A Compositional and Complete approach to Verifying Privacy using the Applied Pi-calculus

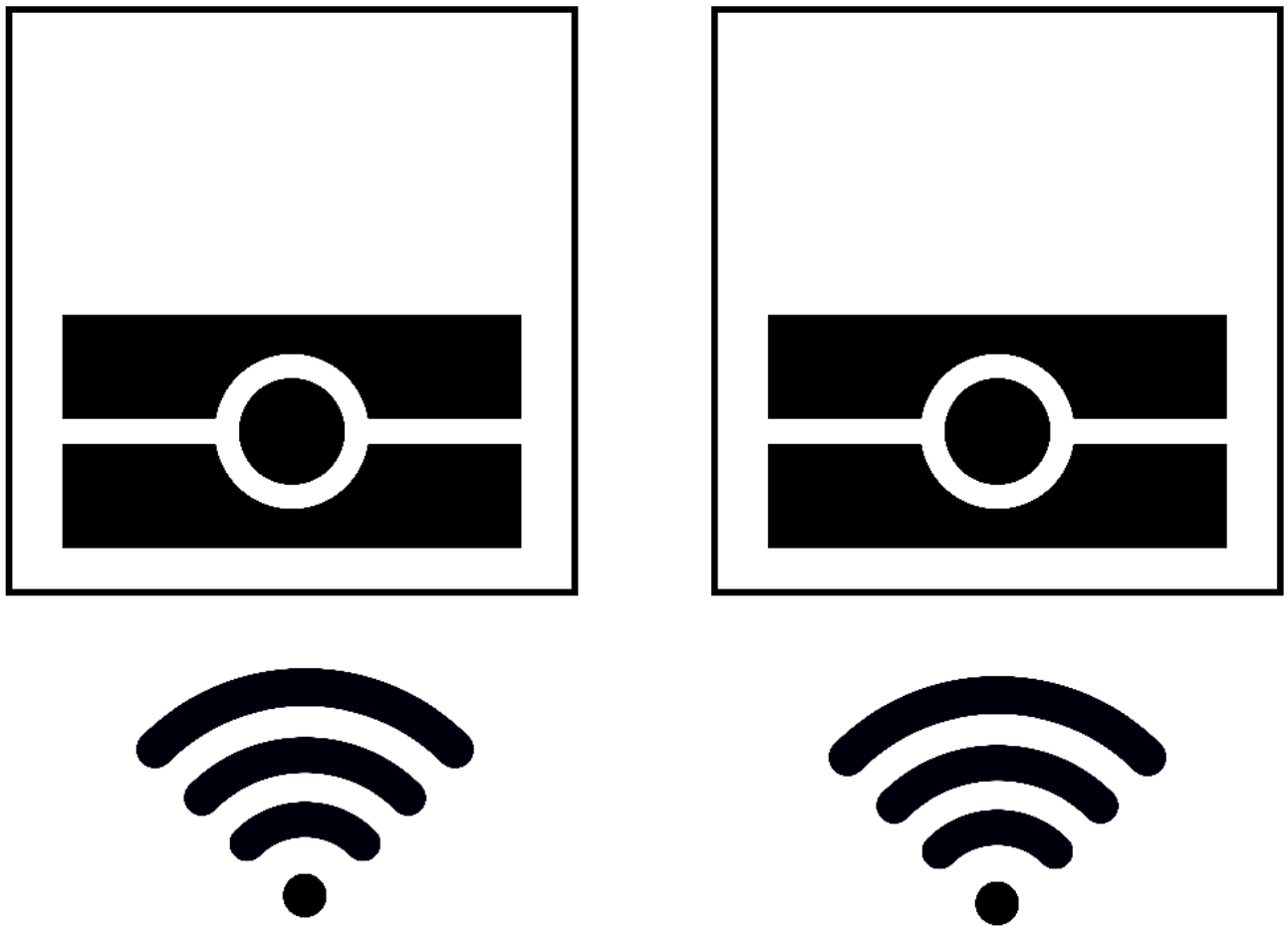
IRISA Seminar

Ross Horne

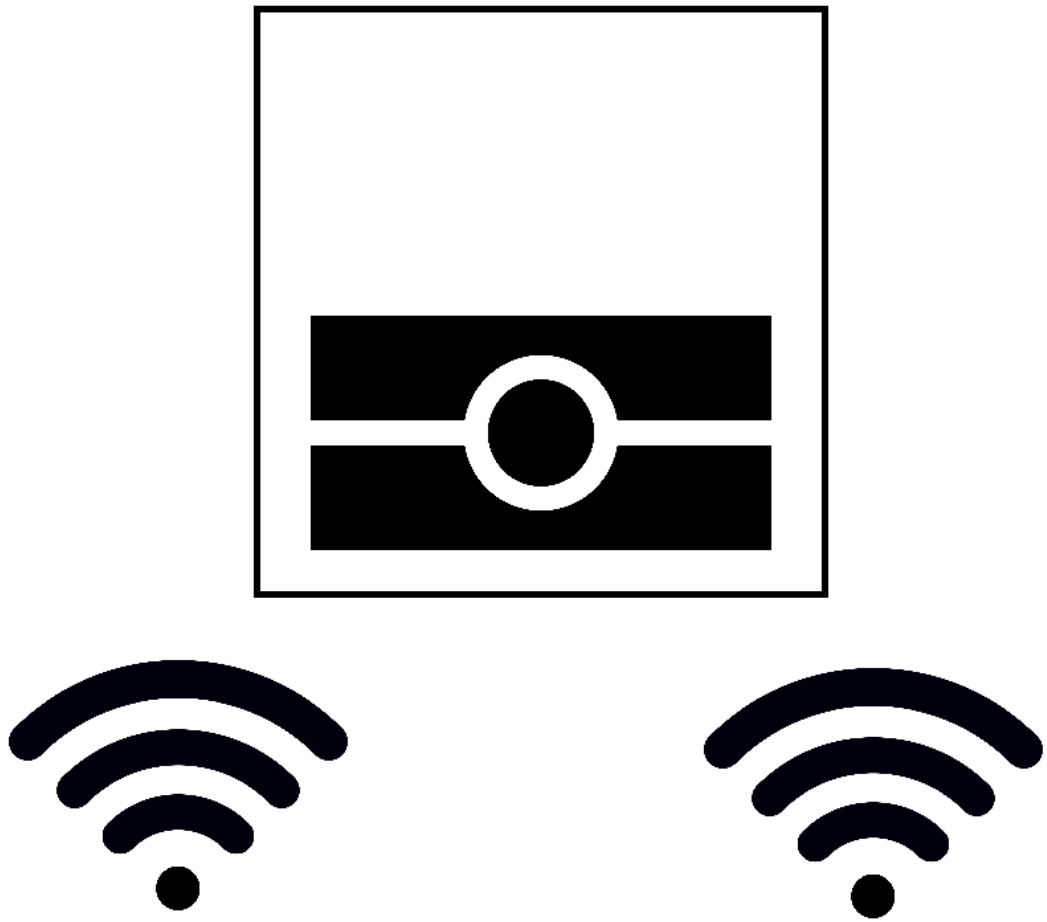
Security and Trust of Software Systems (SaToSS), Computer Science Research Unit, University of Luxembourg

8 February 2019

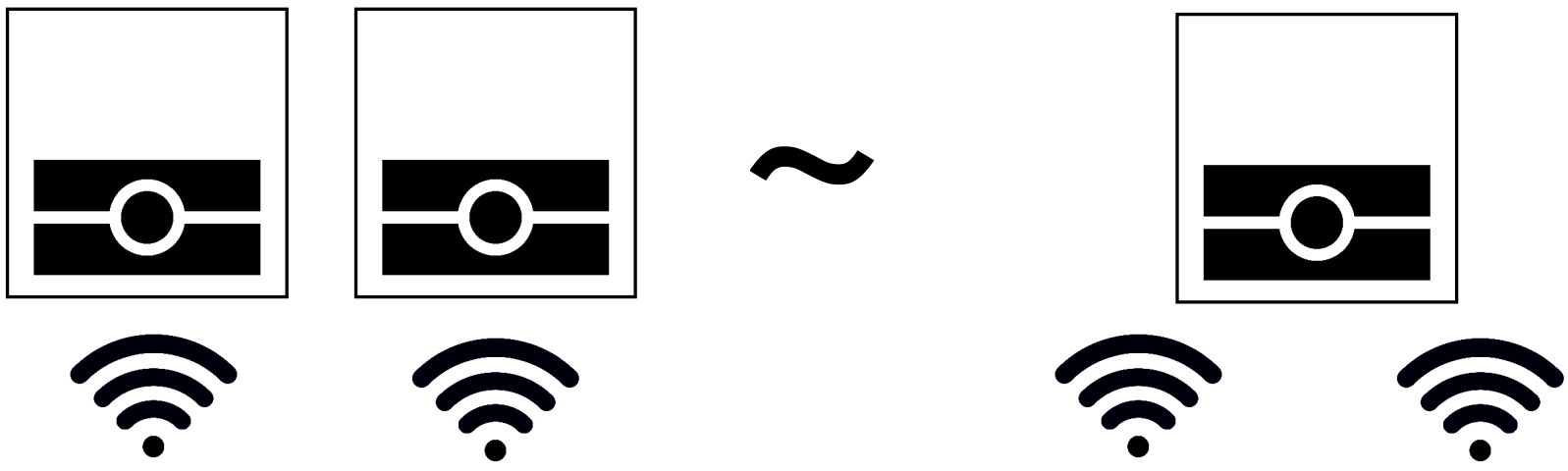
Specification: Every reader session is with a new e-passport



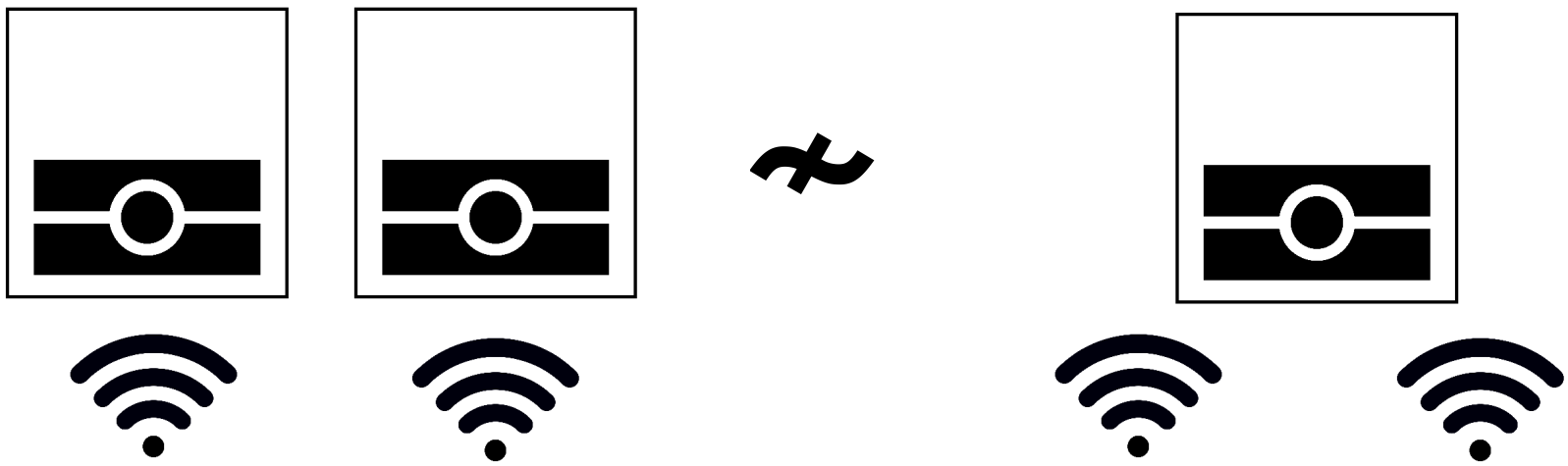
System: An e-passport can be used in multiple sessions



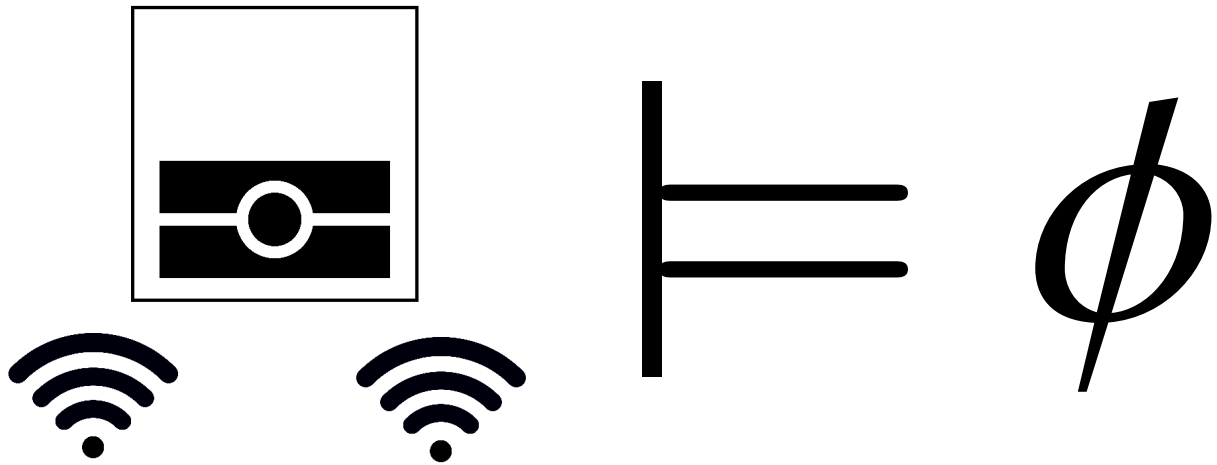
Unlinkability: Attacker cannot tell if same e-passport used twice

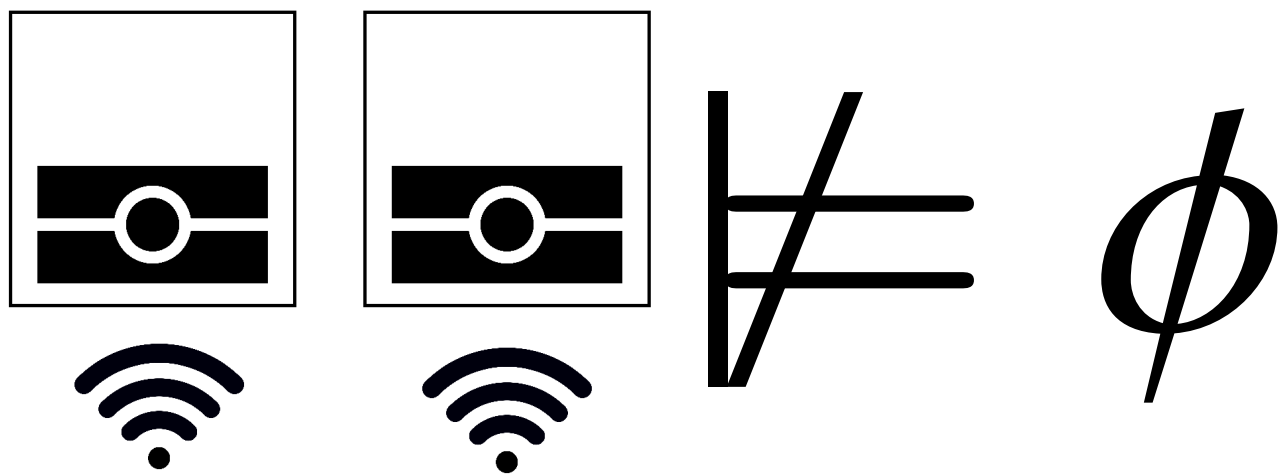


Attack: Attacker can tell if same e-passport used twice

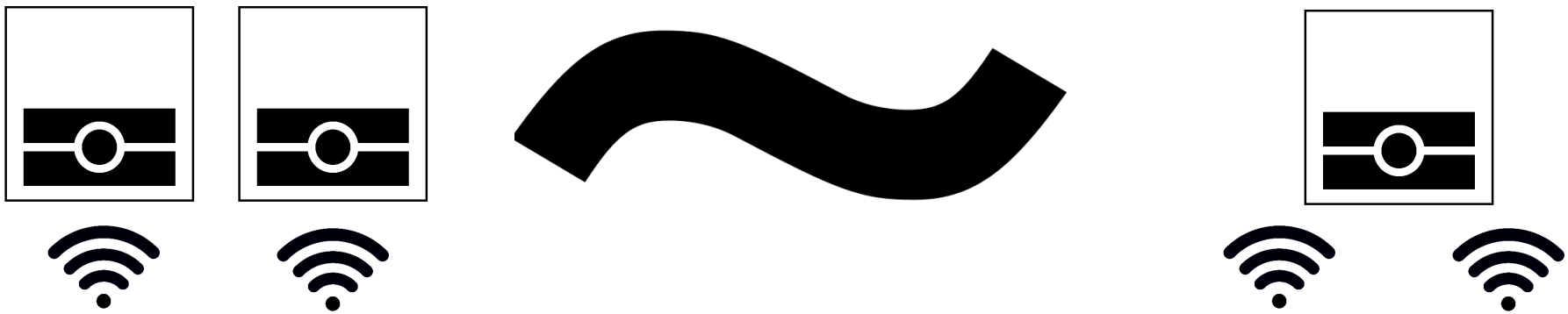


Distinguishing formula: describes an attack whenever one exists





Does it matter which notion of equivalence we use?

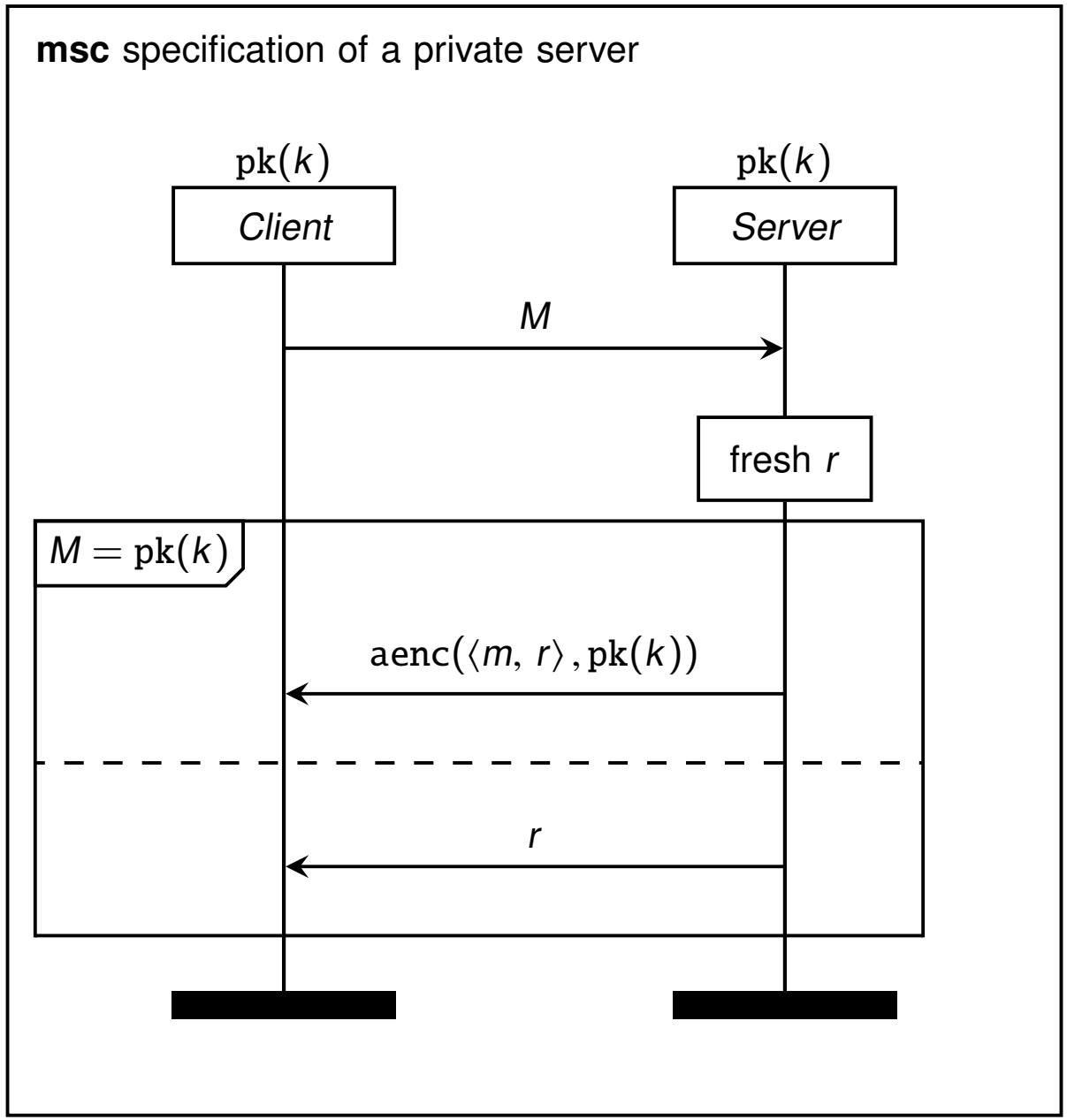


Does it matter which notion of equivalence we use?

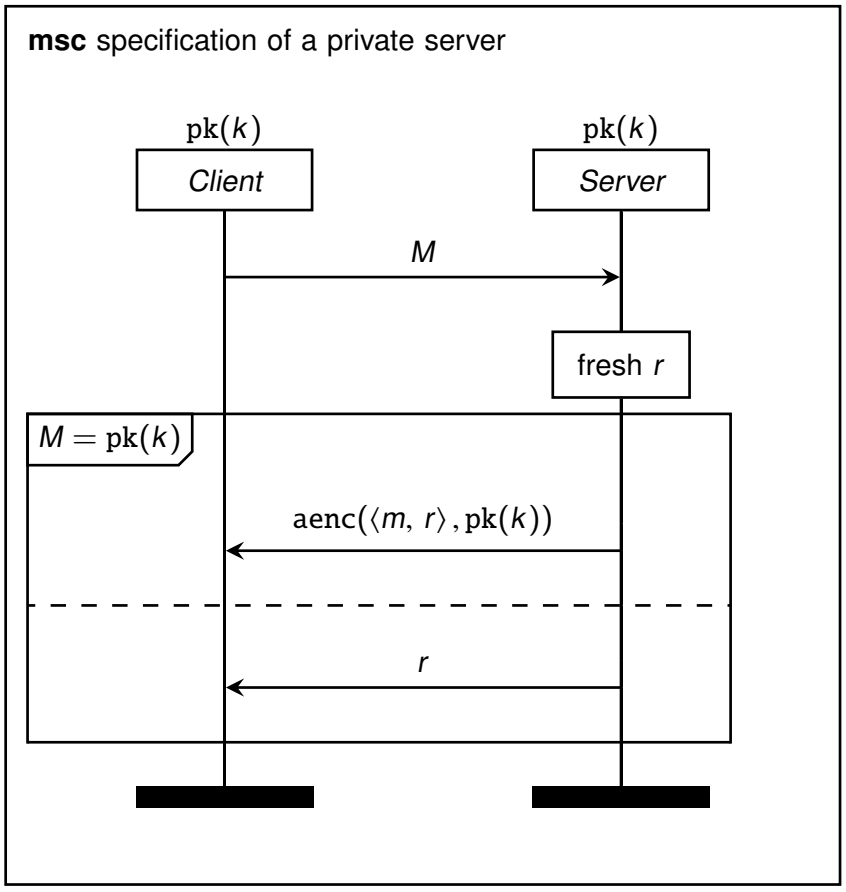
Highlights of half-a-century of research:

- Trace equivalence easy to define (aka. language equivalence, Chomsky 1963).
- . . . but bisimilarity **asymptotically more efficient** (Kanellakis and Smolka 1983, and Paige and Tarjan 1987).
- Bisimilarity sensitive to when decisions are made, uncovering **shorter attacks**.
- Open bisimilarity preserved in all contexts, hence is **compositional** (Sangiorgi 1993).
- Open bisimilarity has **prototype** for Dolev-Yao attacker (Tiu and Dawson 2012).
- Quasi-open bisimilarity is **complete** (Sangiorgi 2001)
- Quasi-open bisimilarity **characterised** by an intuitionistic modal logic (LICS'18)

First a classic private server example

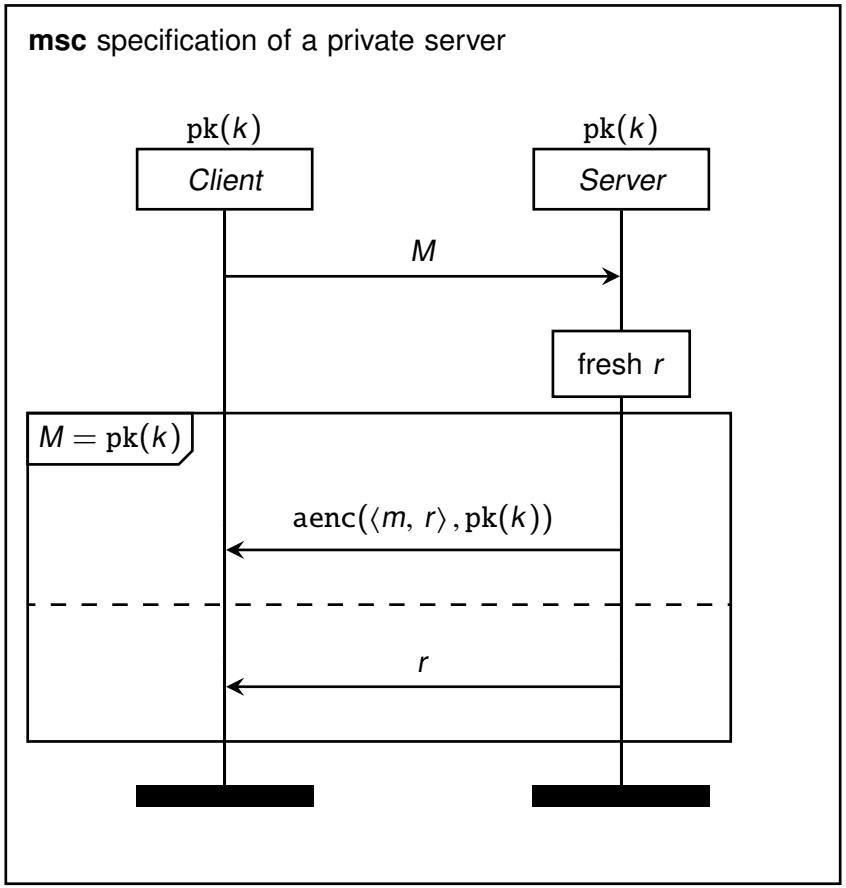


System specification in applied π-calculus



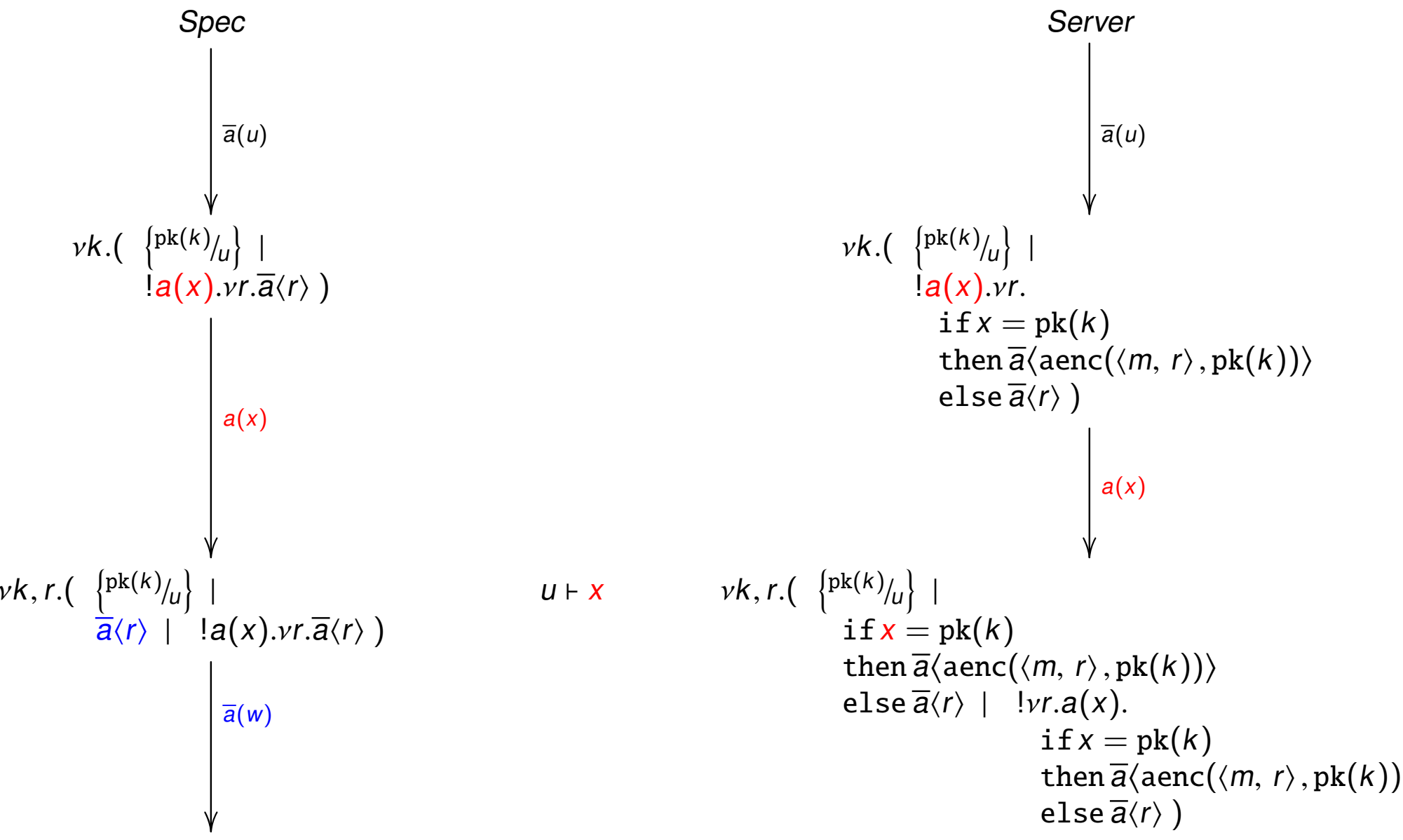
Server: $\nu k.\overline{a}\langle \mathrm{pk}(k)\rangle.$
$!\nu r.a(x).$
$\quad \mathtt{if}\ x = \mathrm{pk}(k)$
$\quad \mathtt{then}\ \overline{a}\langle \mathrm{aenc}(\langle m, r\rangle, \mathrm{pk}(k))\rangle$
$\quad \mathtt{else}\ \overline{a}\langle r\rangle$

Specification of how behaviour should appear to attacker



Spec: $\nu k.\overline{a}\langle \mathrm{pk}(k)\rangle.$
$!a(x).$
$\nu r.\overline{a}\langle r\rangle$

Open bisimilarity finds a false attack on this example



Quasi-open bisimilarity splits into cases: either $x = u$ or $x \neq u$

$$\nu k.\Big(\ \{^{\mathrm{pk}(k)}/_{u}\}\ \mid\ !a(x).\nu r.\ \mathtt{if}\ x = \mathrm{pk}(k)\ \mathtt{then}\ \overline{a}\langle \mathrm{aenc}(\langle m, r\rangle, \mathrm{pk}(k))\rangle\ \mathtt{else}\ \overline{a}\langle r\rangle\ \Big)$$

$$\downarrow\ a\ u$$

$$\nu k, r.\Big(\ \{^{\mathrm{pk}(k)}/_{u}\}\ \mid\ \mathtt{if}\ \mathrm{pk}(k) = \mathrm{pk}(k)\ \mathtt{then}\ \overline{a}\langle \mathrm{aenc}(\langle m, r\rangle, \mathrm{pk}(k))\rangle\ \mathtt{else}\ \overline{a}\langle r\rangle\ \mid\ !\nu r.a(x).\ \mathtt{if}\ x = \mathrm{pk}(k)\ \mathtt{then}\ \overline{a}\langle \mathrm{aenc}(\langle m, r\rangle, \mathrm{pk}(k))\rangle\ \mathtt{else}\ \overline{a}\langle r\rangle\ \Big)$$

$$\nu k.\Big(\ \{^{\mathrm{pk}(k)}/_{u}\}\ \mid\ !a(x).\nu r.\ \mathtt{if}\ x = \mathrm{pk}(k)\ \mathtt{then}\ \overline{a}\langle \mathrm{aenc}(\langle m, r\rangle, \mathrm{pk}(k))\rangle\ \mathtt{else}\ \overline{a}\langle r\rangle\ \Big)$$

$$\downarrow\ a\ x$$

$$\nu k, r.\Big(\ \{^{\mathrm{pk}(k)}/_{u}\}\ \mid\ \mathtt{if}\ x = \mathrm{pk}(k)\ \mathtt{then}\ \overline{a}\langle \mathrm{aenc}(\langle m, r\rangle, \mathrm{pk}(k))\rangle\ \mathtt{else}\ \overline{a}\langle r\rangle\ \mid\ !\nu r.a(x).\ \mathtt{if}\ x = \mathrm{pk}(k)\ \mathtt{then}\ \overline{a}\langle \mathrm{aenc}(\langle m, r\rangle, \mathrm{pk}(k))\rangle\ \mathtt{else}\ \overline{a}\langle r\rangle\ \Big)$$

Prove privacy by constructing a quasi-open bisimulation

$\mathcal{T}$ least symmetric open relation such that:

$$\begin{array}{lcl} & \textit{Spec} \quad \mathcal{T} & \textit{Server} \\ \nu k, r_1, \ldots r_k.(& \sigma \mid P_1 \mid \ldots P_k & \mathcal{T} \quad \nu k, r_1, \ldots r_k.(\ \theta \mid Q_1 \mid \ldots Q_k \mid \\ & \mid !a(x).\nu r.\overline{a}\langle r\rangle \ ) & \qquad\qquad !a(x).\nu r. \ \mathtt{if}\, x = \mathtt{pk}(k) \\ & & \qquad\qquad \mathtt{then}\, \overline{a}\langle \mathtt{aenc}(\langle m, r\rangle, \mathtt{pk}(k))\rangle \\ & & \qquad\qquad \mathtt{else}\, \overline{a}\langle r\rangle \ ) \end{array}$$

I, I', J' partition $\{1, \ldots k\}$

$$u_i\sigma = \begin{cases} \mathtt{pk}(k) & \text{if } i = 0 \\ r_i & \text{if } i \in I' \cup J' \\ u_i & \text{otherwise} \end{cases} \qquad u_i\theta = \begin{cases} \mathtt{pk}(k) & \text{if } i = 0 \\ r_i & \text{if } i \in I' \\ \mathtt{aenc}(\langle m, r_i\rangle, \mathtt{pk}(k)) & \text{if } i \in J' \\ u_i & \text{otherwise} \end{cases}$$

$$P_i = \begin{cases} \overline{a}\langle r_i\rangle & \text{if } i \in I \\ 0 & \text{if } i \in I' \cup J' \end{cases} \qquad Q_i = \begin{cases} \mathtt{if}\, n_i\theta = \mathtt{pk}(k) & \text{if } i \in I \\ \mathtt{then}\, \overline{a}\langle \mathtt{aenc}(\langle m, r\rangle, \mathtt{pk}(k))\rangle & \\ \mathtt{else}\, \overline{a}\langle r\rangle & \\ 0 & \text{if } i \in I' \cup J' \end{cases}$$

a, m, n_i messages fresh for $\{k, r_1, \ldots r_n\}$ $\quad u_0, \ldots u_k$ distinct variables fresh for $\{a, m, k, r_1, \ldots r_n\}$

Deterministic encryption leads to real attack, hence described by formula

$$\begin{array}{ll} \textit{Deterministic\_Server}: & \nu k.\overline{a}\langle \mathrm{pk}(k)\rangle. \\ & !a(x).\nu r. \\ & \mathtt{if}\ x = \mathrm{pk}(k) \\ & \mathtt{then}\ \overline{a}\langle \mathrm{aenc}(m, \mathrm{pk}(k))\rangle \\ & \mathtt{else}\ \overline{a}\langle r\rangle \end{array}$$

$$\textit{Deterministic\_Server} \models \langle \overline{a}(y)\rangle\langle a\, y\rangle\langle \overline{a}(z)\rangle(\mathrm{aenc}(m, y) = z)$$

$$\textit{Spec} \not\models \langle \overline{a}(y)\rangle\langle a\, y\rangle\langle \overline{a}(z)\rangle(\mathrm{aenc}(m, y) = z)$$

Meaning: after transitions $\xrightarrow{\overline{a}(y)}\xrightarrow{a\, y}\xrightarrow{\overline{a}(z)}$, *Deterministic_Server* and *Spec* reach the following respective frames, distiguishable by the given recipe.

$\nu k.\left(\left\{{}^{\mathrm{pk}(k)}/_{y}\right\} \mid \left\{{}^{\mathrm{aenc}(m,\mathrm{pk}(k))}/_{z}\right\}\right)$ not statically equivalent to $\nu k, r.\left(\left\{{}^{\mathrm{pk}(k)}/_{y}\right\} \mid \left\{{}^{r}/_{z}\right\}\right)$

Recap

- Bisimilarity congruences **compositional** and **efficient** to discover.
- Open bisimilarity found a **false attack** on privacy.
- Quasi-open bisimilarity provides just enough information to **avoid such false attacks**.
- Such real attacks can **always** be described using an **intuitionistic modal logic**.

None of these facts are obvious!

We fill an important gap in the literature.

...but what about more substantial **unlinkability** examples?

e-passport example

$$
\begin{aligned}
\mathit{Reader} \triangleq\ & c_k(x_k).d(nt).\nu nr.\nu kr. \\
& \mathtt{let}\ m = \{\langle nr, \langle nt, kr\rangle\rangle\}_{\mathtt{snd}(x_k)}\ \mathtt{in} \\
& \overline{c}\langle m, \mathtt{mac}(\langle m, \mathtt{fst}(x_k)\rangle)\rangle
\end{aligned}
$$

$$
\begin{aligned}
\mathit{MainUK} \triangleq\ & \overline{c_k}\langle ke, km\rangle. \\
& \nu nt.\overline{c}\langle nt\rangle.d(y). \\
& \mathtt{if}\ \mathtt{snd}(y) = \mathtt{mac}(\mathtt{fst}(y), km) \wedge nt = \mathtt{fst}(\mathtt{snd}(\mathtt{dec}(\mathtt{fst}(y), ke))) \\
& \quad \mathtt{then} \quad \nu kt.\mathtt{let}\ m = \{\langle nt, \langle \mathtt{fst}(\mathtt{dec}(\mathtt{fst}(y), ke)), kt\rangle\rangle\}_{ke}\ \mathtt{in} \\
& \qquad\qquad \overline{c}\langle m, \mathtt{mac}(m, km)\rangle \\
& \quad \mathtt{else} \quad \overline{c}\langle error\rangle
\end{aligned}
$$

$$\mathit{System} \triangleq \nu c_k.(!\mathit{Reader} \mid !\nu ke.\nu km.!\mathit{MainUK})$$

$$\mathit{Spec} \triangleq \nu c_k.(!\mathit{Reader} \mid !\nu ke.\nu km.\mathit{MainUK})$$

Failure of **unlinkability**:

$$\mathit{System} \not\sim \mathit{Spec}$$

System leads by starting two sessions with the same e-passport

$$System \xrightarrow{\tau} \xrightarrow{\tau} \xrightarrow{\overline{c}(u)} System2$$

System2:

$$\nu c_k, ke_1, km_1, nt_1.(\{^{nt_1}/_u\} \mid R1_1 \mid R1_1 \mid !Reader \mid SentNonce_1 \mid UK1_1 \mid !MainUK_1 \mid !\nu ke.\nu km.!MainUK\ )$$

Spec can only follow by starting two sessions with different e-passports.

$$Spec \xrightarrow{\tau} \xrightarrow{\tau} \xrightarrow{\overline{c}(u)} Spec2$$

Spec2:

$$\nu c_k, ke_1, km_1, ke_2, km_2, nt_1.(\{^{nt_1}/_u\} \mid R1_1 \mid R1_2 \mid !Reader \mid SentNonce_1 \mid UK1_2 \mid !\nu ke.\nu km.MainUK\ )$$

State of reader with keys km_1, ke_1:

$\nu nt.\overline{c}\langle nt\rangle.$
$<$——— Reached here sending nonce nt_1
$d(y).$
$\mathtt{if}\ \mathtt{snd}(y) = \mathtt{mac}(\mathtt{fst}(y), km_1) \wedge nt_1 = \mathtt{fst}(\mathtt{snd}(\mathtt{dec}(\mathtt{fst}(y), ke_1)))$
$\mathtt{then}\quad \nu kt.\mathtt{let}\ m = \{\langle nt_1, \langle \mathtt{fst}(\mathtt{dec}(\mathtt{fst}(y), ke_1)), kt\rangle\rangle\}_{ke_1}\ \mathtt{in}$
$\overline{c}\langle m, \mathtt{mac}(m, km_1)\rangle$
$\mathtt{else}\quad \overline{c}\langle error\rangle$

Specification takes lead, executing reader with keys ke_2, km_2.

$$Spec2 \xrightarrow{d(nt)} \xrightarrow{\overline{c}(w)} Spec3$$

$Spec3$:

$$\nu c_k, ke_1, km_1, nt_1, ke_2, km_2, nr, kr.(\quad \left\{ {}^{nt_1}/_{u} \right\} \mid \left\{ \left\langle \{\langle nr, \langle nt, kr \rangle \rangle\}_{ke_2}, \mathtt{mac}\left(\{\langle nr, \langle nt, kr \rangle \rangle\}_{ke_2}, km_2\right) \right\rangle_{/w} \right\}$$
$$\mid \quad R1_1 \mid 0 \mid !Reader \mid SentNonce_1 \mid UK1_2 \mid !\nu ke.\nu km.MainUK \;)$$

Execution is completely **lazy**, producing constraint:

$$u \vdash nt$$

$System2$ follows as best as possible:

$$System2 \xrightarrow{d(nt)} \xrightarrow{\overline{c}(w)} System3$$

$System3$:

$$\nu c_k, nt_1, ke_1, km_1, nr, kr.(\quad \left\{ {}^{nt_1}/_{u} \right\} \mid \left\{ \left\langle \{\langle nr, \langle nt, kr \rangle \rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle nt, kr \rangle \rangle\}_{ke_1}, km_1\right) \right\rangle_{/w} \right\}$$
$$\mid \quad R1_1 \mid 0 \mid !Reader \mid SentNonce_1 \mid UK1_1 \mid !MainUK_1 \mid !\nu ke.\nu km.!MainUk$$

Notice **either** reader can be executed.

Execution of e-passport resumes with symbolic input

$$System3 \xrightarrow{d(y)} System4$$

*System*4:

$$\nu c_k, nt_1, ke_1, km_1, nr, kr.(\quad \left\{ {}^{nt_1}/_{u} \right\} \mid \left\{ {}^{\langle \{\langle nr, \langle nt, kr \rangle\rangle\}_{ke_1}, \mathtt{mac}(\{\langle nr, \langle nt, kr \rangle\rangle\}_{ke_1}, km_1) \rangle}/_{w} \right\}$$
$$\mid \quad R1_1 \mid 0 \mid !Reader \mid Rcvd(y)_1 \mid UK1_1 \mid !MainUK_1 \mid !\nu ke.\nu km.!MainUK \;)$$

$$Rcvd(y)_1 \triangleq \quad \mathtt{if}\ \mathtt{snd}(y) = \mathtt{mac}(\mathtt{fst}(y), km_1) \wedge nt_1 = \mathtt{fst}(\mathtt{snd}(\mathtt{dec}(\mathtt{fst}(y), ke_1)))$$
$$\mathtt{then} \quad \nu kt.\mathtt{let}\ m = \{\langle nt_1, \langle \mathtt{fst}(\mathtt{dec}(\mathtt{fst}(y), ke_1)), kt \rangle\rangle\}_{ke_1}\ \mathtt{in}$$
$$\overline{c}\langle m, \mathtt{mac}(m, km_1) \rangle$$
$$\mathtt{else} \quad \overline{c}\langle error \rangle$$

Constraints:

$$u \vdash nt \qquad u, w \vdash y$$

Find Most General Unifier for Equality Constraints

Solve for y: $\mathtt{snd}(y) = \mathtt{mac}(\mathtt{fst}(y), km_1) \wedge nt_1 = \mathtt{fst}(\mathtt{snd}(\mathtt{dec}(\mathtt{fst}(y), ke_1)))$

$$\begin{aligned}
&\text{iff } y = \langle y_1, y_2 \rangle \wedge y_2 = \mathtt{mac}(y_1, km_1) \wedge nt_1 = \mathtt{fst}(\mathtt{snd}(\mathtt{dec}(y_1, ke_1))) \\
&\text{iff } y = \langle y_1, y_2 \rangle \wedge y_1 = \{y_3\}_{ke_1} \wedge y_2 = \mathtt{mac}(y_1, km_1) \wedge nt_1 = \mathtt{fst}(\mathtt{snd}(y_3)) \\
&\text{iff } y = \langle y_1, y_2 \rangle \wedge y_1 = \{y_3\}_{ke_1} \wedge y_2 = \mathtt{mac}(y_1, km_1) \wedge y_3 = \langle y_4, y_5 \rangle \wedge nt_1 = \mathtt{fst}(y_5) \\
&\text{iff } y = \langle y_1, y_2 \rangle \wedge y_1 = \{y_3\}_{ke_1} \wedge y_2 = \mathtt{mac}(y_1, km_1) \wedge y_3 = \langle y_4, y_5 \rangle \wedge y_5 = \langle y_6, y_7 \rangle \wedge y_6 = nt_1
\end{aligned}$$

Applying variable elimination we obtain (where y_4 and y_7 are fresh variables):

$$y = \left\langle \{\langle y_4, \langle nt_1, y_7 \rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle y_4, \langle nt_1, y_7 \rangle\rangle\}_{ke_1}, km_1\right)\right\rangle$$

But is the history respected?

Solve a system of “Deducibility Constraints”

Most general unifier for y:

$$y = \left\langle \{\langle y_4, \langle nt_1, y_7 \rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle y_4, \langle nt_1, y_7 \rangle\rangle\}_{ke_1}, km_1\right)\right\rangle$$

Current **frame** for *System*4.

$$\nu nt_1, ke_1, km_1, nr, kr.\left(\left\{{}^{nt_1}/_{u}\right\} \mid \left\{{}^{\left\langle \{\langle nr, \langle nt, kr\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle nt, kr\rangle\rangle\}_{ke_1}, km_1\right)\right\rangle}/_{w}\right\}\right.$$

Current **constraints**, outputs before each input form **attacker's knowledge** before each input:

$$u \vdash nt \qquad u, w \vdash y$$

Apply substitutions to find constraints to solve (where nt_1, ke_1, km_1, nr, kr names):

$$nt_1 \vdash nt$$

$$nt_1, \left\langle \{\langle nr, \langle nt, kr\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle nt, kr\rangle\rangle\}_{ke_1}, km_1\right)\right\rangle \vdash \left\langle \{\langle y_4, \langle nt_1, y_7\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle y_4, \langle nt_1, y_7\rangle\rangle\}_{ke_1}, km_1\right)\right\rangle$$

Solve the Deducibility Constraints

Want to solve the following:

$$nt_1 \vdash nt$$

$$nt_1, \langle \{\langle nr, \langle nt, kr \rangle\rangle\}_{ke_1}, \mathtt{mac}(\{\langle nr, \langle nt, kr \rangle\rangle\}_{ke_1}, km_1) \rangle \vdash \langle \{\langle y_4, \langle nt_1, y_7 \rangle\rangle\}_{ke_1}, \mathtt{mac}(\{\langle y_4, \langle nt_1, y_7 \rangle\rangle\}_{ke_1}, km_1) \rangle$$

Only one possibility, unify the following (where nt_1, ke_1, km_1, nr, kr names):

$$\langle \{\langle nr, \langle nt, kr \rangle\rangle\}_{ke_1}, \mathtt{mac}(\{\langle nr, \langle nt, kr \rangle\rangle\}_{ke_1}, km_1) \rangle = \langle \{\langle y_4, \langle nt_1, y_7 \rangle\rangle\}_{ke_1}, \mathtt{mac}(\{\langle y_4, \langle nt_1, y_7 \rangle\rangle\}_{ke_1}, km_1) \rangle$$

Most general solution:

$$nt = nt_1 \qquad y_4 = nr \qquad y_7 = kr$$

Applying substitution constraints are provable (remember which are names):

$$nt_1 \vdash nt_1$$

$$nt_1, \langle \{\langle nr, \langle nt_1, kr \rangle\rangle\}_{ke_1}, \mathtt{mac}(\{\langle nr, \langle nt_1, kr \rangle\rangle\}_{ke_1}, km_1) \rangle \vdash \langle \{\langle nr, \langle nt_1, nt \rangle\rangle\}_{ke_1}, \mathtt{mac}(\{\langle nr, \langle nt_1, nt \rangle\rangle\}_{ke_1}, km_1) \rangle$$

Annotate Proofs with “Recipes”

$$u\colon nt_1 \vdash u\colon nt_1$$

$$u\colon nt_1, w\colon \left\langle \{\langle nr, \langle nt_1, kr\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle nt_1, kr\rangle\rangle\}_{ke_1}, km_1\right)\right\rangle \vdash w\colon \left\langle \{\langle nr, \langle nt_1, nt\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle nt_1, nt\rangle\rangle\}_{ke_1}, km_1\right)\right\rangle$$

From recipes, we obtain **respectful substitution** $\{^{u}/_{nt}\}\cdot\left\{^{w}/_{y}\right\}$ enabling guard in *System*4:

$$\nu c_k, nt_1, ke_1, km_1, nr, kr.\big(\quad \left\{^{nt_1}/_{u}\right\} \mid \left\{^{\left\langle \{\langle nr, \langle u, kr\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle u, kr\rangle\rangle\}_{ke_1}, km_1\right)\right\rangle}/_{w}\right\}$$
$$\mid \quad R1_1 \mid 0 \mid !Reader \mid Rcvd(w)_1 \mid UK1_1 \mid !MainUK_1 \mid !\nu ke.\nu km.!MainUK \ \big)$$

applying above frame to the following enables the guard:

$$Rcvd(w)_1 \triangleq \ \mathtt{if}\ \mathtt{snd}(w) = \mathtt{mac}(\mathtt{fst}(w), km_1) \wedge nt_1 = \mathtt{fst}(\mathtt{snd}(\mathtt{dec}(\mathtt{fst}(w), ke_1)))$$
$$\mathtt{then} \quad \nu kt.\mathtt{let}\ m = \{\langle nt_1, \langle \mathtt{fst}(\mathtt{dec}(\mathtt{fst}(y), ke_1)), kt\rangle\rangle\}_{ke_1}\ \mathtt{in}$$
$$\overline{c}\langle m, \mathtt{mac}(m, km_1)\rangle$$
$$\mathtt{else} \quad \overline{c}\langle error\rangle$$

Final Transition of *System*4

Since match enabled, *System*4 proceeds as follows.

$$\begin{aligned}\nu c_k, ke_1, km_1, nr, kr.(\quad & \left\{nt_1/_u\right\} \mid \left\{\left\langle \{\langle nr, \langle nt_1, kr\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle nt_1, kr\rangle\rangle\}_{ke_1}, km_1\right)\right\rangle/_w\right\} \\ \mid \quad & R1_1 \mid 0 \mid !Reader \mid Rcvd(\left\langle \{\langle nr, \langle nt_1, kr\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle nt_1, kr\rangle\rangle\}_{ke_1}, km_1)_1\right)\right\rangle \\ \mid \quad & UK1_1 \mid !MainUK_1 \mid !\nu ke.\nu km.!MainUK\ ))\end{aligned}$$

$$\xrightarrow{\overline{c}(z)}$$

$$\begin{aligned}\nu c_k, nt_1, ke_1, km_1, nr, kr, kt.(\quad & \left\{nt_1/_u\right\} \mid \left\{\left\langle \{\langle nr, \langle nt_1, kr\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle nt_1, kr\rangle\rangle\}_{ke_1}, km_1\right)\right\rangle/_w\right\} \\ \mid \quad & \left\{\left\langle \{\langle nt_1, \langle nr, kt\rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nt_1, \langle nr, kt\rangle\rangle\}_{ke_1}, km_1\right)\right\rangle/_z\right\} \\ \mid \quad & R1_1 \mid 0 \mid !Reader \mid 0 \mid UK1_1 \mid !MainUK_1 \mid !\nu ke.\nu km.!MainUK\ )\end{aligned}$$

Finally we reach states distinguished by **static equivalence**

State of *System*5:

$$\nu c_k, nt_1, ke_1, km_1, nr, kr, kt.(\quad \left\{ {}^{nt_1}/_{u} \right\} \mid \left\{ \left\langle \{\langle nr, \langle u, kr \rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nr, \langle u, kr \rangle\rangle\}_{ke_1}, km_1\right) \right\rangle /_{w} \right\}$$
$$\mid \quad \left\{ \left\langle \{\langle nt_1, \langle nr, kt \rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nt_1, \langle nr, kt \rangle\rangle\}_{ke_1}, km_1\right) \right\rangle /_{z} \right\}$$
$$\mid \quad R1_1 \mid 0 \mid !Reader \mid 0 \mid UK1_1 \mid !MainUK_1 \mid !\nu ke.\nu km.!MainUK \;)$$

State of *Spec*5 after same moves:

$$\nu c_k, ke_1, km_1, nt_1, ke_2, km_2, nr, kr.(\quad \left\{ {}^{nt_1}/_{u} \right\} \mid \left\{ \left\langle \{\langle nr, \langle nt_1, kr \rangle\rangle\}_{ke_2}, \mathtt{mac}\left(\{\langle nr, \langle nt_1, kr \rangle\rangle\}_{ke_2}, km_2\right) \right\rangle /_{w} \right\} \mid \{ {}^{error}/_{z} \}$$
$$\mid \quad R1_1 \mid 0 \mid !Reader \mid 0 \mid UK1_2 \mid !\nu ke.\nu km.MainUK \;)$$

Distinguished by equation:

$$error = z$$

For *System*5 this equation evaluates to (no variables):

$$error = \left\langle \{\langle nt_1, \langle nr, kt \rangle\rangle\}_{ke_1}, \mathtt{mac}\left(\{\langle nt_1, \langle nr, kt \rangle\rangle\}_{ke_1}, km_1\right) \right\rangle$$

For *Spec*5 this equation evaluates to:

$$error = error$$

Checking Attack is a Real Attack: using intuitionistic $\mathcal{FM}$

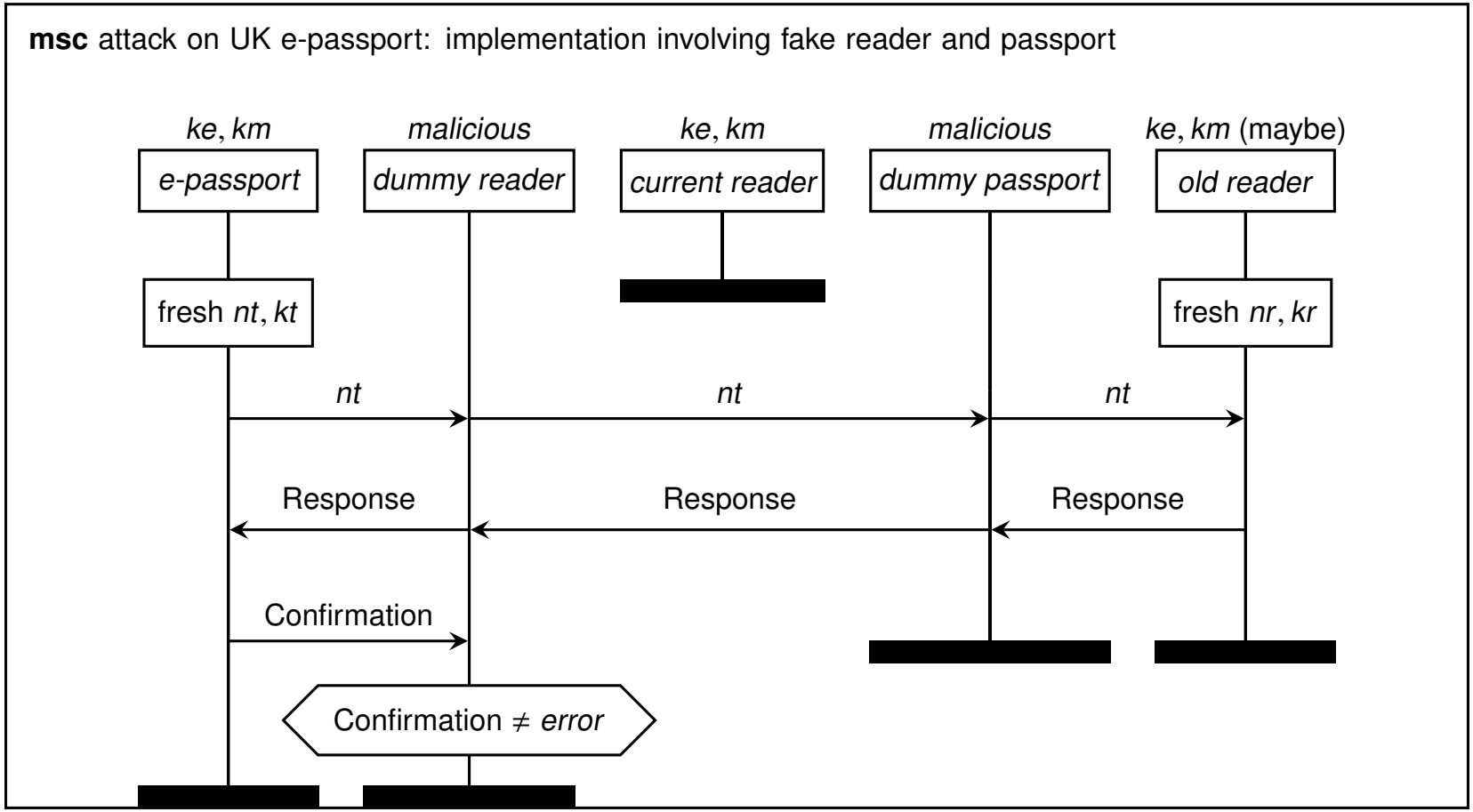
$$\begin{aligned} \mathit{System} \models \quad & \langle\tau\rangle\langle\tau\rangle\langle\overline{c}(u)\rangle \\ & [d\,u]\big(\ \langle\overline{c}(w)\rangle[d\,w][\overline{c}(z)](\mathit{error} \neq z) \\ & \qquad \vee \langle\overline{c}(w)\rangle(w = \mathit{error})\ \big) \end{aligned}$$

$$\begin{aligned} \mathit{Spec} \not\models \quad & \langle\tau\rangle\langle\tau\rangle\langle\overline{c}(u)\rangle \\ & [d\,u]\big(\ \langle\overline{c}(w)\rangle[d\,w][\overline{c}(z)](\mathit{error} \neq z) \\ & \qquad \vee \langle\overline{c}(w)\rangle(w = \mathit{error})\ \big) \end{aligned}$$

Sub-formula in red is main attack branch.

Sub-formula in blue eliminates branch immediately diverging from the attack (challenge is directly fed back to e-passport).

Implementation of attack: is it practical?



$Response = \langle \{\langle nr, \langle nt, kr \rangle\rangle\}_{ke}, \mathtt{mac}(\{\langle nr, \langle nt, kr \rangle\rangle\}_{ke}, km)\rangle$
$Confirmation = \langle \{\langle nt, \langle nr, kt \rangle\rangle\}_{ke}, \mathtt{mac}(\{\langle nt, \langle nr, kt \rangle\rangle\}_{ke}, km)\rangle$

Your questions?

- Can prove refinement of BAC is unlinkable (randomly encrypt errors).
- Automatic, but requires tool for anyone to use.
- Implementation: components reusable from existing tools (ProVerif, Tamarin, etc.).
- All trace attacks are discovered using bisimilarity...
- ...however, attack shown is shorter than any attack found using trace equivalence.
- Attacker may control choices (which readers to use).
- Complements rather than competes, e.g., with respect to POR.

Why no law of excluded middle?

Classically, $\phi \vee \neg\phi$ is a tautology and $\left[\pi\right]\phi = \neg\left\langle\pi\right\rangle\neg\phi$.
Hence for all classical modal logics:

$$\overline{a}b \mid c(x) \models \left\langle\tau\right\rangle\mathrm{tt} \vee \left[\tau\right]\mathrm{ff}$$

Intuitionistically, "Reachable worlds" are processes accessible by substitutions. E.g.

$$\overline{a}b \mid c(x) \leq (\overline{a}b \mid c(x))\{{}^{a}/_{c}\} \qquad \text{and} \qquad \overline{a}b \mid a(x) \xrightarrow{\tau} 0$$

Closing modalities under all reachable worlds (**intuitionistic heredity**):

$$\overline{a}b \mid c(x) \not\models \left\langle\tau\right\rangle\mathrm{tt} \vee \left[\tau\right]\mathrm{ff}$$

$\overline{a}b \mid c(x) \not\models \left\langle\tau\right\rangle\mathrm{tt}$, — no τ-transition in world where a and c are not equal.

$\overline{a}b \mid c(x) \not\models \left[\tau\right]\mathrm{ff}$, — some τ-transition in world where $a = c$.

For congruences, quantify over all names

For congruences (open bisimilarity and late congruence):

$$[x = y]\tau \quad \not\sim \quad 0$$

Distinguishing strategy, in world where $x = y$:

$$([x = y]\tau)\{{}^{y}/_{x}\} \xrightarrow{\tau} 0 \qquad \text{but} \qquad 0\{{}^{y}/_{x}\} \not\downarrow_{\tau}$$

Distinguishing formula biased to the left:

$$[x = y]\tau \models \Big[x = y\Big]\Big\langle\tau\Big\rangle\mathtt{tt} \qquad \text{and} \qquad 0 \not\models \Big[x = y\Big]\Big\langle\tau\Big\rangle\mathtt{tt}$$

Distinguishing formula biased to the right:

$$[x = y]\tau \not\models \Big[\tau\Big]\mathtt{ff} \qquad \text{and} \qquad 0 \models \Big[\tau\Big]\mathtt{ff}$$

No duality between left and right formulae

All bisimulations agree:

$$[x = y]\tau \quad \not\sim \quad \tau$$

Distinguishing formula biased to the right:

$$[x = y]\tau \not\models \langle\tau\rangle\mathtt{tt} \qquad \text{and} \qquad \tau \models \langle\tau\rangle\mathtt{tt}$$

Dual formula is **not distinguishing**.

$$[x = y]\tau \not\models \neg\langle\tau\rangle\mathtt{tt} \qquad \text{and} \qquad \tau \not\models \neg\langle\tau\rangle\mathtt{tt}$$

[read as “there is no reachable world in which we can do a τ-transition”]

What is a distinguishing formula biased to the left?

No duality between left and right formulae

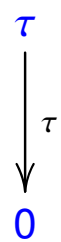
All bisimulations agree:

$$[x = y]\tau \quad \not\sim \quad \tau$$

What is a distinguishing formula biased to the left?

Distinguishing strategy (right process leads):

$$[x = y]\tau$$



Since right leads, for formula biased to the left, write **box**:

$$[\tau](\ldots\ldots\ldots\ldots)$$

No duality between left and right formulae

All bisimulations agree:

$$[x = y]\tau \quad \not\sim \quad \tau$$

What is a distinguishing formula biased to the left?

Distinguishing strategy (right process leads):

$[x = y]\tau$ $\xrightarrow{\tau}$ only in worlds where $x = y$

τ $\xrightarrow{\tau}$ 0

Since right leads and left only follows in worlds where $x = y$, write $x = y$ as post-condition:

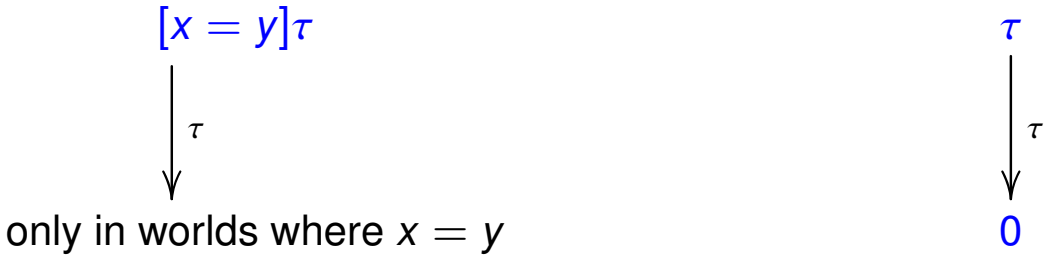
$$\big[\tau\big]\big\langle x = y\big\rangle \mathrm{tt}$$

No duality between left and right formulae

All bisimulations agree:

$$[x = y]\tau \quad \not\sim \quad \tau$$

Distinguishing strategy (right process leads):



Distinguishing formula biased to the left:

$$[x = y]\tau \models \big[\tau\big]\big\langle x = y\big\rangle \mathrm{tt} \qquad \text{and} \qquad 0 \not\models \big[\tau\big]\big\langle x = y\big\rangle \mathrm{tt}$$

Generating distinguishing formulae algorithmically

Not open bisimilar:

$$\tau + \tau.\tau + \tau.[x = y]\tau \quad \not\sim \quad \tau + \tau.\tau$$

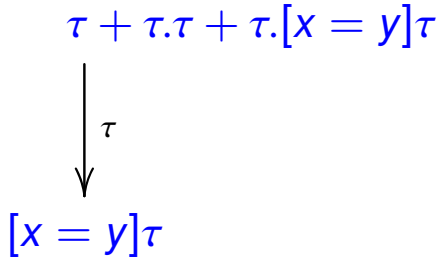
Distinguishing strategy (left process leads first):

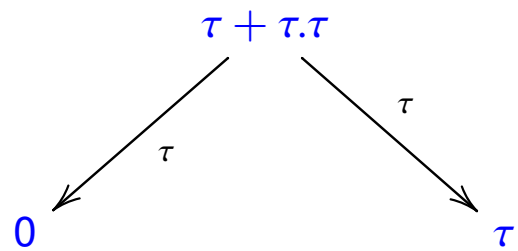
We just saw:

$$[x = y]\tau \not\sim 0 \qquad \text{and} \qquad [x = y]\tau \not\sim \tau$$

Generating distinguishing formulae algorithmically

Distinguishing strategy (left process leads first):





We just saw:

$$[x = y]\tau \models \big[x = y\big]\big\langle\tau\big\rangle\mathtt{tt} \qquad 0 \models \big[\tau\big]\mathtt{ff}$$

$$[x = y]\tau \models \big[\tau\big]\big\langle x = y\big\rangle\mathtt{tt} \qquad \tau \models \big\langle\tau\big\rangle\mathtt{tt}$$

Since left process leads: diamond on left, box on right.

$$\big\langle\tau\big\rangle(\ldots\ldots\ldots\ldots\ldots\ldots) \qquad \big[\tau\big](\ldots\ldots\ldots\ldots\ldots\ldots)$$

Generating distinguishing formulae algorithmically

Distinguishing strategy (left process leads first):

We just saw:

$$[x = y]\tau \models \big[x = y\big]\big\langle\tau\big\rangle\mathtt{tt} \qquad 0 \models \big[\tau\big]\mathtt{ff}$$

$$[x = y]\tau \models \big[\tau\big]\big\langle x = y\big\rangle\mathtt{tt} \qquad \tau \models \big\langle\tau\big\rangle\mathtt{tt}$$

Since left process leads: conjunction on left, disjunction on right.

$$\big\langle\tau\big\rangle\big(\big[x = y\big]\big\langle\tau\big\rangle\mathtt{tt} \wedge \big[\tau\big]\big\langle x = y\big\rangle\mathtt{tt}\big) \qquad \big[\tau\big]\big(\big[\tau\big]\mathtt{ff} \vee \big\langle\tau\big\rangle\mathtt{tt}\big)$$

Generating distinguishing formulae algorithmically

Not open bisimilar:

$$\tau + \tau.\tau + \tau.[x = y]\tau \qquad \not\sim \qquad \tau + \tau.\tau$$

Distinguishing formula biased to left.

$$\tau + \tau.\tau + \tau.[x = y]\tau \models \langle\tau\rangle\big([x = y]\langle\tau\rangle\mathrm{tt} \wedge [\tau]\langle x = y\rangle\mathrm{tt}\big)$$

Distinguishing formula biased to right.

$$\tau + \tau.\tau \models [\tau]\big([\tau]\mathrm{ff} \vee \langle\tau\rangle\mathrm{tt}\big)$$

Only distinguishing if we drop law of excluded middle for name equality. I.e.

$$x = y \text{ or } x \neq y \qquad \text{iff} \qquad \tau + \tau.\tau + \tau.[x = y]\tau \models [\tau]\big([\tau]\mathrm{ff} \vee \langle\tau\rangle\mathrm{tt}\big).$$

[Mechanically proven in intuitionistic proof assistant]

Results for modal logic $\mathcal{OM}$

Theorem (soundness)

If $P \sim Q$ then, for all formulae ϕ, $P \models \phi$ iff $Q \models \phi$.

Proof.

By induction on structure of ϕ. [mechanised] □

Theorem (completeness)

Whenever, for all formulae ϕ, $P \models \phi$ iff $Q \models \phi$, we have that $P \sim Q$.

Proof.

If $P \nsim Q$, by induction on depth of a distinguishing strategy, construct ϕ_L and ϕ_R such that:

- $P \models \phi_L$ and $Q \not\models \phi_L$;
- $P \not\models \phi_R$ and $Q \models \phi_R$.

Proof is constructive, so yields algorithm for generating distinguishing formulae. [implemented] □