICS}} > |\mu_2(ch)|_{\text{ICS}}\). Thus it is not difficult to derive \( |\sigma_1(ch)|_{\text{ICS}} > 0 \Rightarrow |\sigma_2(ch)|_{\text{ICS}} > 0\).

Lemma 5. If \( mem_1 = \text{ICS} \), \( \forall ch \in \text{ICH} : (|\sigma_1(ch)|_{\mu_1(ch)} = |\sigma_2(ch)|_{\mu_2(ch)}), \langle (\text{prog}; \text{mem}_1); \sigma_1; \mu_1 \rangle \Rightarrow \langle (\text{prog}_1'; \text{mem}_1'); \sigma_1'; \mu_1' \rangle \), and \( \langle (\text{prog}; \text{mem}_2); \sigma_2; \mu_2 \rangle \Rightarrow \langle (\text{prog}_2'; \text{mem}_2'); \sigma_2'; \mu_2' \rangle\), then \( \forall ch \in \text{ICH} : (|\sigma_1'(ch)|_{\mu_1'(ch)} = |\sigma_2'(ch)|_{\mu_2'(ch)}\).\)

Proof. We proceed with an induction on the derivation of

\[
\langle (\text{prog}; \text{mem}_1); \sigma_1; \mu_1 \rangle \Rightarrow \langle (\text{prog}_1'; \text{mem}_1'); \sigma_1'; \mu_1' \rangle\]

We only present a few representative cases.
Lemma 6. If \( (\langle \text{prog'; mem'} \rangle; \sigma; \mu') \rightarrow (\langle \text{prog'; mem'} \rangle; \sigma'; \mu') \), \( \forall ch \in \text{ichs-of}(\text{prog}) : \sigma'(ch) = [\sigma(ch)]_{\mu'(ch)} \) and \( \mu' = \mu \), then \( \forall ch \in \text{ichs-of}(\text{prog}) : \mu'(ch) = [\sigma(ch)]_{\mu'(ch)} \).

Proof. We proceed with an induction on the derivation
\[
(\langle \text{prog'; mem'} \rangle; \sigma; \mu) \rightarrow (\langle \text{prog'; mem'} \rangle; \sigma'; \mu')
\] (2)

We only show a few representative cases in detail.

Case [2] is by the rule for send, over an external channel. Here \( \text{prog} \) is \( \text{send}(ch, e) \), with \( ch \in ECh \).

The result of the lemma is straightforward since \( \forall ch \in ICh : \sigma'(ch) = [\sigma(ch)]_{\mu'(ch)} \) and \( \mu' = \mu \).

Case [2] is by the rule for send, over an internal channel. Here \( \text{prog} \) is \( \text{send}(ch, e) \) with \( ch \in ICh \).

We have \( ch \in \text{ichs-of}(\text{prog}) \). Hence \( \mu'(ch) = [\sigma(ch)]_{\mu'(ch)} \). By the instrumented semantics, we have \( \forall ch' : (\mu'(ch')) = [\sigma(ch')]_{\mu'(ch')} \). Thus, we can derive the conclusion of the lemma using the hypothesis \( (\mu')^{\circ} = \mu' \).
The remaining cases where a non-composite command is executed are straightforward – the cases

prior to

The following statements hold.
We prove augmented versions of the statements with universal quantification over sets $chs$ of internal channels.

Case 2 is by a rule for sequential composition. We have $prog = prog_1; prog_2$ for some $prog_1$ and $prog_2$, and $\langle prog_1; mem; \sigma; \mu \rangle \rightarrow \langle prog_1'; mem'; \sigma'; \mu' \rangle$ for some $prog_1'$. The result of the lemma can now be derived using the induction hypothesis.

Case 2 is by a rule for if. We have $\sigma' = \sigma$. Thus it is not difficult to derive the conclusion of the lemma using the hypothesis $(\mu')^o = \mu^o$.

The remaining cases where a non-composite command is executed are straightforward – the cases for communication are analogous to the cases for send. The cases for while are analogous to the cases for if. The induction completes the proof.

\begin{lemma}
If $prog_{10} = prog_{20}$, for all $k < n$, $\langle prog_{1k}; mem_{1k} \rangle \approx \langle prog_{2k}; mem_{2k} \rangle$, $\langle prog_{1k}; mem_{1k}; \sigma'_{1k}; \mu'_{1k} \rangle \rightarrow \langle prog_{1(k+1)}; mem_{1(k+1)}; \sigma'_{1(k+1)}; \mu'_{1(k+1)} \rangle$, $\langle prog_{2k}; mem_{2k}; \sigma'_{2k}; \mu'_{2k} \rangle \rightarrow \langle prog_{2(k+1)}; mem_{2(k+1)}; \sigma'_{2(k+1)}; \mu'_{2(k+1)} \rangle$, $\forall ch \in ICh : \sigma'_{1k}(ch) = \sigma'_{2k}(ch)$, and $\forall ch \in ICh : \mu'_{1k}(ch) \subseteq (\mu'_{2k})^o(ch)$, then $\forall ch \in ICh : (\sigma'_{1n}(ch))_{\mu_{1n}(ch)} = (\sigma'_{2n}(ch))_{\mu_{2n}(ch)}$.
\end{lemma}

\begin{proof}
We make a case analysis on whether the derivatives of $prog_{10}$ and $prog_{20}$ become different prior to $prog_{1n}$ and $prog_{2n}$.

- Suppose there exists some $k_0 < n$ such that $prog_{1k_0} \neq prog_{2k_0}$. We have some $k' \leq k_0$ such that $prog_{1(k_0-1)} = prog_{2(k_0-1)}$ but $prog_{1k'} \neq prog_{2k'}$. By $\langle prog_{1(k'-1)}; mem_{1(k'-1)} \rangle \approx \langle prog_{2(k'-1)}; mem_{2(k'-1)} \rangle$, we have $mem_{1(k'-1)} = mem_{2(k'-1)}$. Using Lemma 4, we can obtain $\langle prog_{1(k'-1)} \rangle_\mu \in HCond$ and $\langle prog_{2(k'-1)} \rangle_\mu \in HCond$. Using Lemma 2, we obtain that $\forall ch \in ichs-of(prog_{1(k'-1)} ; \mu_{1k'}(ch)) = H$, and $\forall ch \in ichs-of(prog_{2(k'-1)} ; \mu_{2k'}(ch)) = H$. It is not difficult to see that

$$ichs-of(prog_{1(k'-1)}) \subseteq ichs-of(prog_{2(k'-1)}) \land ichs-of(prog_{2(k'-1)}) \supseteq ichs-of(prog_{2(n-1)})$$

Using the condition that for all $k < n$, $\forall ch \in ICh : \mu^o_{1k}(ch) \subseteq (\mu'_{1k})^o(ch) \land (\mu'_{2k})^o(ch)$, and the instrumented semantics, we derive $\forall ch \in ichs-of(prog_{1(n-1)}) : (\mu'_{1(n-1)})^o(ch) = H$, and $\forall ch \in ichs-of(prog_{2(n-1)}) : (\mu'_{2(n-1)})^o(ch) = H$. It is not difficult to see that $\mu^o_{1n} = (\mu'_{1(n-1)})^o$ and that $\mu^o_{2n} = (\mu'_{2(n-1)})^o$.

Using Lemma 3 we can derive

$$\forall ch \in ICh : |\sigma'_{1(n-1)}(ch))_{\mu'_{1(n-1)}(ch)} = |\sigma_{1n}(ch))_{\mu_{1n}(ch)}$$

$$\forall ch \in ICh : |\sigma'_{2(n-1)}(ch))_{\mu'_{2(n-1)}(ch)} = |\sigma_{2n}(ch))_{\mu_{2n}(ch)}$$

Thus it follows from $\forall ch \in ICh : (\sigma'_{1(n-1)}(ch))_{\mu'_{1(n-1)}(ch)} = (\sigma'_{2(n-1)}(ch))_{\mu'_{2(n-1)}(ch)}$ that $\forall ch \in ICh : (\sigma_{1n}(ch))_{\mu_{1n}(ch)} = (\sigma_{2n}(ch))_{\mu_{2n}(ch)}$ holds.

- Suppose for all $k < n$, $prog_{1k} = prog_{2k}$. We have $prog_{1(n-1)} = prog_{2(n-1)}$. It follows from Lemma 2 that $\forall ch \in ICh : (\sigma_{1n}(ch))_{\mu_{1n}(ch)} = (\sigma_{2n}(ch))_{\mu_{2n}(ch)}$ holds.

The case analysis above completes the proof.
\end{proof}

\begin{proposition}
The following statements hold.

- If $\langle pcnf; \sigma; \mu \rangle \rightarrow \langle pcnf; \sigma'; \mu' \rangle$, then $\langle pcnf; \sigma' \rangle \rightarrow \langle pcnf'; \sigma' \rangle$.

- If $\langle pcnf; \sigma \rangle \rightarrow \langle pcnf'; \sigma' \rangle$, then for all $\mu$, there exists $\mu'$ such that $\langle pcnf; \sigma; \mu \rangle \rightarrow \langle pcnf'; \sigma'; \mu' \rangle$.
\end{proposition}

\begin{proof}
We prove augmented versions of the statements with universal quantification over sets $chs$ of internal channels:
1. For all $chs \in 2^{ICh}$, if $\langle pcnf; \sigma; \mu \rangle \rightarrow_{chs} \langle pcnf'; \sigma'; \mu' \rangle$, then $\langle pcnf; \sigma \rangle \rightarrow \langle pcnf'; \sigma' \rangle$.
2. If $\langle pcnf; \sigma \rangle \rightarrow \langle pcnf'; \sigma' \rangle$, then for all $\mu$, and $chs \in 2^{ICh}$, there exists $\mu'$ such that $\langle pcnf; \sigma; \mu \rangle \rightarrow_{chs} \langle pcnf'; \sigma'; \mu' \rangle$.

Each of 1 and 2 can be proved straightforwardly by induction on the appropriate semantic derivation. We omit the details. It is not difficult to see that the proposition directly follows from 1 and 2. □

We proceed with the proof of Theorem 1 from the paper.

**Theorem 1.** For a distributed program $dprog = \|_{i} prog_i$, if $LSec(prog_i)$ holds for all $i$, and $dprog$ ensures a sound use of assumptions, then we have $KBSec(dprog)$.

We construct the following binary relation on traces.

$$R_{dprog} \triangleq \{ (\text{trace-of}(rtr_1), \text{trace-of}(rtr_2)) \mid rtr_1 \in \text{traces}_{\xi_1}(dprog) \land rtr_2 \in \text{traces}_{\xi_2}(dprog) \land \nu rtr_1 \in [0, \ldots, \nu rtr_2 - 1] :$$

$$\exists n, prog_1, \ldots, prog_n, prog_{2n}, mem_{1n}, \ldots, mem_{1n}, mem_{2n}, \ldots, mem_{2n}, \sigma_1, \sigma_2, \mu_1, \mu_2 :$$

$$\nu rtr_1(k) = \langle \langle prog_1; mem_{1n} \rangle, \ldots, \langle prog_{1n}; mem_{1n} \rangle ; \sigma_1; \mu_1 \rangle \land$$

$$\nu rtr_2(k) = \langle \langle prog_{2n}; mem_{2n} \rangle, \ldots, \langle prog_{2n}; mem_{2n} \rangle ; \sigma_2; \mu_2 \rangle \land$$

$$(\forall j \in \{1, \ldots, n\} : \langle prog_{1j}; mem_{1j} \rangle \approx \langle prog_{2j}; mem_{2j} \rangle) \land$$

$$\sigma_1 \models \sigma_2 \land \forall ch \in ICh : \sigma_1(ch)_{\mu_1(ch)} = \sigma_2(ch)_{\mu_2(ch)} \land$$

$$\left( k < \nu rtr_1 - 1 \Rightarrow \left( \forall j : \text{step from } rtr_1(k) \text{ is by } prog_{1j} \iff \text{step from } rtr_2(k) \text{ is by } prog_{2j} \right) \right) \land$$

$$\text{(step from } rtr_1(k) \text{ is by env.} \iff \text{step from } rtr_2(k) \text{ is by env.}) \right) \}$$

Theorem 1 immediately follows from the following lemma, which is stated using $R_{dprog}$.

**Lemma 8.** For $dprog = [\|_{i} prog_i]$, if $\forall i \in \{1, \ldots, n\} : LSec(prog_i)$, and $dprog$ ensures a sound use of assumptions, then for all $\xi_1, \xi_2$ satisfying $\xi_1 \models \xi_2$, all $tr_1 \in \text{traces}_{\xi_1}(dprog)$, there exists $tr_2 \in \text{traces}_{\xi_2}(dprog)$ such that $(tr_1, tr_2) \in R_{dprog}$.

**Proof.** Fix $tr_1 \in \text{traces}_{\xi_1}(dprog)$. We prove that there exists $tr_2 \in \text{traces}_{\xi_2}(dprog)$ such that $(tr_1, tr_2) \in R_{dprog}$ by an induction on $|tr_1|$.

**Base case.** We prove the result for the case where $|tr_1| = 1$. By $tr_1 \in \text{traces}_{\xi_1}(dprog)$, we have $tr_1 = [ \langle \langle prog_1; mem_{i1} \rangle, \ldots, \langle prog_n; mem_{i1} \rangle ; \sigma_{i1} \rangle ]$. Pick $tr_2 = tr_1$. By $\forall i \in \{1, \ldots, n\} : LSec(prog_i)$, we have $\forall i \in \{1, \ldots, n\} : \langle prog_i; mem_{i1} \rangle \approx \langle prog_i; mem_{i1} \rangle$. Using $rtr_1 = rtr_2 = [ \langle \langle prog_1; mem_{i1} \rangle, \ldots, \langle prog_n; mem_{i1} \rangle ; \sigma_{i1}; \mu_{i1} \rangle ]$, it is not difficult to obtain $(tr_1, tr_2) \in R_{dprog}$.

**Inductive case.** We prove the existence of a proper $tr_2$ in the case where $|tr_1| = n$ ($n > 1$).

We know that there exist some $tr_{10}$ and $gcnf_1$ such that $|tr_{10}| = n - 1$ and $tr_1 = tr_{10} \cdot gcnf_1$. By the induction hypothesis, there exists $tr_{20} \in \text{traces}_{\xi_2}(dprog)$ such that $(tr_{10}, tr_{20}) \in R_{dprog}$. By
the construction of $R_{dprog}$, there exist $tr_{10}$ and $tr_{20}$ such that

$$tr_{10} = \text{trace-of}(tr_{10}) \land tr_{20} = \text{trace-of}(tr_{20})$$

(3)

$$tr_{10} \in rtraces_{\xi_1}(dprog) \land tr_{20} \in rtraces_{\xi_2}(dprog)$$

(4)

$$|tr_{10}| = |tr_{20}|$$

(5)

$$\forall k \in \{0, \ldots, |tr_{10}|-1\} :$$

(6)

\[ \exists n, \ prog_{11}, \ldots, \ prog_{1n}, \ prog_{21}, \ldots, \ prog_{2n}, \ mem_{11}, \ldots, \ mem_{1n}, \ mem_{21}, \ldots, \ mem_{2n}, \ \sigma_1, \ \sigma_2, \ \mu_1, \ \mu_2 : \]

$$rtr_{10}(k) = \langle \langle prog_{11}; \ mem_{11} \rangle, \ldots, \langle prog_{1n}; \ mem_{1n} \rangle; \ \sigma_1; \ \mu_1 \rangle \land$$

$$rtr_{20}(k) = \langle \langle prog_{21}; \ mem_{21} \rangle, \ldots, \langle prog_{2n}; \ mem_{2n} \rangle; \ \sigma_2; \ \mu_2 \rangle \land$$

$$\forall j \in \{1, \ldots, n\} : \ \langle prog_{ij}; \ mem_{ij} \rangle \approx \langle prog_{2j}; \ mem_{2j} \rangle \land$$

(7)

$$\sigma_1 \preceq \sigma_2 \land \forall ch \in ICh : [\sigma_1(ch)]_{\mu_1(ch)} = [\sigma_2(ch)]_{\mu_2(ch)} \land$$

(8)

\[ k < |tr_{10}|-1 \Rightarrow \left( \forall j : \text{step from } rtr_{10}(k) \text{ is by } prog_{ij} \Leftrightarrow \text{step from } rtr_{20}(k) \text{ is by } prog_{2j} \right) \land (\text{step from } rtr_{10}(k) \text{ is by env. } \Leftrightarrow \text{step from } rtr_{20}(k) \text{ is by env.}) \right) \]

By (6), there exist $prog_{11}, \ldots, prog_{1n}, \ prog_{21}, \ldots, prog_{2n}, \ mem_{11}, \ldots, mem_{1n}, \ mem_{21}, \ldots, mem_{2n}, \ \sigma_1, \ \sigma_2, \ \mu_1, \ \mu_2$, such that

$$rtr_{10}(n-2) = \langle \langle prog_{11}; \ mem_{11} \rangle, \ldots, \langle prog_{1n}; \ mem_{1n} \rangle; \ \sigma_1; \ \mu_1 \rangle$$

(9)

$$rtr_{20}(n-2) = \langle \langle prog_{21}; \ mem_{21} \rangle, \ldots, \langle prog_{2n}; \ mem_{2n} \rangle; \ \sigma_2; \ \mu_2 \rangle$$

(10)

$$\forall j \in \{1, \ldots, n\} : \ \langle prog_{ij}; \ mem_{ij} \rangle \approx \langle prog_{2j}; \ mem_{2j} \rangle$$

(11)

We make a case analysis as to whether the step from the last configuration of $tr_{10}$ in $tr_1$ is by a process or by the environment.

- Suppose the step from the last configuration of $tr_{10}$ in $tr_1$ is by the $j$-the process. That is, we have $\langle \langle prog_{ij}; \ mem_{ij} \rangle; \ \sigma_1 \rangle \rightarrow \langle \langle prog'_{ij}; \ mem'_{ij} \rangle; \ \sigma_1' \rangle$ for some $prog'_{ij}$, $mem'_{ij}$, and $\sigma_1'$. Hence, there exists $\mu_1'$ such that

$$\langle \langle prog_{ij}; \ mem_{ij} \rangle; \ \sigma_1; \ \mu_1 \rangle \rightarrow \langle \langle prog'_{ij}; \ mem'_{ij} \rangle; \ \sigma_1' ; \ \mu_1' \rangle$$

(12)

by Proposition 2. Let $rtr_1 = rtr_{10} \cdot \langle \ldots, \langle prog'_{ij}; \ mem'_{ij} \rangle, \ldots \rangle; \ \sigma_1'; \ \mu_1' \rangle$. We then have $rtr_1 \in rtraces_{\xi_j}(dprog)$. We also have $tr_1 = \text{trace-of}(rtr_1)$.

From the hypothesis that $dprog$ ensures a sound use of assumptions, (4), and (7), we have

$$\sigma_1, \ \mu_1 \models \text{asm-of}(prog_{1j}) \land \sigma_2, \ \mu_2 \models \text{asm-of}(prog_{2j})$$

(13)

From (11), (13), and Proposition 1, we have

$$\sigma_1 \models \text{asm-of}(prog_{1j}) \land \sigma_2 \models \text{asm-of}(prog_{2j})$$

(14)

By (13), we also have

$$\sigma_1 \times NE \ \text{asm-of}(prog_{1j}) \land \sigma_2 \times NE \ \text{asm-of}(prog_{2j})$$

(15)
By (9), (10), (14), (15), and (12), there exist $\text{prog}^t_{2j}$, $\text{mem}^t_{2j}$, $\sigma^t_j$ and $\mu^t_j$ such that
\begin{align}
\langle \langle \text{prog}^t_{2j}; \text{mem}^t_{2j} \rangle; \sigma^t_2; \mu^t_2 \rangle & \to \langle \langle \text{prog}^t_{2j}; \text{mem}^t_{2j} \rangle; \sigma^t_2; \mu^t_2 \rangle \\
\sigma^t_1 & \simeq \Sigma \sigma^t_2 \\
\langle \text{prog}^t_{1j}; \text{mem}^t_{1j} \rangle & \simeq \langle \text{prog}^t_{2j}; \text{mem}^t_{2j} \rangle
\end{align}

We proceed to show $\forall \text{ch} \in \text{ICH} : (\sigma^t_1(\text{ch}))_{\mu^t_1(\text{ch})} = (\sigma^t_2(\text{ch}))_{\mu^t_2(\text{ch})}$. Without loss of generality, we assume that the indices $k$ such that the steps from $\text{rtr}_{10}(k)$ and $\text{rtr}_{20}(k)$ are taken by the $j$-th process are $k_1, \ldots, k_m$ for some $m > 0$, where $k_m = n - 2$. For each $r$, supposing the instrumentation states right after the steps from $\text{rtr}_{10}(k_r)$ and $\text{rtr}_{20}(k_r)$ are $\mu_{1k_r}$ and $\mu_{2k_r}$, and the instrumentation states right before the steps from $\text{rtr}_{10}(k_{r+1})$ and $\text{rtr}_{20}(k_{r+1})$ are $\mu_{1k_{r+1}}$ and $\mu_{2k_{r+1}}$, we have $\forall \text{ch} \in \text{ICH} : (\mu^t_1)_{\mu^t_1(\text{ch})}(\text{ch}) \subseteq \mu^t_{1k_{r+1}}(\text{ch}) \wedge (\mu^t_2)_{\mu^t_2(\text{ch})}(\text{ch}) \subseteq \mu^t_{2k_{r+1}}(\text{ch})$, by (11). Using the above conditions together with (6), we now have two related executions of $\text{prog}^t_j$ (that might be interrupted in the middle by steps from other programs or from the overall environment of the distributed program) that satisfy the conditions of Lemma 7. Thus we have
\begin{align}
\forall \text{ch} \in \text{ICH} : (\sigma^t_1(\text{ch}))_{\mu^t_1(\text{ch})} = (\sigma^t_2(\text{ch}))_{\mu^t_2(\text{ch})}
\end{align}

by Lemma 7.

Let $\text{rtr}_2 = \text{rtr}_{20} \cdot ([\ldots, \langle \text{prog}^t_{2j}; \text{mem}^t_{2j}, \ldots \rangle; \sigma^t_2; \mu^t_2], \text{tr}_2 = \text{trace-of}(\text{rtr}_2)$. It is not difficult to see that $\text{tr}_2 \in \text{traces}_{\xi_2}(\text{dprog})$ with the help of Proposition 2. We can derive $(\text{tr}_1, \text{tr}_2) \in \text{D}_{\text{dprog}}$ by using $\text{rtr}_1$ and $\text{rtr}_2$.

Suppose the step from the last configuration of $\text{tr}_{10}$ in $\text{tr}_1$ is by the environment. We have
\begin{align}
\text{tr}_1 = \text{trace-of}(\text{rtr}_{10} \cdot ([\ldots, \langle \text{prog}^t_{1j}; \text{mem}^t_{1j} \rangle, \ldots \rangle; \sigma^t_1; \mu^t_1)),
\end{align}

where $\sigma^t_1 = \sigma_1[\text{ECh} \Rightarrow \xi_1(\text{tr}_{10})(\text{ECh})]$. Let
\begin{align}
\text{tr}_2 = \text{trace-of}(\text{rtr}_{20} \cdot ([\ldots, \langle \text{prog}^t_{2j}; \text{mem}^t_{2j} \rangle, \ldots \rangle; \sigma^t_2; \mu^t_2)),
\end{align}

where $\sigma^t_2 = \sigma_2[\text{ECh} \Rightarrow \xi_2(\text{tr}_{20})(\text{ECh})]$. From (6), we have $\text{tr}_{10} \simeq_{Tr} \text{tr}_{20}$. Thus we have $\sigma^t_1 \simeq \sigma^t_2$ from (10), and the hypothesis $\xi_1 \simeq \xi_2$. On this basis, it is not difficult to establish $(\text{tr}_1, \text{tr}_2) \in \text{D}_{\text{dprog}}$.

The induction on $|\text{tr}_1|$ above completes the proof.

We define pairings $(\mathbb{C}[\text{A}_1, \ldots, \text{A}_n], \varphi(\text{A}_1, \ldots, \text{A}_n))$ of secure contexts and conditions, with holes $\text{A}_1, \ldots, \text{A}_n$ to be filled in with programs.

\begin{align}
(\mathbb{C}[\text{A}_1, \ldots, \text{A}_n], \varphi(\text{A}_1, \ldots, \text{A}_n)) & := \\
| (x := e, \text{lev}(e) \subseteq \text{lev}(x)) \\
| (\text{send}(\text{ch}, e), \text{lev}(e) \subseteq \text{lev}^*(\text{ch}, \emptyset)) \\
| (\text{as-rev}(\text{ch}, x), (\text{NE} \notin \text{as} \Rightarrow \text{lev}^*(\text{ch}, \text{as}) \subseteq \text{lev}(x)) \wedge \text{lev}^*(\text{ch}, \text{as}) \subseteq \text{lev}(x)) \\
| (\text{as-if-rev}(\text{ch}, x, x_0), (\text{NE} \notin \text{as} \Rightarrow \text{lev}^*(\text{ch}, \text{as}) \subseteq \text{lev}(x_0)) \wedge \text{lev}^*(\text{ch}, \text{as}) \subseteq \text{lev}(x)) \\
| (\text{if} e \text{ then} \text{A}_1 \text{ else} \text{A}_2 \text{ fi}, \text{lev}(e) \equiv \text{H} \Rightarrow \text{A}_1 \sim \text{A}_2) \\
| (\text{while} e \text{ do} \text{A}_1 \text{ od}, \text{lev}(e) = \text{H}) \\
| (\text{A}_1; \text{A}_2, \text{ true})
\end{align}

We prove the following hook-up property of $\text{LSec}(\cdot)$.
Theorem 3. For all indices $n \geq 0$, pairs $(C[\uparrow_1, \ldots, \uparrow_n], \varphi(\uparrow_1, \ldots, \uparrow_n))$, programs $prog_1$, $\ldots$, $prog_n$, we have $LSec(C[prog_1, \ldots, prog_n])$, if we have $\varphi(prog_1, \ldots, prog_n)$ and $\forall j \in \{1, \ldots, n\} : LSec(prog_j)$.

Proof. We first consider the non-composite cases $(C[prog_1, \ldots, prog_n], \varphi(\ldots))$ where $prog$ is one of $\text{skip}$, $x := e$, $\text{send}(ch, e)$, $\text{recv}(ch, x)$, and $\text{if-recv}(ch, x, x_b)$.

For each of the non-composite cases, we construct the relation

$$R_{prog} = \{((\text{prog}; \text{mem}_1), (\text{prog}; \text{mem}_2)) \mid \text{mem}_1 =_{L} \text{mem}_2\} \cup$$

$$\{((\text{stop}; \text{mem}_1), (\text{stop}; \text{mem}_2)) \mid \text{mem}_1 =_{L} \text{mem}_2\}$$

(20)

(21)

It is trivial that for all $\text{mem}_1$ and $\text{mem}_2$ such that $\text{mem}_1 =_{L} \text{mem}_2$, we have $(\text{prog}; \text{mem}_1) R_{prog} (\text{prog}; \text{mem}_2)$.

We proceed to show that $R_{prog}$ is an assumption-aware bisimulation. It is not difficult to see that $R_{prog}$ is symmetric. Pick arbitrary pair $((\text{prog}_1; \text{mem}_1), (\text{prog}_2; \text{mem}_2))$ from $R_{prog}$. We have $\text{mem}_1 =_{L} \text{mem}_2$. We also have $\text{stop} \equiv \text{prog}_1 = \text{stop} = \text{prog}_2$.

We show how the remaining proof obligations are discharged for the interesting cases for $\text{prog}$ below.

Case $\text{send}(ch, e)$. We assume the hypothesis

$$\text{lev}(e) \subseteq \text{lev}^*(ch, \emptyset)$$

(22)

We also assume $\sigma_1 \equiv \sigma_2, \sigma_1 \not\equiv \emptyset$, and $\sigma_2 \not\equiv \emptyset$.

Suppose for some $\sigma'_1$ we have

$$\langle(\text{send}(ch, e); \text{mem}_1); \sigma_1 \rangle \rightarrow \langle(\text{stop}; \text{mem}_1); \sigma'_1 \rangle$$

It is not difficult to see that there is some $\sigma'_2$ such that

$$\langle(\text{send}(ch, e); \text{mem}_2); \sigma_2 \rangle \rightarrow \langle(\text{stop}; \text{mem}_2); \sigma'_2 \rangle$$

We have $(\text{stop}; \text{mem}_1) R_{prog} (\text{stop}; \text{mem}_2)$ by $\text{mem}_1 =_{L} \text{mem}_2$. We proceed to show $\sigma'_1 \sim_{L} \sigma'_2$ with a case analysis on whether $\text{ch} \in \text{ECh}$.

Sub-case $\text{ch} \in \text{ECh}$. We make a further case analysis on the class of $\text{ch}$.

- Suppose $\text{ch} \in \text{PriCh}$. We have $ob(ch, \sigma'_1) = ob(ch, \sigma'_2) = \emptyset$. It is not difficult to see $\sigma'_1 \sim_{L} \sigma'_2$, since the message queues for the other channels are unchanged in $\sigma'_1$ and $\sigma'_2$.

- Suppose $\text{ch} \in \text{EncCh}$. From $\sigma_1 \sim_{L} \sigma_2$, we have $ob(ch, \sigma_1) = ob(ch, \sigma_2) = \bigcirc^n$ for some $n$. We then have $ob(ch, \sigma'_1) = ob(ch, \sigma'_2) = \bigcirc^{n+1}$. It is not difficult to see that $\sigma'_1 \sim_{L} \sigma'_2$.

- Suppose $\text{ch} \in \text{PubCh}$. From $\sigma_1 \sim_{L} \sigma_2$, we have $ob(ch, \sigma_1) = ob(ch, \sigma_2) = \text{vlst}$ for some list $\text{vlst}$ of values. We have $\text{lev}^*(ch, \emptyset) = \text{L}$. We thus have $\text{lev}(e) = \text{L}$ by (22). Thus we have $\llbracket e \rrbracket_{\text{mem}_1} = \llbracket e \rrbracket_{\text{mem}_2}$ by $\text{mem}_1 =_{L} \text{mem}_2$. We have $ob(ch, \sigma'_1) = ob(ch, \sigma'_2) = \text{vlst} \cdot \text{v}$, where $\text{v} = \llbracket e \rrbracket_{\text{mem}_1} = \llbracket e \rrbracket_{\text{mem}_2}$. It is not difficult to see that $\sigma'_1 \sim_{L} \sigma'_2$.

Sub-case $\text{ch} \in \text{Ich}$. Since the message queues of all the external channels are unaffected, we trivially have $\sigma'_1 \sim_{L} \sigma'_2$. 
Case $a^s \text{recv}(ch, x)$. We assume the following hypotheses

$$\forall NE \notin as \Rightarrow \text{lev}^\Sigma(ch, as) = \text{L}$$  
(23)

$$\text{lev}^\Sigma(ch, as) \sqcup \text{lev}^\Sigma(ch, as) \subseteq \text{lev}(x)$$  
(24)

We also assume

$$\sigma_1 \overset{\text{ax}(ch)}{\longrightarrow} \sigma_2$$  
(25)

$$\sigma_1 \overset{\text{NE}}{\times} (as \times \{ch\}) \land \sigma_2 \overset{\text{NE}}{\times} (as \times \{ch\})$$  
(26)

Suppose for some $\text{mem}_1'$ and $\sigma_1'$ we have

$$\langle \langle a^s \text{recv}(ch, x); \text{mem}_1'; \sigma_1 \rangle \rightarrow \langle \langle \text{stop}; \text{mem}_1'; \sigma_1' \rangle \rangle$$  
(27)

We make a case analysis on whether $ch \in ECh$ to discharge the remaining proof obligations.

Sub-case $ch \in ECh$. We make a further case analysis on whether $NE \in as$.

- Suppose $NE \in as$.
  
  By [26], we have $|\sigma_2(ch)| > 0$. Hence there exists some $\sigma_2'$ and $\text{mem}_2'$ such that
  
  $$\langle \langle a^s \text{recv}(ch, x); \text{mem}_2'; \sigma_2 \rangle \rightarrow \langle \langle \text{stop}; \text{mem}_2'; \sigma_2' \rangle \rangle$$

  We make a further case analysis on the class of $ch$.

• Suppose $ch \in \text{PriCh}$. By [24], we have $\text{lev}(x) = \text{H}$. Thus we vacuously have $\text{lev}(x) = \text{L} \Rightarrow \text{mem}_1'(x) = \text{mem}_2'(x)$. It is not difficult to establish $\text{mem}_1' = \text{mem}_2'$ since the values for the other variables are unchanged in $\text{mem}_1'$ and $\text{mem}_2'$. Hence we have $\langle \text{stop}; \text{mem}_1' \rangle R_{\text{prog}} \langle \text{stop}; \text{mem}_2' \rangle$.

  We have $\text{ob}(ch, \sigma_1') = \text{ob}(ch, \sigma_2') = \emptyset$. Thus, it is not difficult to establish $\sigma_1' \succeq \Sigma \sigma_2'$, since the message queues for the other channels are unchanged in $\sigma_1'$ and $\sigma_2'$.

• Suppose $ch \in \text{EncCh}$. That $\langle \text{stop}; \text{mem}_1' \rangle R_{\text{prog}} \langle \text{stop}; \text{mem}_2' \rangle$ can be established analogously to the case where $ch \in \text{PriCh}$.

  From $\sigma_1 \succeq \Sigma \sigma_2$, we have $\text{ob}(ch, \sigma_1) = \text{ob}(ch, \sigma_2) = \bigodot^n$ for some $n$, where $n > 0$ since $NE \in as$. Hence $\text{ob}(ch, \sigma_1') = \text{ob}(ch, \sigma_2') = \bigodot^{n-1}$. On this basis, it is not difficult to see that $\sigma_1' \succeq \Sigma \sigma_2'$.

• Suppose $ch \in \text{PubCh}$.

  From $\sigma_1 \succeq \Sigma \sigma_2$, we have $\text{ob}(ch, \sigma_1) = \text{ob}(ch, \sigma_2) = \text{vlst}$, where $\text{vlst}$ is a non-empty list of values since $NE \in as$.

  Suppose $\text{vlst} = v \cdot \text{vlst}'$ for some $v \in \text{Val}$ and $\text{vlst}' \in \text{Val}^*$. We have $\text{mem}_1'(x) = \text{mem}_2'(x) = v$. On this basis, it is not difficult to see that $\text{mem}_1' = \text{mem}_2'$ holds. Hence we have $\langle \text{stop}; \text{mem}_1' \rangle R_{\text{prog}} (\text{stop}; \text{mem}_2')$. In addition, we have $\sigma_1' (ch) = \sigma_2' (ch) = \text{vlst}'$. On this basis, it is not difficult to establish $\sigma_1' \succeq \Sigma \sigma_2'$.

- Suppose $NE \notin as$. By [23], we have $\text{lev}^\Sigma(ch, as) = \text{L}$. Hence $ch \in \text{PubCh}$ or $ch \in \text{EncCh}$. By [27], we have $|\sigma_1(ch)| > 0$. Thus we have $|\sigma_2(ch)| > 0$ by $\sigma_1 \succeq \Sigma \sigma_2$ and the possible classes of $ch$. Hence there exists some $\sigma_2'$ and $\text{mem}_2'$ such that

  $$\langle \langle a^s \text{recv}(ch, x); \text{mem}_2'; \sigma_2 \rangle \rightarrow \langle \langle \text{stop}; \text{mem}_2'; \sigma_2' \rangle \rangle$$
The remaining proof obligations can be discharged by a case analysis on whether \( \text{ch} \in \text{PubCh} \) or \( \text{ch} \in \text{EncCh} \), analogously to the case where \( \text{NE} \in \text{as} \).

**Sub-case** \( \text{ch} \in \text{ICh} \). We make a further case analysis on whether \( \text{NE} \in \text{as} \).

- Suppose \( \text{NE} \in \text{as} \).
  By (26), we have \( |\sigma_2(\text{ch})| > 0 \). Hence there exist some \( \sigma'_2 \) and \( \text{mem}'_2 \) such that
  \[
  \langle \langle *\text{recv}(\text{ch}, x); \text{mem}_2 \rangle; \sigma_2 \rangle \rightarrow \langle \langle \text{stop}; \text{mem}'_2 \rangle; \sigma'_2 \rangle
  \]
  Since no message queues for the external channels are affected in \( \sigma'_1 \) or \( \sigma'_2 \), we trivially have \( \sigma'_1 \simeq_S \sigma'_2 \).

  We make a further case analysis on whether \( \text{L}^0 \) and \( \text{L}^* \) are in \( \text{as} \), to show \( \langle \text{stop}; \text{mem}'_1 \rangle \text{R}_{\text{prog}} \langle \text{stop}; \text{mem}'_2 \rangle \), which boils down to showing \( \text{mem}'_1 =_L \text{mem}'_2 \).

  - Suppose \( \text{L}^* \notin \text{as} \) or \( \text{L}^0 \notin \text{as} \).

    From (24), we have \( \text{lev}(x) = \mathbb{H} \). Hence it vacuously holds that \( \text{lev}(x) = \text{L} \Rightarrow \text{mem}'_1(x) = \text{mem}'_2(x) \). Thus we have \( \text{mem}'_1 =_L \text{mem}'_2 \) from \( \text{mem}_1 =_L \text{mem}_2 \), and the fact that the values of the other variables are unchanged in \( \text{mem}'_1 \) and \( \text{mem}'_2 \).

  - Suppose \( \text{L}^* \in \text{as} \) and \( \text{L}^0 \in \text{as} \).

    By (26) and \( \text{NE} \in \text{as} \), we have \( |\sigma_1(\text{ch})| > 0 \), and \( |\sigma_2(\text{ch})| > 0 \). Hence we can obtain \( \text{first}(\sigma_1(\text{ch})) = \text{first}(\sigma_2(\text{ch})) \) using (25). Hence we can derive \( \text{mem}'_1(x) = \text{mem}'_2(x) \). On this basis, it is not difficult to derive \( \text{mem}'_1 =_L \text{mem}'_2 \).

- Suppose \( \text{NE} \notin \text{as} \).

  Using (23), we derive \( \text{L}^0 \in \text{as} \). By (27), we have \( |\sigma_1(\text{ch})| > 0 \). Thus we have \( |\sigma_2(\text{ch})| > 0 \) by (25). Hence there exist some \( \sigma'_2 \) and \( \text{mem}'_2 \) such that
  \[
  \langle \langle *\text{recv}(\text{ch}, x); \text{mem}_2 \rangle; \sigma_2 \rangle \rightarrow \langle \langle \text{stop}; \text{mem}'_2 \rangle; \sigma'_2 \rangle
  \]
  Since no message queues for the external channels are affected in \( \sigma'_1 \) or \( \sigma'_2 \), we trivially have \( \sigma'_1 \simeq_S \sigma'_2 \).

  We make a case analysis on whether \( \text{L}^* \in \text{as} \) to show \( \langle \text{stop}; \text{mem}'_1 \rangle \text{R}_{\text{prog}} \langle \text{stop}; \text{mem}'_2 \rangle \), which boils down to showing \( \text{mem}'_1 =_L \text{mem}'_2 \).

  - Suppose \( \text{L}^* \notin \text{as} \).

    By (24), we have \( \text{lev}(x) = \mathbb{H} \). Hence we have \( \text{lev}(x) = \text{L} \Rightarrow \text{mem}'_1(x) = \text{mem}'_2(x) \). On this basis, \( \text{mem}'_1 =_L \text{mem}'_2 \) can be derived.

  - Suppose \( \text{L}^* \in \text{as} \).

    By (25), \( |\sigma_1(\text{ch})| > 0 \), and \( |\sigma_2(\text{ch})| > 0 \), we have \( \text{first}(\sigma_1(\text{ch})) = \text{first}(\sigma_2(\text{ch})) \). Hence, we have \( \text{mem}'_1(x) = \text{mem}'_2(x) \). On this basis, \( \text{mem}'_1 =_L \text{mem}'_2 \) can be derived.

  **Case** \(*\text{if-recv}(\text{ch}, x, x_b)\). The reasoning can be structured similarly to the case for \(*\text{recv}(\text{ch}, x)\).

For each of the composite cases, we construct a specific relation that is shown to be an assumption-aware bisimulation, which serves to justify the local security of the corresponding program.
Case if $e$ then $prog_a$ else $prog_b$, fi. We construct the following relation where if is a shorthand for the program if $e$ then $prog_a$ else $prog_b$, fi.

$$R_d = \{(\text{if}; \text{mem}_1), (\text{if}; \text{mem}_2) \mid \text{mem}_1 =_{L} \text{mem}_2\} \cup \approx$$

For all $\text{mem}_1$, $\text{mem}_2$ such that $\text{mem}_1 =_{L} \text{mem}_2$, we have $(\text{if}; \text{mem}_1) R_d (\text{if}; \text{mem}_2)$. We proceed to show that $R_d$ is an assumption-aware bisimulation. It is obvious that $R_d$ is symmetric. Pick an arbitrary pair $p = ((\text{prog}_1; \text{mem}_1), (\text{prog}_2; \text{mem}_2))$ from $R_d$. We can also derive $\text{mem}_1 =_{L} \text{mem}_2$ and $\text{prog}_1 = \text{stop} \Leftrightarrow \text{prog}_2 = \text{stop}$.

To discharge the remaining proof obligations, we make a case analysis on which part of $R_d p$ belongs to. We assume the following hypotheses.

$$L\text{Sec}(prog_a) \quad (28)$$

$$L\text{Sec}(prog_b) \quad (29)$$

$$\text{lev}(e) = \mathbb{H} \Rightarrow prog_a \sim prog_b \quad (30)$$

Sub-case $p \in \{(\text{if}; \text{mem}_1), (\text{if}; \text{mem}_2) \mid \text{mem}_1 =_{L} \text{mem}_2\}$. We have $\text{prog}_1 = \text{prog}_2 = \text{if}$.

Pick arbitrary channel states $\sigma_1$ and $\sigma_2$ such that $\sigma_1 \approx_{\Sigma} \sigma_2$, $\sigma_1 \models_{\Sigma} \emptyset$, and $\sigma_2 \times^{NE} \emptyset$.

Suppose without loss of generality that

$$\langle (\text{if}; \text{mem}_1); \sigma_1 \rangle \rightarrow \langle (\text{prog}_a; \text{mem}_1); \sigma_2 \rangle$$

We make a case analysis on whether $[e]_{\text{mem}_2}$ is equal to $[e]_{\text{mem}_1}$.

- Suppose $[e]_{\text{mem}_2} \neq [e]_{\text{mem}_1}$. We have

$$\langle (\text{if}; \text{mem}_2); \sigma_2 \rangle \rightarrow \langle (\text{prog}_b; \text{mem}_2); \sigma_2 \rangle$$

From $\text{mem}_1 =_{L} \text{mem}_2$, we have $\text{lev}(e) = \mathbb{H}$. Hence we have $prog_a \sim prog_b$ by (30). Hence we have $(\text{prog}_a; \text{mem}_1) \approx (\text{prog}_b; \text{mem}_2)$, which gives $(\text{prog}_a; \text{mem}_1) R_d (\text{prog}_b; \text{mem}_2)$. We also have $\sigma_1 \approx_{\Sigma} \sigma_2$, which is preserved from before.

- Suppose $[e]_{\text{mem}_2} = [e]_{\text{mem}_1}$. We have

$$\langle (\text{if}; \text{mem}_2); \sigma_2 \rangle \rightarrow \langle (\text{prog}_a; \text{mem}_2); \sigma_2 \rangle$$

By (28) and $\text{mem}_1 =_{L} \text{mem}_2$, we have $(\text{prog}_a; \text{mem}_1) \approx (\text{prog}_b; \text{mem}_2)$, which directly gives $(\text{prog}_a; \text{mem}_1) R_d (\text{prog}_b; \text{mem}_2)$. We also have $\sigma_1 \approx_{\Sigma} \sigma_2$, which is preserved from before.

Sub-case $p \in \approx$. Straightforward from the fact that $\approx$ is an assumption-aware bisimulation.

Case while $e$ do $prog_a$, od. We construct the relation $R_{\text{while}} = R_0 \cup R_1 \cup R_2$, where while is a shorthand for while $e$ do $prog_a$, od, and

$$R_0 = \{(\text{while}; \text{mem}_1), (\text{while}; \text{mem}_2) \mid \text{mem}_1 =_{L} \text{mem}_2\}$$

$$R_1 = \{(\text{prog}_1; \text{while}; \text{mem}_1), (\text{prog}_2; \text{while}; \text{mem}_2) \mid (\text{prog}_1; \text{mem}_1) \approx (\text{prog}_2; \text{mem}_2)\}$$

$$R_2 = \{(\text{stop}; \text{mem}_1), (\text{stop}; \text{mem}_2) \mid \text{mem}_1 =_{L} \text{mem}_2\}$$

For all $\text{mem}_1$ and $\text{mem}_2$ such that $\text{mem}_1 =_{L} \text{mem}_2$, we have $(\text{while}; \text{mem}_1) R_{\text{while}} (\text{while}; \text{mem}_2)$. We proceed to show that $R_{\text{while}}$ is an assumption-aware bisimulation. We have that $R_{\text{while}}$ is
symmetric. Pick an arbitrary pair $p = \langle\langle prog_1; mem_1\rangle, \langle prog_2; mem_2\rangle\rangle$ from $R_{\text{while}}$. We have $\text{mem}_1 =_{\text{L}} \text{mem}_2$, and $\text{prog}_1 \neq \text{stop} \Leftrightarrow \text{prog}_2 \neq \text{stop}$.

To discharge the remaining proof obligations, we make a case analysis on which part of $R_{\text{while}} p$ belongs to. We assume the following hypotheses.

\[ L\text{Sec}(\text{prog}_a) \]
\[ \text{lev}(e) = \text{L} \]

**Sub-case** $p \in R_0$. Pick arbitrary channel states $\sigma_1$ and $\sigma_2$ such that $\sigma_1 \simeq_{\Sigma} \sigma_2$, $\sigma_1 \equiv \sigma_2$, $\sigma_1 \times^{_{\text{NE}}} \emptyset$, and $\sigma_2 \times^{_{\text{NE}}} \emptyset$.

We make a further case analysis on whether $\text{while}$ continues or terminates in one step.

- Suppose $(\langle \text{while}; \text{mem}_1 \rangle; \sigma_1) \rightarrow (\langle \text{prog}_a; \text{while}; \text{mem}_1 \rangle; \sigma_1)$. By (33) and $\text{mem}_1 =_{\text{L}} \text{mem}_2$, we have $\llbracket e \rrbracket_{\text{mem}_2} = \llbracket e \rrbracket_{\text{mem}_1}$. Hence we have

  \[ (\langle \text{while}; \text{mem}_2 \rangle; \sigma_2) \rightarrow (\langle \text{prog}_a; \text{while}; \text{mem}_2 \rangle; \sigma_2) \]

  By (32) and $\text{mem}_1 =_{\text{L}} \text{mem}_2$, we have $\langle \text{prog}_a; \text{mem}_1 \rangle \simeq \langle \text{prog}_a; \text{mem}_2 \rangle$. Hence, we have $\langle \text{prog}_a; \text{while}; \text{mem}_1 \rangle R_{\text{while}} \langle \text{prog}_a; \text{while}; \text{mem}_2 \rangle$. We also have $\sigma_1 \simeq_{\Sigma} \sigma_2$, which is trivially preserved.

- Suppose $(\langle \text{while}; \text{mem}_1 \rangle; \sigma_1) \rightarrow (\langle \text{stop}; \text{mem}_1 \rangle; \sigma_1)$. This case is straightforward.

**Sub-case** $p \in R_1$. We have $\text{prog}_1 = \text{prog}_{10}; \text{while}$, and $\text{prog}_2 = \text{prog}_{20}; \text{while}$ for some $\text{prog}_{10}$ and $\text{prog}_{20}$ such that

\[ \langle \text{prog}_{10}; \text{mem}_1 \rangle \approx \langle \text{prog}_{20}; \text{mem}_2 \rangle \]

Pick arbitrary channel states $\sigma_1$ and $\sigma_2$ such that

\[ \sigma_1 \simeq_{\Sigma} \sigma_2 \land \sigma_1 \equiv \sigma_2 \land \sigma_1 \times^{_{\text{NE}}} \text{asm-of}(\text{prog}_{10}) \land \sigma_2 \times^{_{\text{NE}}} \text{asm-of}(\text{prog}_{20}) \]

We make a further case analysis on whether $\text{prog}_{10}$ continues or terminates after one step.

- Suppose $(\langle \text{prog}_{10}; \text{while}; \text{mem}_1 \rangle; \sigma_1) \rightarrow (\langle \text{prog}_{10}; \text{while}; \text{mem}_1' \rangle; \sigma_1')$, with $(\langle \text{prog}_{10}; \text{mem}_1 \rangle; \sigma_1) \rightarrow (\langle \text{prog}_{10}; \text{mem}_1' \rangle; \sigma_1')$, and $\text{prog}_{10} \neq \text{stop}$. By (34) and (35), there exist $\text{prog}_{20}', \text{mem}_{2}'$, and $\sigma_2'$ such that $(\langle \text{prog}_{20}; \text{mem}_2 \rangle; \sigma_2) \rightarrow (\langle \text{prog}_{20}; \text{mem}_{2}' \rangle; \sigma_2')$, $\sigma_1 \simeq_{\Sigma} \sigma_2$, and $(\langle \text{prog}_{10}; \text{mem}_1 \rangle; \sigma_1) \approx (\langle \text{prog}_{20}; \text{mem}_{2}' \rangle; \sigma_2')$. Hence, we have $\text{prog}_{10}' = \text{stop} \Leftrightarrow \text{prog}_{20}' = \text{stop}$, which gives $\text{prog}_{20}' \neq \text{stop}$.

Thus, we have $(\langle \text{prog}_{20}; \text{while}; \text{mem}_2 \rangle; \sigma_2) \rightarrow (\langle \text{prog}_{20}; \text{while}; \text{mem}_2' \rangle; \sigma_2')$, $\sigma_1' \simeq_{\Sigma} \sigma_2'$, and $(\langle \text{prog}_{10}; \text{while}; \text{mem}_1 \rangle R_{\text{while}} \langle \text{prog}_{20}; \text{while}; \text{mem}_2 \rangle$.

- Suppose $(\langle \text{prog}_{10}; \text{while}; \text{mem}_1 \rangle; \sigma_1) \rightarrow (\langle \text{stop}; \text{mem}_1' \rangle; \sigma_1')$, with $(\langle \text{prog}_{10}; \text{mem}_1 \rangle; \sigma_1) \rightarrow (\langle \text{stop}; \text{mem}_1' \rangle; \sigma_1')$. By (34) and (35), we know that there exist $\text{prog}_{20}', \text{mem}_{2}'$, and $\sigma_2'$ such that $(\langle \text{prog}_{20}; \text{mem}_2 \rangle; \sigma_2) \rightarrow (\langle \text{prog}_{20}; \text{mem}_{2}' \rangle; \sigma_2')$, $\sigma_1' \simeq_{\Sigma} \sigma_2'$, and $(\langle \text{stop}; \text{mem}_1 \rangle; \sigma_1) \approx (\langle \text{prog}_{20}; \text{mem}_{2}' \rangle; \sigma_2')$. Hence, we have $\text{mem}_1' =_{\text{L}} \text{mem}_2'$, and $\text{prog}_{20}' = \text{stop}$.

Thus, we have $(\langle \text{prog}_{20}; \text{while}; \text{mem}_2 \rangle; \sigma_2) \rightarrow (\langle \text{while}; \text{mem}_2' \rangle; \sigma_2')$, $\sigma_1' \simeq_{\Sigma} \sigma_2'$, as well as $(\langle \text{while}; \text{mem}_1' \rangle R_{\text{while}} \langle \text{while}; \text{mem}_2 \rangle$.

**Sub-case** $p \in R_2$. Trivial.
Case $\text{prog}_a; \text{prog}_b$. We construct the relation $R_r = R_0 \cup \approx$, where
\[ R_0 = \{ ((\text{prog}_{10}; \text{prog}_b; \text{mem}_1), (\text{prog}_{20}; \text{prog}_b; \text{mem}_2)) \mid (\text{prog}_{10}; \text{mem}_1) \approx (\text{prog}_{20}; \text{mem}_2) \} \]

We assume the following hypotheses
\begin{align*}
\text{LSec}(\text{prog}_a) \\
\text{LSec}(\text{prog}_b)
\end{align*} \tag{36} \tag{37}

Pick arbitrary $\text{mem}_1$ and $\text{mem}_2$ such that $\text{mem}_1 \equiv \text{mem}_2$. By \eqref{36}, we have $(\text{prog}_a; \text{mem}_1) \approx (\text{prog}_a; \text{mem}_2)$. Hence we have $(\text{prog}_a; \text{prog}_b; \text{mem}_1) \approx (\text{prog}_a; \text{prog}_b; \text{mem}_2)$. We proceed to show that $R_r$ is an assumption-aware bisimulation. It is obvious that $R_r$ is symmetric. Pick arbitrary pair $p = ((\text{prog}_a; \text{mem}_1), (\text{prog}_b; \text{mem}_2))$ from $R_r$. We have $\text{mem}_1 \equiv \text{mem}_2$, and $\text{prog}_a = \text{stop} \Leftrightarrow \text{prog}_b = \text{stop}$.

We discharge the remaining proof obligations with a case analysis on which part of $R_r$ $p$ belongs.

**Sub-case** $p \in R_0$. We have $\text{prog}_a = \text{prog}_{10}; \text{prog}_b$, and $\text{prog}_b = \text{prog}_{20}; \text{prog}_b$, for some $\text{prog}_{10}$ and $\text{prog}_{20}$ such that
\[ (\text{prog}_{10}; \text{mem}_1) \approx (\text{prog}_{20}; \text{mem}_2) \] \tag{38}

Pick arbitrary channel states $\sigma_1$ and $\sigma_2$ such that
\begin{align*}
\sigma_1 &\succeq \Sigma \land \sigma_1 \equiv \text{asm-of}(\text{prog}_{10}) \land \text{asm-of}(\text{prog}_{20}) \sigma_2 \\
&\land \sigma_1 \equiv \text{asm-of}(\text{prog}_{10}) \land \sigma_2 \equiv \text{asm-of}(\text{prog}_{20})
\end{align*} \tag{39}

We make a case analysis on whether $\text{prog}_{10}$ is exhausted in the next step of $\text{prog}_{10}; \text{prog}_b$.

- Suppose for some $\text{prog}'_{10}$, $\text{mem}'_1$, and $\sigma'_1$, we have
  \[ (\text{prog}'_{10}; \text{mem}'_1; \sigma_1) \to (\text{prog}'_{10}; \text{mem}'_1; \sigma'_1) \]
  with $(\text{prog}_{10}; \text{mem}_1; \sigma_1) \to (\text{prog}'_{10}; \text{mem}'_1; \sigma'_1)$, and $\text{prog}'_{10} \neq \text{stop}$. By \eqref{38} and \eqref{39}, there exist $\text{prog}'_{20}$, $\text{mem}'_2$, $\sigma'_2$ such that
  \[ (\text{prog}'_{20}; \text{mem}'_2; \sigma_2) \to (\text{prog}'_{20}; \text{mem}'_2; \sigma'_2) \]
  $\rho'_1 \succeq \rho'_2$, and $(\text{prog}'_{10}; \text{mem}_1) \approx (\text{prog}'_{20}; \text{mem}'_2)$. Hence $\text{prog}'_{10} = \text{stop} \Leftrightarrow \text{prog}'_{20} = \text{stop}$. Hence $\text{prog}'_{20} \neq \text{stop}$.

  Thus, we have $((\text{prog}_{20}; \text{prog}_b; \text{mem}_2) ; \sigma_2) \to (\text{prog}_{20}; \text{prog}_b; \text{mem}_2; \sigma'_2)$, $\rho'_1 \succeq \rho'_2$, and $(\text{prog}_{10}; \text{prog}_b; \text{mem}_1) \approx (\text{prog}_{20}; \text{prog}_b; \text{mem}_2)$.

  - Suppose for some $\text{mem}'_1$, and $\sigma'_1$, we have
    \[ (\text{prog}_{10}; \text{mem}_1; \sigma_1) \to (\text{stop}; \text{mem}'_1; \sigma'_1) \]
    with $(\text{prog}_{10}; \text{mem}_1; \sigma_1) \to (\text{stop}; \text{mem}'_1; \sigma'_1)$. By \eqref{38} and \eqref{39}, there exist $\text{prog}'_{20}$, $\text{mem}'_2$, $\sigma'_2$ such that
    \[ (\text{prog}_{20}; \text{mem}_2; \sigma_2) \to (\text{prog}_{20}; \text{mem}_2; \sigma'_2) \]
    $\rho'_1 \succeq \rho'_2$, and $(\text{stop}; \text{mem}'_1) \approx (\text{prog}_{20}; \text{mem}'_2)$. Hence $\text{mem}'_1 \equiv \text{mem}'_2$, and $\text{prog}_{20} = \text{stop}$. Hence we have $((\text{prog}_{20}; \text{prog}_b; \text{mem}_2) ; \sigma_2) \to (\text{prog}_b; \text{mem}'_2; \sigma'_2)$. By \eqref{37} and $\text{mem}_1 = \text{mem}'_2$, we also have $((\text{prog}_b; \text{mem}'_1) \approx (\text{prog}_b; \text{mem}'_2)$. Thus $((\text{prog}_b; \text{mem}'_1) R (\text{prog}_b; \text{mem}'_2)$. 

16
**Sub-case** \( p \in \approx \). Trivial.

The above case analysis on the pairs of programs with holes and conditions completes the proof. \( \Box \)

We next prove Theorem 2.

**Theorem 2.** If \( \text{lev} \vdash \text{prog} \), then \( \text{LSec}(\text{prog}) \).

**Proof.** The proof is by induction on the derivation of \( \text{lev} \vdash \text{prog} \). In each case we build on the hook-up property of \( \text{LSec}(\cdot) \) (Proposition 3) to obtain the desired result. We only present one base case and one inductive case below.

**Case** \( \text{asrecv}(\text{ch}, x) \): By \( \text{lev} \vdash \text{asrecv}(\text{ch}, x) \), we have

\[
\begin{align*}
\text{NE} \notin \text{as} & \Rightarrow \text{lev}^0(\text{ch}, \text{as}) = L \\
\text{lev}^0(\text{ch}, \text{as}) \sqcup \text{lev}^*(\text{ch}, \text{as}) & \sqsubseteq \text{lev}(x)
\end{align*}
\]

Instantiating Proposition 3 with \( n = 0 \), and the fourth pair of context and condition, we know that \( \text{LSec}(\text{asrecv}(\text{ch}, x)) \) holds, if \( (\text{NE} \notin \text{as} \Rightarrow \text{lev}^0(\text{ch}, \text{as}) = L) \land \text{lev}^0(\text{ch}, \text{as}) \sqcup \text{lev}^*(\text{ch}, \text{as}) \sqsubseteq \text{lev}(x) \), which is ensured by (40), (41).

**Case** \( \text{if} \ e \ \text{then prog}_1 \ \text{else prog}_2 \ \text{fi} \): By \( \text{lev} \vdash \text{if} \ e \ \text{then prog}_1 \ \text{else prog}_2 \ \text{fi} \), we have

\[
\begin{align*}
\text{lev} \vdash \text{prog}_1 \\
\text{lev} \vdash \text{prog}_2 \\
\text{lev}(e) = \text{H} & \Rightarrow \text{prog}_1 \sim \text{prog}_2
\end{align*}
\]

Instantiating Proposition 3 with \( n = 2 \), the sixth pair of context and condition, \( \text{prog}_1 \), and \( \text{prog}_2 \), we have \( \text{LSec}(\text{if} \ e \ \text{then prog}_1 \ \text{else prog}_2 \ \text{fi}) \) holds if \( \text{lev}(e) = \text{H} \Rightarrow \text{prog}_1 \sim \text{prog}_2, \text{LSec}(\text{prog}_1) \), and \( \text{LSec}(\text{prog}_2) \). Using the induction hypothesis on (42) and (43), we can derive \( \text{LSec}(\text{prog}_1) \) and \( \text{LSec}(\text{prog}_2) \). Combining this with (44), it is not difficult to see that all the conditions for \( \text{LSec}(\text{if} \ e \ \text{then prog}_1 \ \text{else prog}_2 \ \text{fi}) \) to be established are satisfied.

In the remaining cases, the premises of the typing rules give rise to the premises of the corresponding statements in the hook-up property in an analogous fashion to the cases above. The induction completes the proof of this theorem. \( \Box \)
This type system establishes the judgment

\[ \text{lev} \vdash_S \text{prog}, \text{sayingly that the program prog is (fully}
\] syntactically) typable in the environment \( \text{lev} \).

The typing rules are presented in Fig. 1. Except for the if rule, all the rules in Fig. 1 are identical to the rules of our original type system (in Fig. 1 of [1]) for the same language constructs.

For the if rule, the side condition \( \text{lev}(e) = \mathbb{H} \Rightarrow \text{low-slice-of}(\text{prog}_1) = \text{low-slice-of}(\text{prog}_2) \) is used to replace the semantic side condition \( \text{lev}(e) = \mathbb{H} \Rightarrow \text{prog}_1 \sim \text{prog}_2 \) in our original type system. Here, the function \( \text{low-slice-of} : \text{Prog} \to \text{LS} \cup \{\perp\} \) gives the low slice of each program (defined in Fig. 2). The set \( \text{LS} \) of low slices is the same as the set of programs, except that the set of expressions is extended with the special element \( \varnothing \), which represents an expression that is not contained in a low slice. Intuitively, the low slice of a program is a slice that captures the effects on the low parts of the memory, and the public content or presence of messages over communication channels, created by executing the program. Hence, the side condition \( \text{lev}(e) = \mathbb{H} \Rightarrow \text{low-slice-of}(\text{prog}_1) = \text{low-slice-of}(\text{prog}_2) \) captures the requirement that the execution of the two branches of the if should have the same effects on the public parts of the memory and channel states.

We have the following theoretical results about the syntactic security type system.

**Theorem 3.** If \( \text{lev} \vdash_S \text{prog} \), then \( \text{lev} \vdash \text{prog} \).

**Corollary 1.** If \( \text{lev} \vdash_S \text{prog} \), then \( \text{LSec}(\text{prog}) \).

The theorem says that the fully syntactic security type system is sound wrt. the security type system presented in Fig. 1 of the paper. The corollary says that the fully syntactic security type system is sound wrt. local security. Hence, the fully syntactic security type system can be used as a replacement of the security type system presented in the paper to the benefit of fully operational type checking, and verification of local security.

Theorem 3 can be shown with a straightforward structural induction on \( \text{prog} \) once the following lemma is shown. Corollary 1 then follows immediately from Theorem 2 and Theorem 3.
Lemma 9. If \( \text{lev} \models \text{prog}_1 \), \( \text{lev} \models \text{prog}_2 \), and \( \text{low-slice-of}(\text{prog}_1) = \text{low-slice-of}(\text{prog}_2) \), then \( \text{prog}_1 \sim \text{prog}_2 \).

This lemma can be shown with a structural induction on \( \text{prog}_1 \), using the two following lemmas in the case for if. The proofs of these two lemmas are straightforward and omitted here.

Lemma 10. If \( \text{lev} \models \text{prog} \), \( \text{low-slice-of}(\text{prog}) = \text{skip} \), \( \sigma \times^{\text{low}} \text{asm-of}(\text{prog}) \), then for all \( \text{mem} \), there exist \( \text{mem}' \) and \( \sigma' \), such that \( \langle \langle \text{prog}; \text{mem} \rangle; \sigma \rangle \rightarrow \langle \langle \text{stop}; \text{mem}' \rangle; \sigma' \rangle \).

Lemma 11. If \( \text{lev} \models \text{prog} \), \( \text{low-slice-of}(\text{prog}) = \text{skip} \), and \( \langle \langle \text{prog}; \text{mem} \rangle; \sigma \rangle \rightarrow \langle \langle \text{prog}'; \text{mem}' \rangle; \sigma' \rangle \), then the following statements hold:
1. \( \forall x : \text{Var} : \text{mem}'(x) \neq \text{mem}(x) \Rightarrow \text{lev}(x) = \mathbb{H} \),
2. \( \forall ch \in \text{EncCh} : \sigma'(ch) \neq \sigma(ch) \Rightarrow ch \in \text{PriCh} \).
4 Typability of the Auction Example and Authentication Example

Type-Checking Using the Type System from the Paper. As outlined in the paper, the authentication example and the auction example can successfully be type-checked using the type system presented in Fig. 1 of the paper. While for the authentication example the semantic condition in the premise of the if-rule is not used in the type-checking, the auction example contains two high if-branches where the semantic condition is used. We provide the bisimulation relations that can be used to established the semantic condition for the two if-branches, respectively.

Client Program. With the symmetric closure of the following relation the conditional branching in \textit{auct-cl} can be type-checked.

\[
\{(\text{send}(\text{int}_1, \text{calc}(\text{min}, \text{thres})); \text{mem}_1, \langle \text{skip}; \text{mem}_2 \rangle) \mid \text{mem}_1 \equiv \text{L} \text{mem}_2 \}
\cup\{(\text{stop}; \text{mem}_1, \langle \text{stop}; \text{mem}_2 \rangle) \mid \text{mem}_1 \equiv \text{L} \text{mem}_2 \}
\]

Server Program. With the symmetric closure of the following relation the conditional branching in \textit{auct-srv} can be type-checked.

\[
\{(\text{send}(\text{pri}, \text{bid}); \text{mem}_1, \langle \text{skip}; \text{mem}_2 \rangle) \mid \text{mem}_1 \equiv \text{L} \text{mem}_2 \}
\cup\{(\text{stop}; \text{mem}_1, \langle \text{stop}; \text{mem}_2 \rangle) \mid \text{mem}_1 \equiv \text{L} \text{mem}_2 \}
\]

Type-Checking Using the Fully-Syntactic Type System of this Addendum. The fully-syntactic type system provided in Sect. 3 of this addendum allows one to type-check both the auction example and the authentication example without constructing bisimulation relations.

For the authentication example, the type-checking can be conducted analogously to the type-checking using the type system from the paper. This is because neither the client program nor the server program contains a high conditional branching. Hence, the semantic condition and also its syntactic replacement are not used in the type-checking.

For the auction example, the type-checking of each high conditional branching can be conducted by a comparison of the low-slices of the two branches. Since for each high conditional branching these two low-slices are equal, both the client program and the server program can be successfully typed. We give the computed low-slices below.

Client Program. For the client program, the relevant low-slices are the following:

\[
\text{low-slice-of}(\text{send}(\text{int}_1, \text{calc}(\text{min}, \text{thres}))) = \text{skip}
\]

\[
\text{low-slice-of}(\text{skip}) = \text{skip}
\]

Server Program. For the server program, the relevant low-slices are the following:

\[
\text{low-slice-of}(\text{send}(\text{pri}, \text{bid})) = \text{skip}
\]

\[
\text{low-slice-of}(\text{skip}) = \text{skip}
\]

It is worth mentioning that all the example programs from Sect. 2 of our paper \cite{1} are also typable using the fully syntactic security type system.

References

1. Ximeng Li, Heiko Mantel, and Markus Tasch. Taming message-passing communication in compositional reasoning about confidentiality. In 15th Asian Symposium on Programming Languages and Systems (APLAS), 2017. Accepted for publication.