A Core Calculus for Equational Proofs of Distributed Cryptographic Protocols: Technical Report

September 10, 2022

Abstract

We outline the proof that the exact equality of protocols in IPDL implies the existence of a protocol bisimulation.

1 Soundness for Reactions

Definition 1 (Reaction bisimulation)**.** *A* reaction bisimulation $\sim$ *is a binary relation on distributions on reactions* $\Delta;\ \cdot \vdash R : I \to \tau$ *satisfying the following conditions:*

- Closure under joint convex combinations*: We have*

$$\sum_{i:=1,\ldots,k} c_i\eta_i \ \sim \ \sum_{i:=1,\ldots,k} c_i\varepsilon_i$$

for convex coefficients $\sum_{i:=1,\ldots,k} c_i = 1$ *and distributions* $\eta_i \sim \varepsilon_i$ *for* $i := 1, \ldots, k$.

- Closure under input assignment*: For any distributions* $\eta \sim \varepsilon$*, channel* $i : \tau \in \Delta$*, and value* $v \in \{0,1\}^{[\![\tau]\!]}$*, we have* $\eta[\mathsf{read}\ i := \mathsf{val}\ v] \sim \varepsilon[\mathsf{read}\ i := \mathsf{val}\ v]$.

- Closure under evaluation*: For any distributions* $\eta \sim \varepsilon$*, if* $\eta \Downarrow \eta'$ *and* $\varepsilon \Downarrow \varepsilon'$*, then* $\eta' \sim \varepsilon'$.

- Valuation property*: For any distributions* $\eta \sim \varepsilon$*, there exists a joint convex combination*

$$\eta = \sum_{i:=1,\ldots,k} c_i\eta_i \ \sim \ \sum_{i:=1,\ldots,k} c_i\varepsilon_i = \varepsilon$$

such that for each $i := 1, \ldots, k$*, the distributions* $\eta_i \sim \varepsilon_i$ *have the same value* v*, or lack thereof.*

Lemma 1. *We have the following:*

- *The identity relation is a reaction bisimulation.*
- *The inverse of a reaction bisimulation is a reaction bisimulation.*
- *The composition of two reaction bisimulations is a reaction bisimulation.*

We now describe one canonical way to construct reaction bisimulations:

Definition 2. *Let* $\sim$ *be an arbitrary relation on distributions on reactions* $\Delta;\ \cdot \vdash R : I \to \tau$*. The* lifting $\sim_{\mathcal{L}}$ *is the closure of* $\sim$ *under joint convex combinations. Explicitly,* $\sim_{\mathcal{L}}$ *is defined by*

$$\sum_{i:=1,\ldots,k} c_i\eta_i \ \sim_{\mathcal{L}} \ \sum_{i:=1,\ldots,k} c_i\varepsilon_i$$

for convex coefficients $\sum_{i:=1,\ldots,k} c_i = 1$ *and distributions* $\eta_i \sim \varepsilon_i$ *for* $i := 1, \ldots, k$.

Lemma 2. *Let* $\sim$ *be a relation on distributions on reactions* $\Delta;\ \cdot \vdash R : I \to \tau$ *satisfying the following conditions:*

- Closure under input assignment*: For any distributions $\eta \sim \varepsilon$, channel $i : \tau \in \Delta$, and value $v \in \{0,1\}^{[\![\tau]\!]}$, we have $\eta[\mathsf{read}\ i := \mathsf{val}\ v] \sim \varepsilon[\mathsf{read}\ i := \mathsf{val}\ v]$.*

- Lifting closure under evaluation*: For any distributions $\eta \sim \varepsilon$, if $\eta \Downarrow \eta'$ and $\varepsilon \Downarrow \varepsilon'$, then $\eta' \sim_{\mathcal{L}} \varepsilon'$.*

- Valuation property*: For any distributions $\eta \sim \varepsilon$, there exists a joint convex combination*

$$\eta = \sum_{i:=1,\ldots,k} c_i \eta_i \ \sim \ \sum_{i:=1,\ldots,k} c_i \varepsilon_i = \varepsilon$$

  such that for each $i := 1, \ldots, k$, the distributions $\eta_i \sim \varepsilon_i$ have the same value v, or lack thereof.

Then the lifting $\sim_{\mathcal{L}}$ is a reaction bisimulation.

$$\frac{\mathsf{d}_1 : \sigma_1 \to \tau_1, \mathsf{d}_2 : \sigma_2 \to \tau_2 \in \Sigma \qquad \Gamma \vdash e_1 : \sigma_1 \qquad \Gamma \vdash e_2 : \sigma_2}{\begin{array}{l}\Delta;\ \Gamma \vdash \big(x_1 \leftarrow \mathsf{samp}\ (\mathsf{d}_1\ e_1);\ x_2 \leftarrow \mathsf{samp}\ (\mathsf{d}_2\ e_2);\ \mathsf{ret}\ (x_1, x_2)\big) = \\ \qquad \big(x_2 \leftarrow \mathsf{samp}\ (\mathsf{d}_2\ e_2);\ x_1 \leftarrow \mathsf{samp}\ (\mathsf{d}_1\ e_1);\ \mathsf{ret}\ (x_1, x_2)\big) : I \to \tau_1 \times \tau_2\end{array}}\ \textsc{exch-samp-samp}$$

$$\frac{\mathsf{d} : \sigma \to \tau_1 \in \Sigma \qquad \Gamma \vdash e : \sigma \qquad i : \tau_2 \in \Delta \qquad i \in I}{\begin{array}{l}\Delta;\ \Gamma \vdash \big(x_1 \leftarrow \mathsf{samp}\ (\mathsf{d}\ e);\ x_2 \leftarrow \mathsf{read}\ i;\ \mathsf{ret}\ (x_1, x_2)\big) = \\ \qquad \big(x_2 \leftarrow \mathsf{read}\ i;\ x_1 \leftarrow \mathsf{samp}\ (\mathsf{d}\ e);\ \mathsf{ret}\ (x_1, x_2)\big) : I \to \tau_1 \times \tau_2\end{array}}\ \textsc{exch-samp-read}$$

$$\frac{i_1 : \tau_1, i_2 : \tau_2 \in \Delta \qquad i_1, i_2 \in I}{\begin{array}{l}\Delta;\ \Gamma \vdash \big(x_1 \leftarrow \mathsf{read}\ i_1;\ x_2 \leftarrow \mathsf{read}\ i_2;\ \mathsf{ret}\ (x_1, x_2)\big) = \\ \qquad \big(x_2 \leftarrow \mathsf{read}\ i_2;\ x_1 \leftarrow \mathsf{read}\ i_1;\ \mathsf{ret}\ (x_1, x_2)\big) : I \to \tau_1 \times \tau_2\end{array}}\ \textsc{exch-read-read}$$

Figure 1: Alternative formulation of the EXCH rule.

Lemma 3 (Soundness of equality of reactions)**.** *If $\Delta;\ \Gamma \vdash R_1 = R_2 : I \to \tau$, then there is a reaction bisimulation $\sim$ such that for any valued substitution $\theta : \cdot \to \Gamma$, we have $1[\theta^\star(R_1)] \sim 1[\theta^\star(R_2)]$.*

Proof. We first replace the exchange rule EXCH by the three rules EXCH-SAMP-SAMP, EXCH-SAMP-READ, and EXCH-READ-READ in Figure 1; it is easy to see that this new set of rules is equivalent to the original one. □

2 Soundness for Protocols (Exact)

Definition 3 (Protocol bisimulation)**.** *A* protocol bisimulation $\sim$ *is a binary relation on distributions on protocols $\Delta \vdash P : I \to O$ satisfying the following conditions:*

- Closure under joint convex combinations*: We have*

$$\sum_{i:=1,\ldots,k} c_i \eta_i \ \sim \ \sum_{i:=1,\ldots,k} c_i \varepsilon_i$$

  for convex coefficients $\sum_{i:=1,\ldots,k} c_i = 1$ and distributions $\eta_i \sim \varepsilon_i$ for $i := 1, \ldots, k$.

- Closure under input assignment*: For any distributions $\eta \sim \varepsilon$, channel $i : \tau \in \Delta$, and value $v \in \{0,1\}^{[\![\tau]\!]}$, we have $\eta[\mathsf{read}\ i := \mathsf{val}\ v] \sim \varepsilon[\mathsf{read}\ i := \mathsf{val}\ v]$.*

- Closure under evaluation*: For any distributions $\eta \sim \varepsilon$, if $\eta \Downarrow \eta'$ and $\varepsilon \Downarrow \varepsilon'$, then $\eta' \sim \varepsilon'$.*

- Valuation property*: For any output channel o and distributions $\eta \sim \varepsilon$, there exists a joint convex combination*

$$\eta = \sum_{i:=1,\ldots,k} c_i \eta_i \ \sim \ \sum_{i:=1,\ldots,k} c_i \varepsilon_i = \varepsilon$$

  such that for each $i := 1, \ldots, k$, the distributions $\eta_i \sim \varepsilon_i$ have the same value v, or lack thereof, on o.

Lemma 4. *We have the following:*

- *The identity relation is a protocol bisimulation.*
- *The inverse of a protocol bisimulation is a protocol bisimulation.*
- *The composition of two protocol bisimulations is a protocol bisimulation.*

We now describe one canonical way to construct protocol bisimulations:

Definition 4. *Let $\sim$ be an arbitrary relation on distributions on protocols $\Delta \vdash P : I \to O$. The* lifting *$\sim_{\mathcal{L}}$ is the closure of $\sim$ under joint convex combinations. Explicitly, $\sim_{\mathcal{L}}$ is defined by*

$$\sum_{i:=1,\ldots,k} c_i \eta_i \sim_{\mathcal{L}} \sum_{i:=1,\ldots,k} c_i \varepsilon_i$$

for convex coefficients $\sum_{i:=1,\ldots,k} c_i = 1$ and distributions $\eta_i \sim \varepsilon_i$ for $i := 1, \ldots, k$.

Lemma 5. *Let $\sim$ be a relation on distributions on protocols $\Delta \vdash P : I \to O$ satisfying the following conditions:*

- Closure under input assignment*: For any distributions $\eta \sim \varepsilon$, channel $i : \tau \in \Delta$, and value $v \in \{0,1\}^{[\![\tau]\!]}$, we have $\eta[\mathsf{read}\ i := \mathsf{val}\ v] \sim \varepsilon[\mathsf{read}\ i := \mathsf{val}\ v]$.*
- Lifting closure under evaluation*: For any distributions $\eta \sim \varepsilon$, if $\eta \Downarrow \eta'$ and $\varepsilon \Downarrow \varepsilon'$, then $\eta' \sim_{\mathcal{L}} \varepsilon'$.*
- Valuation property*: For any output channel o and distributions $\eta \sim \varepsilon$, there exists a joint convex combination*

  $$\eta = \sum_{i:=1,\ldots,k} c_i \eta_i \sim \sum_{i:=1,\ldots,k} c_i \varepsilon_i = \varepsilon$$

  such that for each $i := 1, \ldots, k$, the distributions $\eta_i \sim \varepsilon_i$ have the same value v, or lack thereof, on o.

Then the lifting $\sim_{\mathcal{L}}$ is a reaction bisimulation.

$$\frac{o : \tau \in \Delta \qquad o \notin I \qquad b : \mathsf{Bool} \in \Delta \qquad \Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau \qquad \Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau}{\begin{array}{c}\Delta \vdash \big(\mathsf{new}\ l : \tau\ \mathsf{in}\ o := x \leftarrow \mathsf{read}\ b;\ \mathsf{if}\ x\ \mathsf{then}\ \mathsf{read}\ l\ \mathsf{else}\ S_2 \mid\mid l := x \leftarrow \mathsf{read}\ b;\ S_1\big) = \\ \big(o := x \leftarrow \mathsf{read}\ b;\ \mathsf{if}\ x\ \mathsf{then}\ S_1\ \mathsf{else}\ S_2\big) : I \to \{o\}\end{array}}\ \textsc{fold-if-left}$$

$$\frac{o : \tau \in \Delta \qquad o \notin I \qquad b : \mathsf{Bool} \in \Delta \qquad \Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau \qquad \Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau}{\begin{array}{c}\Delta \vdash \big(\mathsf{new}\ r : \tau\ \mathsf{in}\ o := x \leftarrow \mathsf{read}\ b;\ \mathsf{if}\ x\ \mathsf{then}\ S_1\ \mathsf{else}\ \mathsf{read}\ r \mid\mid r := x \leftarrow \mathsf{read}\ b;\ S_2\big) = \\ \big(o := x \leftarrow \mathsf{read}\ b;\ \mathsf{if}\ x\ \mathsf{then}\ S_1\ \mathsf{else}\ S_2\big) : I \to \{o\}\end{array}}\ \textsc{fold-if-right}$$

Figure 2: Alternative formulation of the FOLD-IF-LEFT and FOLD-IF-RIGHT rules.

Lemma 6 (Soundness of equality of protocols)**.** *If the ambient exact IPDL theory is sound, and $\Delta \vdash P_1 = P_2 : I \to O$, then there is a protocol bisimulation $\sim$ such that $1[P_1] \sim 1[P_2]$.*

Proof. We first replace the rules FOLD-IF-LEFT and FOLD-IF-RIGHT by their equivalent formulation in Figure 2. We now proceed by induction on this alternative set of rules for exact protocol equality.

- REFL: Our desired bisimulation is the identity relation.
- SYM: Our desired bisimulation is the inverse of the bisimulation obtained from the premise $\Delta \vdash P_1 = P_2 : I \to O$.
- TRANS: Our desired bisimulation is the composition of the two bisimulations obtained from the two premises $\Delta \vdash P_1 = P_2 : I \to O$ and $\Delta \vdash P_2 = P_3 : I \to O$.

- AXIOM: The desired bisimulation exists by assumption.
- EMBED: Let $\sim$ be the bisimulation obtained from the premise $\Delta \vdash P_1 = P_2 : I \to O$. Our desired bisimulation $\sim_\theta$ is defined by
  - $\theta^\star(\eta) \sim_\theta \theta^\star(\eta')$ if $\eta \sim \eta'$
- CONG-REACT: Let $\sim$ be the (reaction) bisimulation obtained from the premise $\Delta;\ \cdot \vdash R = R' : I \cup \{o\} \to \tau$. Our desired bisimulation is the lifting of the relation $\sim_{\mathsf{rea}}$ defined by
  - $(o := \eta) \sim_{\mathsf{rea}} (o := \eta')$ if $\eta \sim \eta'$
  - $1[o := v] \sim_{\mathsf{rea}} 1[o := v]$ for a value $v \in \{0,1\}^{[\![\tau]\!]}$
- CONG-COMP-LEFT: Let $\sim$ be the bisimulation obtained from the premise $\Delta \vdash P = P' : I \cup O_2 \to O_1$. Our desired bisimulation is the lifting of the relation $\sim_{\mathsf{par}}$ defined by
  - $(\eta \mid\mid Q) \sim_{\mathsf{par}} (\eta' \mid\mid Q)$ for $\eta \sim \eta'$ and a protocol $\Delta \vdash Q : I \cup O_1 \to O_2$
- CONG-NEW: Let $\sim$ be the bisimulation obtained from the premise $\Delta, o : \tau \vdash P = P' : I \to O \cup \{o\}$. Our desired bisimulation $\sim_{\mathsf{new}}$ is defined by
  - $(\mathsf{new}\ o : \tau\ \mathsf{in}\ \eta) \sim_{\mathsf{new}} (\mathsf{new}\ o : \tau\ \mathsf{in}\ \eta')$ if $\eta \sim \eta'$
- COMP-COMM: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[P_1 \mid\mid P_2] \sim 1[P_2 \mid\mid P_1]$
    for protocols $\Delta \vdash P_1 : I \cup O_2 \to O_1$ and $\Delta \vdash P_2 : I \cup O_1 \to O_2$
- COMP-ASSOC: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[(P_1 \mid\mid P_2) \mid\mid P_3] \sim 1[P_1 \mid\mid (P_2 \mid\mid P_3)]$
    for protocols $\Delta \vdash P_1 : I \cup O_2 \cup O_3 \to O_1$ and $\Delta \vdash P_2 : I \cup O_1 \cup O_3 \to O_2$ and $\Delta \vdash P_3 : I \cup O_1 \cup O_2 \to O_3$
- NEW-EXCH: The desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1\big[\mathsf{new}\ o_1 : \tau_1\ \mathsf{in}\ \mathsf{new}\ o_2 : \tau_2\ \mathsf{in}\ P\big] \sim 1\big[\mathsf{new}\ o_2 : \tau_2\ \mathsf{in}\ \mathsf{new}\ o_1 : \tau_1\ \mathsf{in}\ P\big]$
    for a protocol $\Delta, o_1 : \tau_1, o_2 : \tau_2 \vdash P : I \to O \cup \{o_1, o_2\}$
- COMP-NEW: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1\big[P \mid\mid (\mathsf{new}\ o : \tau\ \mathsf{in}\ Q)\big] \sim 1\big[\mathsf{new}\ o : \tau\ \mathsf{in}\ (P \mid\mid Q)\big]$
    for protocols $\Delta \vdash P : I \cup O_2 \to O_1$ and $\Delta, o : \tau \vdash Q : I \cup O_1 \to O_2 \cup \{o\}$
- ABSORB-LEFT: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[P \mid\mid Q] \sim 1[P]$ for protocols $\Delta \vdash P : I \to O$ and $\Delta \vdash Q : I \cup O \to \varnothing$
- DIVERGE: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[o := x : \tau \leftarrow \mathsf{read}\ o;\ R] \sim 1[o := \mathsf{read}\ o]$ for a reaction $\Delta;\ \cdot \vdash R : I \cup \{o\} \to \tau$
- FOLD-IF-LEFT: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1\big[\mathsf{new}\ l : \tau\ \mathsf{in}\ o := x \leftarrow \mathsf{read}\ b;\ \mathsf{if}\ x\ \mathsf{then}\ \mathsf{read}\ l\ \mathsf{else}\ S_2 \mid\mid l := x \leftarrow \mathsf{read}\ b;\ S_1\big] \sim$
    $1[o := x \leftarrow \mathsf{read}\ b;\ \mathsf{if}\ x\ \mathsf{then}\ S_1\ \mathsf{else}\ S_2]$ for reactions $\Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau$ and $\Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau$
  - $1\big[\mathsf{new}\ l : \tau\ \mathsf{in}\ o := x \leftarrow \mathsf{val}\ v;\ \mathsf{if}\ x\ \mathsf{then}\ \mathsf{read}\ l\ \mathsf{else}\ S_2 \mid\mid l := x \leftarrow \mathsf{val}\ v;\ S_1\big] \sim$
    $1[o := x \leftarrow \mathsf{val}\ v;\ \mathsf{if}\ x\ \mathsf{then}\ S_1\ \mathsf{else}\ S_2]$ for a value $v \in \{0,1\}$ and reactions $\Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau$ and $\Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau$
  - $1[\mathsf{new}\ l : \tau\ \mathsf{in}\ o := \mathsf{read}\ l \mid\mid l := S_1] \sim 1[o := S_1]$ for a reaction $\Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau$

– $1\big[\textsf{new } l : \tau \textsf{ in } o := v_1 \mid\mid l := v_1\big] \sim 1[o := v_1]$ for a value $v_1 \in \{0,1\}^{[\![\tau]\!]}$
– $1\big[\textsf{new } l : \tau \textsf{ in } o := S_2 \mid\mid l := S_1\big] \sim$
$1[o := S_2]$ for reactions $\Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau$ and $\Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau$
– $1\big[\textsf{new } l : \tau \textsf{ in } o := S_2 \mid\mid l := v_1\big] \sim$
$1[o := S_2]$ for a value $v_1 \in \{0,1\}^{[\![\tau]\!]}$ and a reaction $\Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau$
– $1\big[\textsf{new } l : \tau \textsf{ in } o := v_2 \mid\mid l := S_1\big] \sim$
$1[o := v_2]$ for a reaction $\Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau$ and a value $v_2 \in \{0,1\}^{[\![\tau]\!]}$
– $1\big[\textsf{new } l : \tau \textsf{ in } o := v_2 \mid\mid l := v_1\big] \sim$
$1[o := v_2]$ for values $v_1, v_2 \in \{0,1\}^{[\![\tau]\!]}$

- FOLD-IF-RIGHT: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  – $1\big[\textsf{new } r : \tau \textsf{ in } o := x \leftarrow \textsf{read } b;\ \textsf{if } x \textsf{ then } S_1 \textsf{ else read } r \mid\mid r := x \leftarrow \textsf{read } b;\ S_2\big] \sim$
  $1[o := x \leftarrow \textsf{read } b;\ \textsf{if } x \textsf{ then } S_1 \textsf{ else } S_2]$ for reactions $\Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau$ and $\Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau$
  – $1\big[\textsf{new } r : \tau \textsf{ in } o := x \leftarrow \textsf{val } v;\ \textsf{if } x \textsf{ then } S_1 \textsf{ else read } r \mid\mid r := x \leftarrow \textsf{val } v;\ S_2\big] \sim$
  $1[o := x \leftarrow \textsf{val } v;\ \textsf{if } x \textsf{ then } S_1 \textsf{ else } S_2]$ for a value $v \in \{0,1\}$ and reactions $\Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau$ and $\Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau$
  – $1\big[\textsf{new } r : \tau \textsf{ in } o := S_1 \mid\mid r := S_2\big] \sim$
  $1[o := S_1]$ for reactions $\Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau$ and $\Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau$
  – $1\big[\textsf{new } r : \tau \textsf{ in } o := S_1 \mid\mid r := v_2\big] \sim$
  $1[o := S_1]$ for a reaction $\Delta;\ \cdot \vdash S_1 : I \cup \{o\} \to \tau$ and a value $v_2 \in \{0,1\}^{[\![\tau]\!]}$
  – $1\big[\textsf{new } r : \tau \textsf{ in } o := v_1 \mid\mid r := S_2\big] \sim$
  $1[o := v_1]$ for a value $v_1 \in \{0,1\}^{[\![\tau]\!]}$ and a reaction $\Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau$
  – $1\big[\textsf{new } r : \tau \textsf{ in } o := v_1 \mid\mid r := v_2\big] \sim$
  $1[o := v_1]$ for values $v_1, v_2 \in \{0,1\}^{[\![\tau]\!]}$
  – $1\big[\textsf{new } r : \tau \textsf{ in } o := \textsf{read } r \mid\mid r := S_2\big] \sim$
  $1[o := S_2]$ for a reaction $\Delta;\ \cdot \vdash S_2 : I \cup \{o\} \to \tau$
  – $1\big[\textsf{new } r : \tau \textsf{ in } o := v_2 \mid\mid r := v_2\big] \sim$
  $1[o := v_2]$ for a value $v_2 \in \{0,1\}^{[\![\tau]\!]}$
- FOLD-BIND: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  – $1\big[\textsf{new } c : \sigma \textsf{ in } o := x : \sigma \leftarrow \textsf{read } c;\ S \mid\mid c := R\big] \sim 1[o := x : \sigma \leftarrow R;\ S]$
  for reactions $\Delta;\ \cdot \vdash R : I \cup \{o\} \to \tau$ and $\Delta;\ x : \sigma \vdash S : I \cup \{o\} \to \tau$
  – $1\big[\textsf{new } c : \sigma \textsf{ in } o := S \mid\mid c := u\big] \sim 1[o := S]$
  for a value $u \in \{0,1\}^{[\![\sigma]\!]}$ and a reaction $\Delta;\ \cdot \vdash S : I \cup \{o\} \to \tau$
  – $1[\textsf{new } c : \sigma \textsf{ in } o := v \mid\mid c := u] \sim 1[o := v]$ for values $u \in \{0,1\}^{[\![\sigma]\!]}$ and $v \in \{0,1\}^{[\![\tau]\!]}$
- SUBSUME: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  – $1\big[o_1 := x_0 : \tau_0 \leftarrow \textsf{read } o_0;\ R_1 \mid\mid o_2 := x_0 : \tau_0 \leftarrow \textsf{read } o_0;\ x_1 : \tau_1 \leftarrow \textsf{read } o_1;\ R_2\big] \sim$
  $1\big[o_1 := x_0 : \tau_0 \leftarrow \textsf{read } o_0;\ R_1 \mid\mid o_2 := x_1 : \tau_1 \leftarrow \textsf{read } o_1;\ R_2\big]$
  for reactions $\Delta;\ x_0 : \tau_0 \vdash R_1 : I \cup \{o_1, o_2\} \to \tau_1$ and $\Delta;\ x_1 : \tau_1 \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$
  – $1\big[o_1 := x_0 : \tau_0 \leftarrow \textsf{val } v_0;\ R_1 \mid\mid o_2 := x_0 : \tau_0 \leftarrow \textsf{val } v_0;\ x_1 : \tau_1 \leftarrow \textsf{read } o_1;\ R_2\big] \sim$
  $1\big[o_1 := x_0 : \tau_0 \leftarrow \textsf{val } v_0;\ R_1 \mid\mid o_2 := x_1 : \tau_1 \leftarrow \textsf{read } o_1;\ R_2\big]$
  for reactions $\Delta;\ x_0 : \tau_0 \vdash R_1 : I \cup \{o_1, o_2\} \to \tau_1$ and $\Delta;\ x_1 : \tau_1 \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$, and a value $v_0 \in \{0,1\}^{[\![\tau_0]\!]}$
  – $1\big[o_1 := R_1 \mid\mid o_2 := x_1 : \tau_1 \leftarrow \textsf{read } o_1;\ R_2\big] \sim 1\big[o_1 := R_1 \mid\mid o_2 := x_1 : \tau_1 \leftarrow \textsf{read } o_1;\ R_2\big]$
  for reactions $\Delta;\ \cdot \vdash R_1 : I \cup \{o_1, o_2\} \to \tau_1$ and $\Delta;\ x_1 : \tau_1 \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$

- $1\big[o_1 := v_1 \mid\mid o_2 := R_2\big] \sim 1\big[o_1 := v_1 \mid\mid o_2 := R_2\big]$
  for a value $v_1 \in \{0,1\}^{[\![\tau_1]\!]}$ and a reaction $\Delta;\ \cdot \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$
- $1\big[o_1 := v_1 \mid\mid o_2 := v_2\big] \sim 1\big[o_1 := v_1 \mid\mid o_2 := v_2\big]$
  for values $v_1 \in \{0,1\}^{[\![\tau_1]\!]}$ and $v_2 \in \{0,1\}^{[\![\tau_2]\!]}$

- SUBST: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1\big[o_1 := R_1 \mid\mid o_2 := x_1 : \tau_1 \leftarrow \mathsf{read}\ o_1;\ R_2\big] \sim 1\big[o_1 := R_1 \mid\mid o_2 := x_1 : \tau_1 \leftarrow R_1;\ R_2\big]$
    for reactions $\Delta;\ \cdot \vdash R_1 : I \cup \{o_1, o_2\} \to \tau_1$ and $\Delta;\ x_1 : \tau_1 \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$
  - $1\big[o_1 := v_1 \mid\mid o_2 := R_2\big] \sim 1\big[o_1 := v_1 \mid\mid o_2 := R_2\big]$
    for a value $v_1 \in \{0,1\}^{[\![\tau_1]\!]}$ and a reaction $\Delta;\ \cdot \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$
  - $1\big[o_1 := v_1 \mid\mid o_2 := v_2\big] \sim 1\big[o_1 := v_1 \mid\mid o_2 := v_2\big]$
    for values $v_1 \in \{0,1\}^{[\![\tau_1]\!]}$ and $v_2 \in \{0,1\}^{[\![\tau_2]\!]}$

- UNUSED: Let $\sim$ be the (reaction) bisimulation obtained from the premise $\Delta;\ \cdot \vdash (x_1 : \tau_1 \leftarrow R_1;\ R_2) = R_2 : I \cup \{o_1, o_2\} \to \tau_2$. Our desired bisimulation is the lifting of the relation $\sim_{\mathsf{drop}}$ defined by
  - $\big(o_1 := \eta_1 \mid\mid o_2 := x_1 \leftarrow \mathsf{read}\ o_1;\ R_2\big) \sim_{\mathsf{drop}} \big(o_1 := \eta_1 \mid\mid o_2 := \eta_2\big)$ for
    * a distribution η_1 on reactions $\Delta;\ \cdot \vdash R_1 : I \cup \{o_1, o_2\} \to \tau_1$
    * a distribution η_2 on reactions $\Delta;\ \cdot \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$
    * computed distributions ε, μ on reactions $\Delta;\ \cdot \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$
    * a reaction $\Delta;\ \cdot \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$

    such that $R_2 \Downarrow \varepsilon$, $\eta_2 \Downarrow \varepsilon$, $(x_1 : \tau_1 \leftarrow \eta_1;\ R_2) \Downarrow \mu$, and $\mu \sim \varepsilon$
  - $\big(o_1 := \eta_1 \mid\mid o_2 := x_1 \leftarrow \mathsf{read}\ o_1;\ R_2\big) \sim_{\mathsf{drop}} \big(o_1 := \eta_1 \mid\mid o_2 := \eta_2\big)$ for
    * distributions $\eta_1, \bar{\eta}_1$ on reactions $\Delta;\ \cdot \vdash R_1 : I \cup \{o_1, o_2\} \to \tau_1$
    * a distribution η_2 on reactions $\Delta;\ \cdot \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$
    * computed distributions ε, μ on reactions $\Delta;\ \cdot \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$
    * a reaction $\Delta;\ \cdot \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$

    such that $R_2 \Downarrow \varepsilon$, $\eta_2 \Downarrow \varepsilon$, $(x_1 : \tau_1 \leftarrow c\eta_1 + \bar{c}\bar{\eta}_1;\ R_2) \Downarrow \mu$ for some $c + \bar{c} = 1$, and $\mu \sim \varepsilon$
  - $(o_1 := v_1 \mid\mid o_2 := R_2) \sim_{\mathsf{drop}} (o_1 := v_1 \mid\mid o_2 := R_2)$
    for a value $v_1 \in \{0,1\}^{[\![\tau_1]\!]}$ and reaction $\Delta;\ \cdot \vdash R_2 : I \cup \{o_1, o_2\} \to \tau_2$
  - $(o_1 := v_1 \mid\mid o_2 := v_2) \sim_{\mathsf{drop}} (o_1 := v_1 \mid\mid o_2 := v_2)$
    for values $v_1 \in \{0,1\}^{[\![\tau_1]\!]}$ and $v_2 \in \{0,1\}^{[\![\tau_2]\!]}$

$\square$