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

September 10, 2022

1 Soundness for Reactions

Definition 1 (Reaction bisimulation)**.** *A* reaction bisimulation $\sim$ *is a binary relation on distributions on reactions* $\Delta;\ \cdot \vdash R : I \to A$ *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 any 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* $\eta' \sim \mu'$.
- 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 bisimulations:

Definition 2. *Let* $\sim$ *be an arbitrary binary 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 any 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 binary 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 $\eta' \sim_{\mathcal{L}} \mu'$.*
- 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.

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 **??**; it is easy to see that this new set of rules is equivalent to the original one. We now proceed by induction on the alternative set of rules for reaction equality.

- REFL: Our desired bisimulation is the identity relation.
- SYM: Our desired bisimulation is the inverse of the bisimulation obtained inductively from the premise $\Delta;\ \Gamma \vdash R_1 = R_2 : \tau$.
- TRANS: Our desired bisimulation is the composition of the two bisimulations obtained inductively from the two premises $\Delta;\ \Gamma \vdash R_1 = R_2 : \tau$ and $\Delta;\ \Gamma \vdash R_2 = R_3 : \tau$.
- CONG-RET: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[\mathsf{ret}\ (e)] \sim 1[\mathsf{ret}\ (e')]$ for any expressions e, e' evaluating to the same value
  - $1[\mathsf{val}\ v] \sim 1[\mathsf{val}\ v]$
- CONG-SAMP: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[\mathsf{samp}\ (d)] \sim 1[\mathsf{samp}\ (d')]$ for any distributions d, d' evaluating to the same distribution
  - $1[\mathsf{val}\ v] \sim 1[\mathsf{val}\ v]$
- CONG-BRANCH: Let $\sim_1$ and $\sim_2$ be the two bisimulations obtained inductively from the two premises $\Delta;\ \Gamma \vdash R_1 = R_1' : \tau$ and $\Delta;\ \Gamma \vdash R_2 = R_2' : \tau$. Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1\big[\mathsf{if}\ e\ \mathsf{then}\ R_1\ \mathsf{else}\ R_2\big] \sim 1\big[\mathsf{if}\ e'\ \mathsf{then}\ R_1'\ \mathsf{else}\ R_2'\big]$ for any messages e, e' such that $\cdot \vdash e = e' : \mathsf{Bool}$, and any reactions R_1, R_1' and R_2, R_2' such that $1[R_1] \sim_1 1[R_1']$ and $1[R_2] \sim_2 1[R_2']$
  - $\eta \sim \eta'$ for $\eta \sim_1 \eta'$
  - $\eta \sim \eta'$ for $\eta \sim_2 \eta'$
- CONG-BIND: Let $\sim_1$ and $\sim_2$ be the two bisimulations obtained inductively from the two premises $\Delta;\ \Gamma \vdash R = R' : \tau_1$ and $\Delta;\ \Gamma, x : \tau_1 \vdash S = S' : \tau_2$. Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $(x \leftarrow \eta;\ S) \sim (x \leftarrow \eta';\ S')$ for any $\eta \sim_1 \eta'$, and any reactions $\Delta;\ x : \tau_1 \vdash S : \tau_2$ and $\Delta;\ x : \tau_1 \vdash S' : \tau_2$ such that for any e we have $1[S(x := e)] \sim_2 1[S'(x := e)]$
- BRANCH-LEFT: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[\mathsf{if}\ \mathsf{true}\ \mathsf{then}\ R_1\ \mathsf{else}\ R_2] \sim 1[R_1]$ for any reactions R_1, R_2
  - $\eta \sim \eta$ for any η
- BRANCH-RIGHT: Our desired bisimulation is the lifting of the relation $\sim$ defined by

$$\frac{\Gamma \vdash d_1 : \sigma_1 \qquad \Gamma \vdash d_2 : \sigma_2}{\begin{array}{l}\Delta;\ \Gamma \vdash \big(x_1 : \sigma_1 \leftarrow \mathsf{samp}\ (d_1);\ x_2 : \sigma_2 \leftarrow \mathsf{samp}\ (d_2);\ \mathsf{ret}\ ((x_1, x_2))\big) = \\ \qquad \big(x_2 : \sigma_2 \leftarrow \mathsf{samp}\ (d_2);\ x_1 : \sigma_1 \leftarrow \mathsf{samp}\ (d_1);\ \mathsf{ret}\ ((x_1, x_2))\big) : I \to \sigma_1 \times \sigma_2\end{array}} \textsc{exch-samp-samp}$$

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

$$\frac{i_1 : \sigma_1, i_2 : \sigma_2 \in \Delta \qquad i_1, i_2 \in I}{\begin{array}{l}\Delta;\ \Gamma \vdash_\Sigma \big(x_1 : \sigma_1 \leftarrow \mathsf{read}\ i_1;\ x_2 : \sigma_2 \leftarrow \mathsf{read}\ i_2;\ \mathsf{ret}\ ((x_1, x_2))\big) = \\ \qquad \big(x_2 : \sigma_2 \leftarrow \mathsf{read}\ i_2;\ x_1 : \sigma_1 \leftarrow \mathsf{read}\ i_1;\ \mathsf{ret}\ ((x_1, x_2))\big) : I \to \sigma_1 \times \sigma_2\end{array}} \textsc{exch-read-read}$$

Figure 1: Alternative formulation of the EXCH rule.

  - $1[\mathsf{if\ false\ then}\ R_1\ \mathsf{else}\ R_2] \sim 1[R_2]$ for any reactions R_1, R_2
  - $\eta \sim \eta$ for any η

- BRANCH-EXT: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[R(x := e)] \sim 1\big[\mathsf{if}\ e\ \mathsf{then}\ R(x := \mathsf{true})\ \mathsf{else}\ R(x := \mathsf{false})\big]$ for any expression e and reaction $\Delta;\ x : \mathsf{Bool} \vdash R : \tau$
  - $\eta \sim \eta'$ if $\eta \sim_{\mathsf{val}} \eta'$

- RET-BIND: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[x \leftarrow \mathsf{ret}\ (e);\ R] \sim 1[R(x := e)]$ for any expression e and reaction $\Delta;\ x : \tau_1 \vdash R : \tau_2$
  - $\eta \sim \eta'$ if $\eta \sim_{\mathsf{val}} \eta'$

- BIND-RET: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[x \leftarrow R;\ \mathsf{ret}\ (x)] \sim 1[R]$ for any reaction R
  - $1[\mathsf{val}\ v] \sim 1[\mathsf{val}\ v]$

- BIND-BIND: Our desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1\big[x_2 \leftarrow (x_1 \leftarrow R_1;\ R_2);\ R_3\big] = 1\big[x_1 \leftarrow R_1;\ (x_2 \leftarrow R_2;\ R_3)\big]$ for any reactions R_1, R_2, R_3
  - $\eta \sim \eta$ for any η

$\square$

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 any 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* $\eta' \sim \mu'$*.*

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

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

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

- Valuation property*: For any output channel o and 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 on the channel 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 binary 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 any 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 binary 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 $\eta'\sim_{\mathcal{L}}\mu'$.*
- Valuation property*: For any output channel o and 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, on the channel o.

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

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 $1[P_1]\sim1[P_2]$.*

Proof. We first replace the rules FOLD-IF-LEFT and FOLD-IF-RIGHT by the equivalent formulation in Figure 2. We subsequently proceed by induction on the derivation $\Delta \vdash P_1 = P_2 : I \to O$ using this alternative system of protocol equality rules.

- REFL: Our desired bisimulation is the identity relation.
- SYM: Our desired bisimulation is the inverse of the bisimulation obtained inductively from the premise $\Delta \vdash P_1 = P_2 : I \to O$.
- TRANS: Our desired bisimulation is the composition of the two bisimulations obtained inductively 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 inductively from the premise $\Delta \vdash P_1 = P_2 : I \to O$. The 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 $\Delta;\ \cdot \vdash R = R' : I \cup \{o\} \to \tau$. The desired bisimulation is the lifting of the relation $\sim_{:=}$ defined by
  - $(o := \eta) \sim_{:=} (o := \eta')$ for $\eta \sim \eta'$
  - $1[o := v] \sim_{:=} 1[o := v]$
- CONG-COMP-LEFT: Let $\sim$ be the bisimulation obtained inductively from the premise $\Delta \vdash P = P' : I \cup O_2 \to O_1$. The desired bisimulation is the lifting of the relation $\sim_{||}$ defined by
  - $\eta \mid\mid Q \sim_{||} \eta' \mid\mid Q$ for $\eta \sim \eta'$ and a protocol Q
- CONG-NEW: Let $\sim$ be the bisimulation obtained inductively from the premise $\Delta, o : \tau \vdash P = P' : I \to O \cup \{o\}$. The desired bisimulation $\sim_{\mathsf{new}}$ is defined by
  - $\mathsf{new}\ o : \tau\ \mathsf{in}\ \eta \sim_{\mathsf{new}} \mathsf{new}\ o : \tau\ \mathsf{in}\ \eta'$ for $\eta \sim \eta'$
- COMP-COMM: The desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[P_1 \mid\mid P_2] = 1[P_2 \mid\mid P_1]$ for protocols P_1, P_2
- COMP-ASSOC: The desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[(P_1 \mid\mid P_2) \mid\mid P_3] = 1[P_1 \mid\mid (P_2 \mid\mid P_3)]$ for protocols P_1, P_2, P_3
- NEW-EXCH: The desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1\big[\mathsf{new}\ o_1 : \tau_1\ \mathsf{in}\ \mathsf{new}\ o_2 : \tau_2\ \mathsf{in}\ P\big] = 1\big[\mathsf{new}\ o_2 : \tau_2\ \mathsf{in}\ \mathsf{new}\ o_1 : \tau_1\ \mathsf{in}\ P\big]$ for a protocol P
- COMP-NEW: The desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1\big[P \mid\mid (\mathsf{new}\ o : \tau\ \mathsf{in}\ Q)\big] = 1\big[\mathsf{new}\ o : \tau\ \mathsf{in}\ (P \mid\mid Q)\big]$ for protocols P and Q
- ABSORB-LEFT: The desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[P \mid\mid Q] = 1[P]$ for protocols P and Q
- DIVERGE: The desired bisimulation is the lifting of the relation $\sim$ defined by
  - $1[o := x : \tau \leftarrow \mathsf{read}\ o;\ R] = 1[o := \mathsf{read}\ o]$ for a reaction R

□