Breaking Unlinkability

of the ICAO 9303 Standard for e-Passports

using Bisimilarity

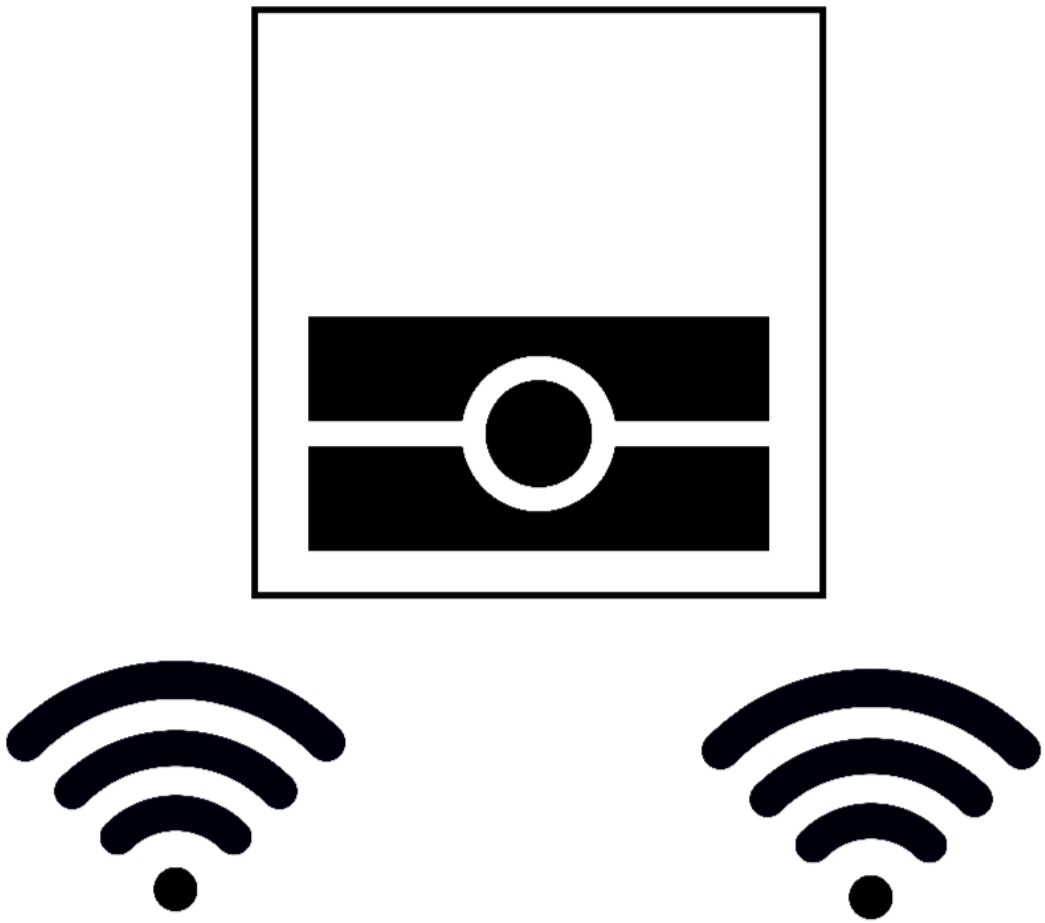
ESORICS 2019. 24th European Symposium on Research in Computer Security,
Luxembourg, September 23-27, 2019

Ihor Filimonov, Ross Horne, Sjouke Mauw, and Zach Smith

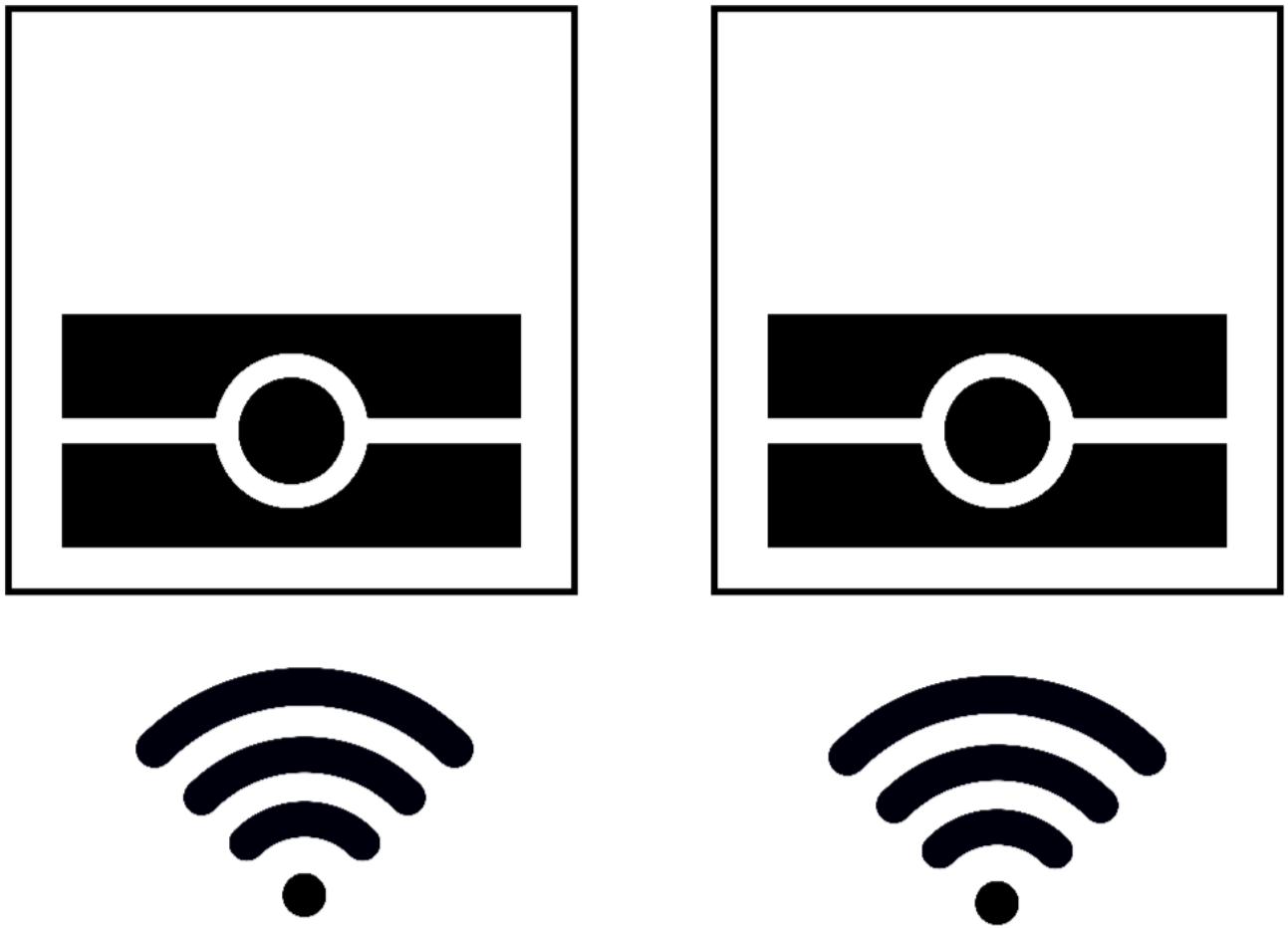
Computer Science, University of Luxembourg

24 September 2019

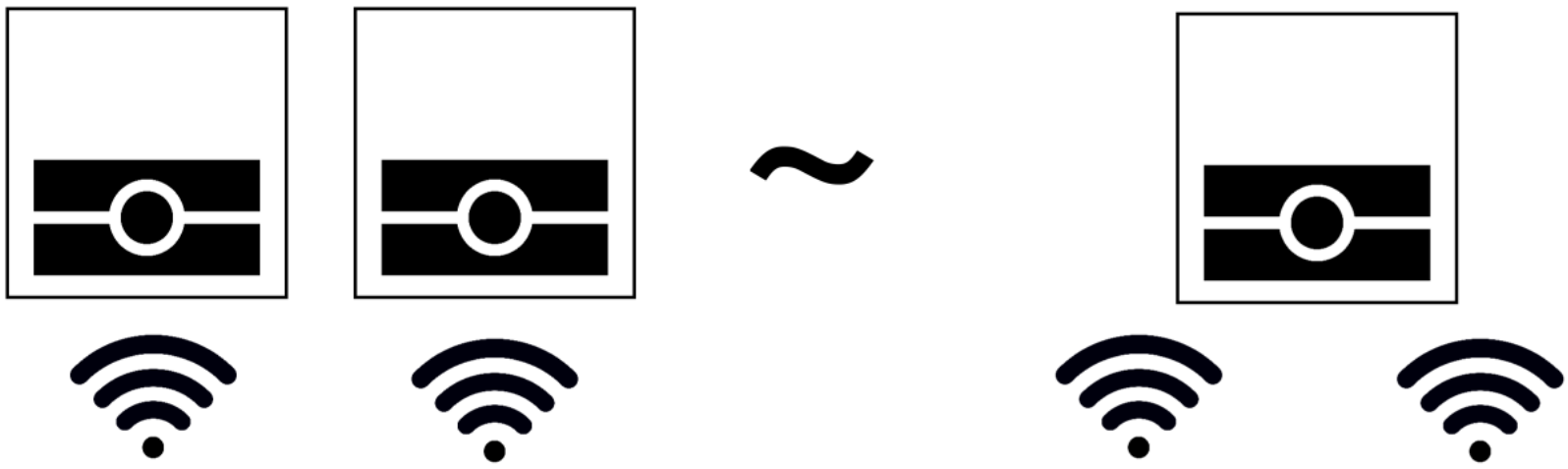
The System: multiple sessions may use same e-passport



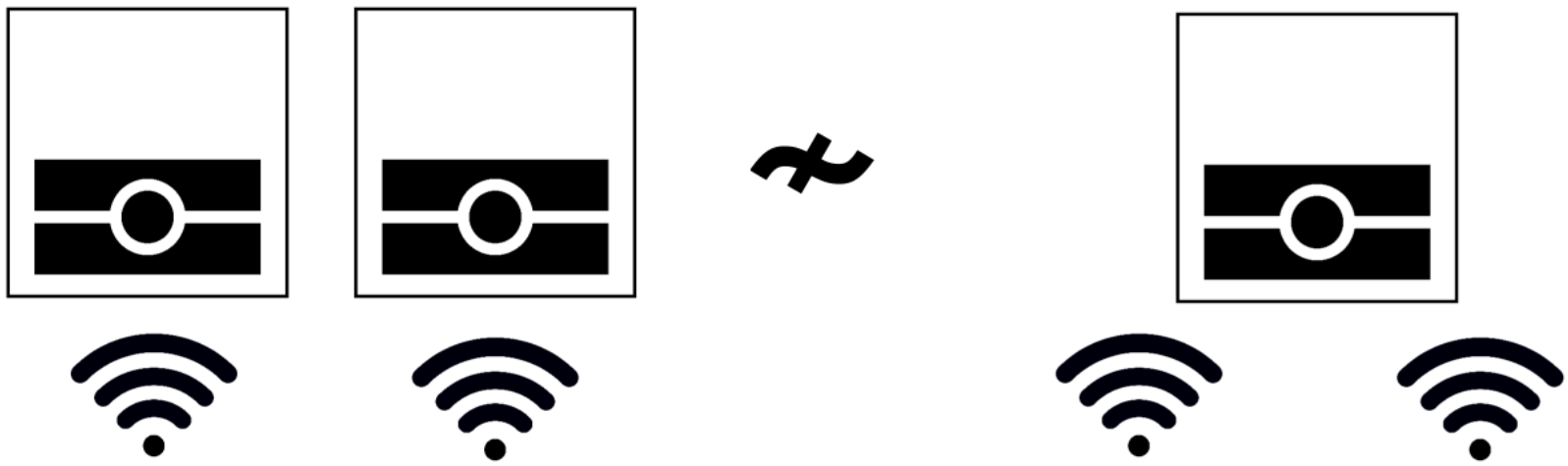
The Specification: every session is with a new e-passport



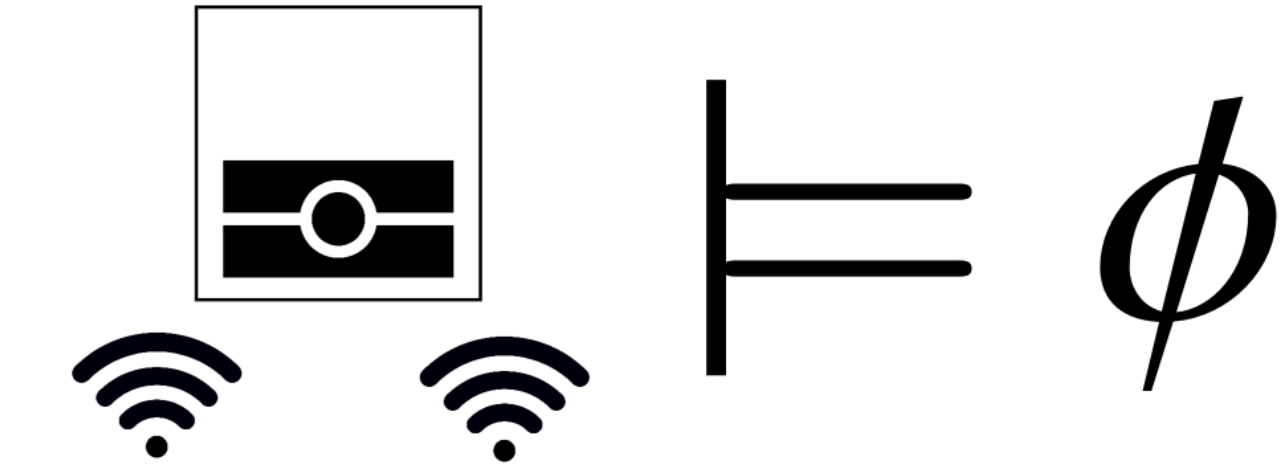
Unlinkability: all sessions appear to be with new e-passport

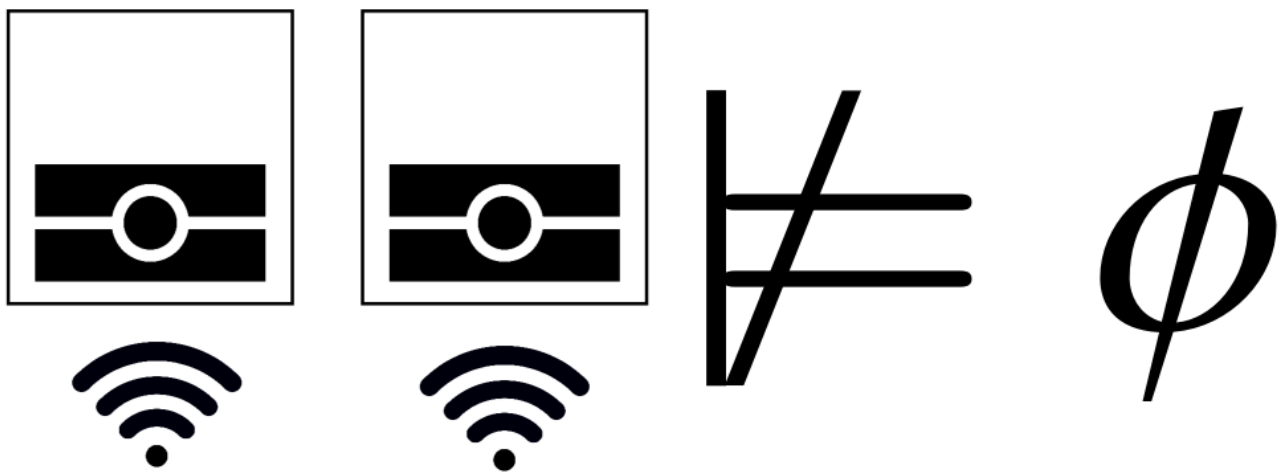


Attack: attacker has distinguishing strategy

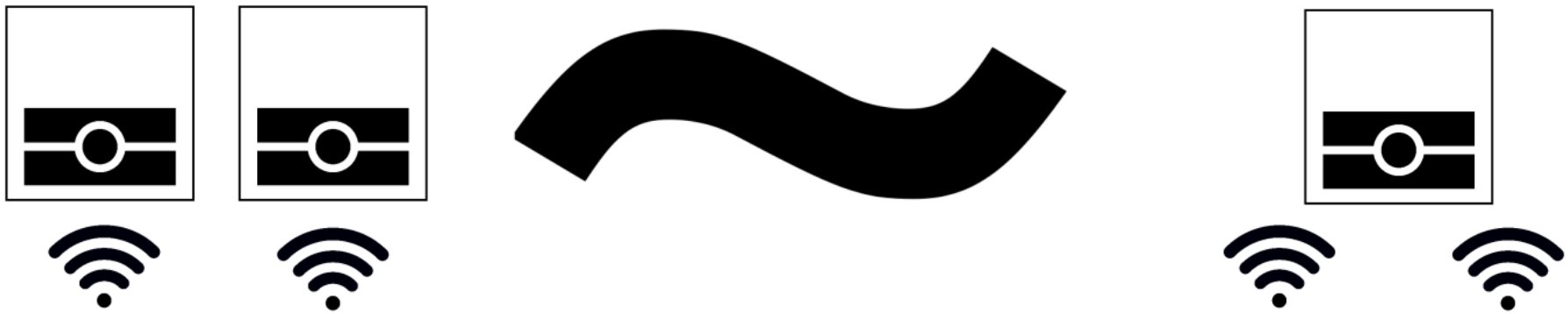


Modal Logic: describes attack strategy whenever attack exists

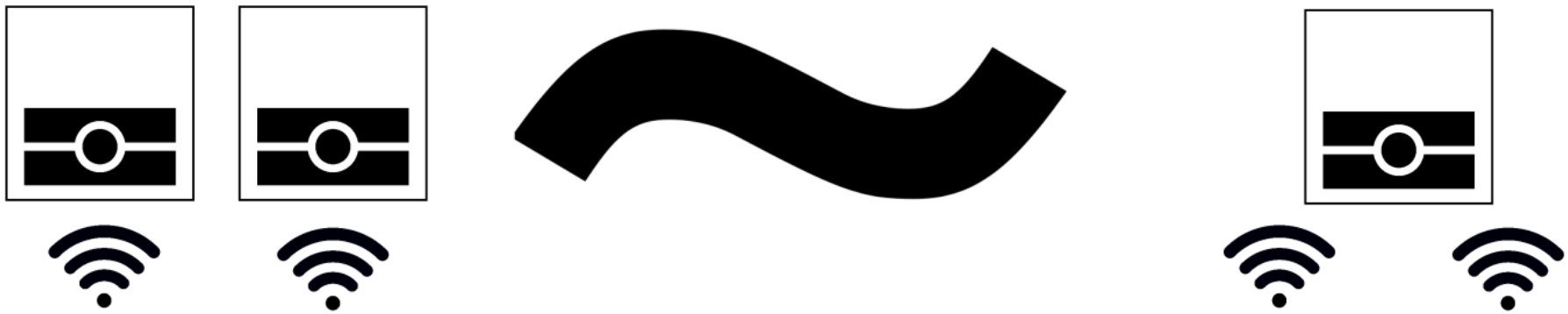




Does the notion of equivalence matter?



Does the notion of equivalence matter?



Very much so.

Timeline: a decade debating the Unlinkability of (UK) BAC

2010 — **false unlinkability proof.** *Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. CSF'10.* Claims to have proof of strong unlinkability, but none provided.

Timeline: a decade debating the Unlinkability of (UK) BAC

2010 — **false unlinkability proof.** *Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. CSF'10.* Claims to have proof of strong unlinkability, but none provided.

2012 — **false attack.** *Vincent Cheval. PhD Thesis.* ProVerif improved, but diff-equivalence will always find false unlinkability attacks.

Timeline: a decade debating the Unlinkability of (UK) BAC

2010 — **false unlinkability proof.** *Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. CSF'10.* Claims to have proof of strong unlinkability, but none provided.

2012 — **false attack.** *Vincent Cheval. PhD Thesis.* ProVerif improved, but diff-equivalence will always find false unlinkability attacks.

2014 — **unknown outcome.** *Vincent Cheval. TACAS'15.* APTE tool for trace equivalence fails to terminate on two sessions.

Timeline: a decade debating the Unlinkability of (UK) BAC

2010 **false unlinkability proof.** *Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. CSF'10.* Claims to have proof of strong unlinkability, but none provided.

2012 **false attack.** *Vincent Cheval. PhD Thesis.* ProVerif improved, but diff-equivalence will always find false unlinkability attacks.

2014 **unknown outcome.** *Vincent Cheval. TACAS'15.* APTE tool for trace equivalence fails to terminate on two sessions.

2016 **proof of *weak* unlinkability.** Lucca Hirschi, Stéphanie Delaune, Davide Baelde. S&P'16. However, . . .

- Uses term *strong unlinkability*, despite proving results with respect to trace equivalence (explained in journal version).
- Analysis conducted under model with less observables.

Timeline: a decade debating the Unlinkability of (UK) BAC

2010 — **false unlinkability proof.** *Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. CSF'10.* Claims to have proof of strong unlinkability, but none provided.

2012 — **false attack.** *Vincent Cheval. PhD Thesis.* ProVerif improved, but diff-equivalence will always find false unlinkability attacks.

2014 — **unknown outcome.** *Vincent Cheval. TACAS'15.* APTE tool for trace equivalence fails to terminate on two sessions.

2016 — **proof of *weak* unlinkability.** Lucca Hirschi, Stéphanie Delaune, Davide Baelde. S&P'16. However, . . .

- Uses term *strong unlinkability*, despite proving results with respect to trace equivalence (explained in journal version).
- Analysis conducted under model with less observables.

2018 — **attack or proof, under differing assumptions** Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. S&P'18. DEEPSEC tool for trace equivalence. Ongoing debate on whether attack is a trace. . .

Timeline: a decade debating the Unlinkability of (UK) BAC

2010 — **false unlinkability proof.** *Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. CSF'10.* Claims to have proof of strong unlinkability, but none provided.

2012 — **false attack.** *Vincent Cheval. PhD Thesis.* ProVerif improved, but diff-equivalence will always find false unlinkability attacks.

2014 — **unknown outcome.** *Vincent Cheval. TACAS'15.* APTE tool for trace equivalence fails to terminate on two sessions.

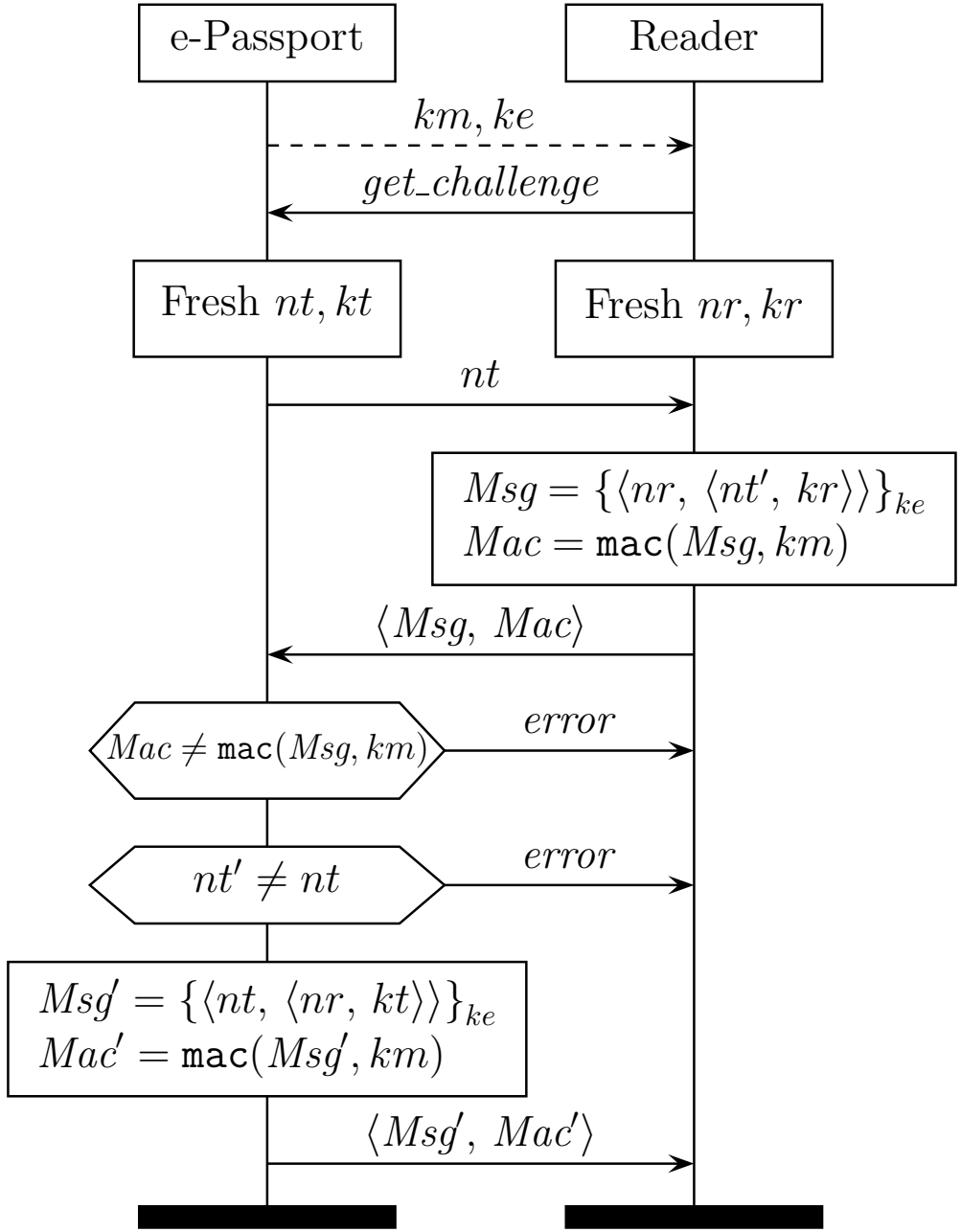
2016 — **proof of *weak* unlinkability.** Lucca Hirschi, Stéphanie Delaune, Davide Baelde. S&P'16. However, . . .

- Uses term *strong unlinkability*, despite proving results with respect to trace equivalence (explained in journal version).
- Analysis conducted under model with less observables.

2018 — **attack or proof, under differing assumptions** Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. S&P'18. DEEPSEC tool for trace equivalence. Ongoing debate on whether attack is a trace. . .

2019 — **attack on strong unlinkability — practical.** Ross Horne, Sjouke Mauw, and Zach Smith. Attack confirmed using state-of-the-art bisimilarity techniques.

ICAO 9303 BAC Protocol (UK version)



Strong Unlinkability of UK BAC (as in Arapinis et al. 2010)

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

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

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

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

Theorem

SystemUK $\not\approx$ *SpecUK.*

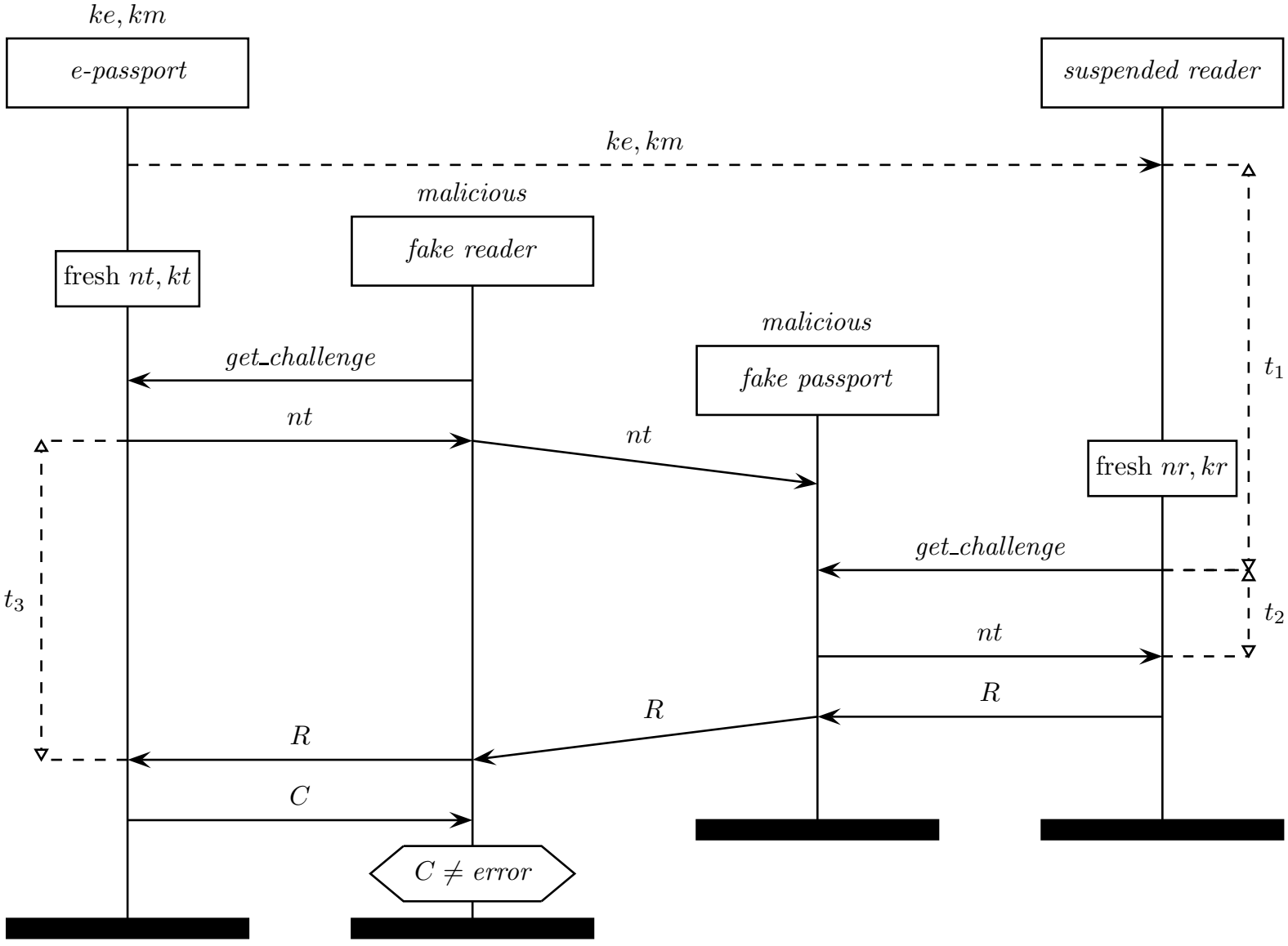
Certificate for Attack in Classical $\mathcal{FM}$

$\phi ::=$	$M = N$	equality	abbreviations:
$\mid$	$\phi \wedge \phi$	conjunction	$M \neq N \triangleq \neg(M = N)$
$\mid$	$\langle \pi \rangle \phi$	diamond	$[\pi]\phi \triangleq \neg\langle \pi \rangle \neg\phi$
$\mid$	$\neg\phi$	negation	$\phi \vee \psi \triangleq \neg(\neg\phi \wedge \neg\psi)$

$\nu\vec{x}.(\sigma \mid P) \models M = N$	iff	$M\sigma =_E N\sigma$ and $\vec{x} \cap (\mathrm{fv}(M) \cup \mathrm{fv}(N)) = \emptyset$
$A \models \langle \pi \rangle \phi$	iff	there exists B such that $A \xrightarrow{\pi} B$ and $B \models \phi$.
$A \models \phi_1 \wedge \phi_2$	iff	$A \models \phi_1$ and $A \models \phi_2$.
$A \models \neg\phi$	iff	$A \models \phi$ does not hold.

$$
\begin{aligned}
\mathit{SystemUK} \models\ & \langle \overline{c}(x) \rangle \langle \overline{c}(y) \rangle \langle d\, get \rangle \langle \overline{c}(z) \rangle (\\
& \quad z \neq get \wedge \\
& \quad [d\, z] (\\
& \qquad \langle \overline{c}(u) \rangle \langle d\, u \rangle \langle \overline{c}(v) \rangle (u \neq get \wedge v \neq get \wedge v \neq error) \\
& \qquad \vee \\
& \qquad [\overline{c}(w)](w = get) \\
& \quad) \\
&) \\
\end{aligned}
$$

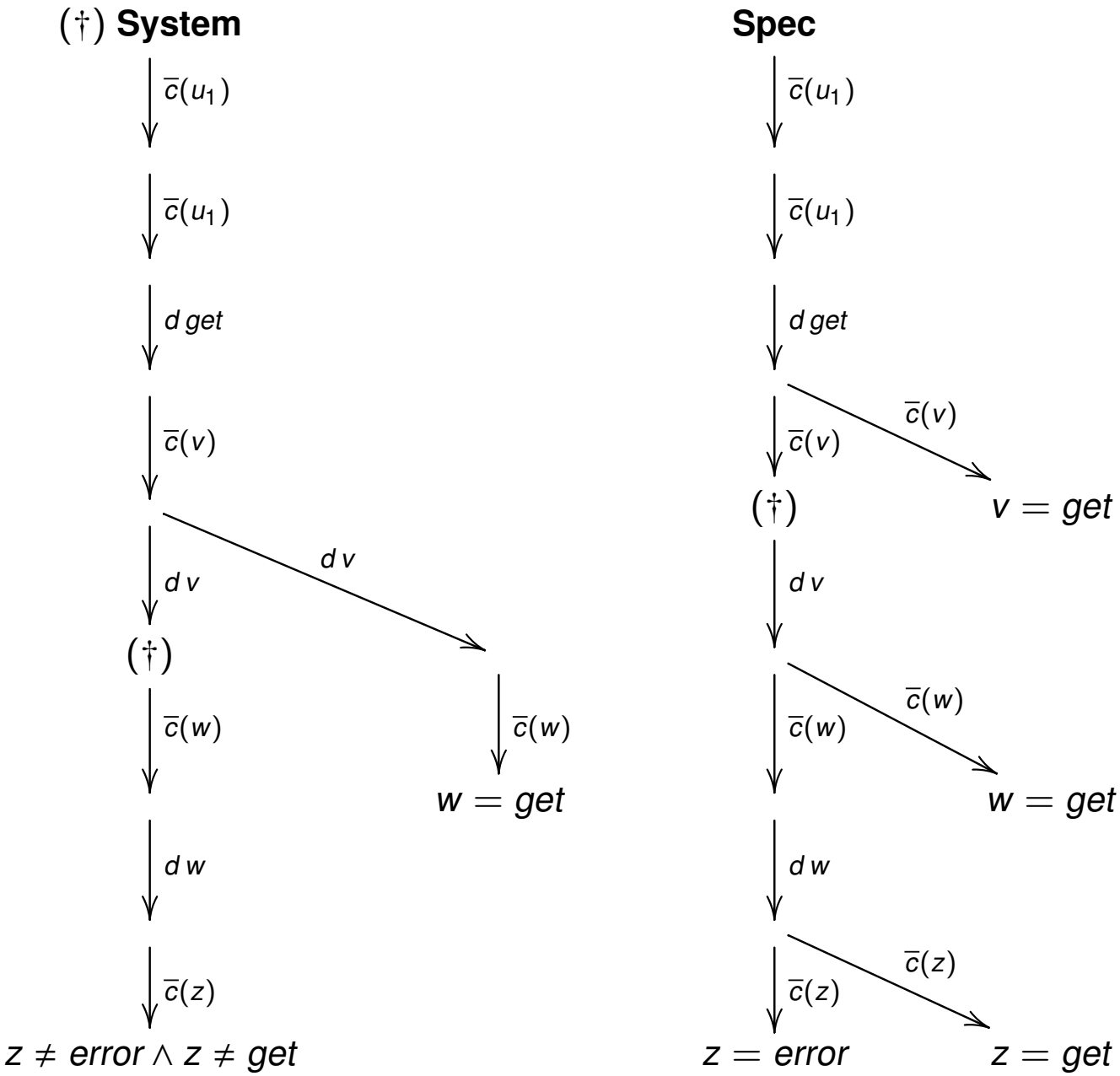
Practicalities of Attack, informally



Assume $Msg = \{\langle nr, \langle nt, kr\rangle\rangle\}_{ke}$, $R = \langle Msg, \mathtt{mac}(Msg, km)\rangle$

and $Msg' = \{\langle nt, \langle nr, kt\rangle\rangle\}_{ke}$, $C = \langle Msg', \mathtt{mac}(Msg', km)\rangle$.

The distinguishing strategy behind the distinguishing formula



A Reformulation of Unlinkability

- Reduce weak to equivalent strong bisimilarity problem.
- Make oberserving session initialisation less ad hoc.

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

$$
\begin{aligned}
\mathit{Reader}(c, ke, km) \triangleq \quad & c(nt).\nu nr.\nu kr. \\
& \mathtt{let}\ m = \{\langle nr, \langle nt, kr\rangle\rangle\}_{ke}\ \mathtt{in} \\
& \overline{c}\langle m, \mathtt{mac}(\langle m, km\rangle)\rangle
\end{aligned}
$$

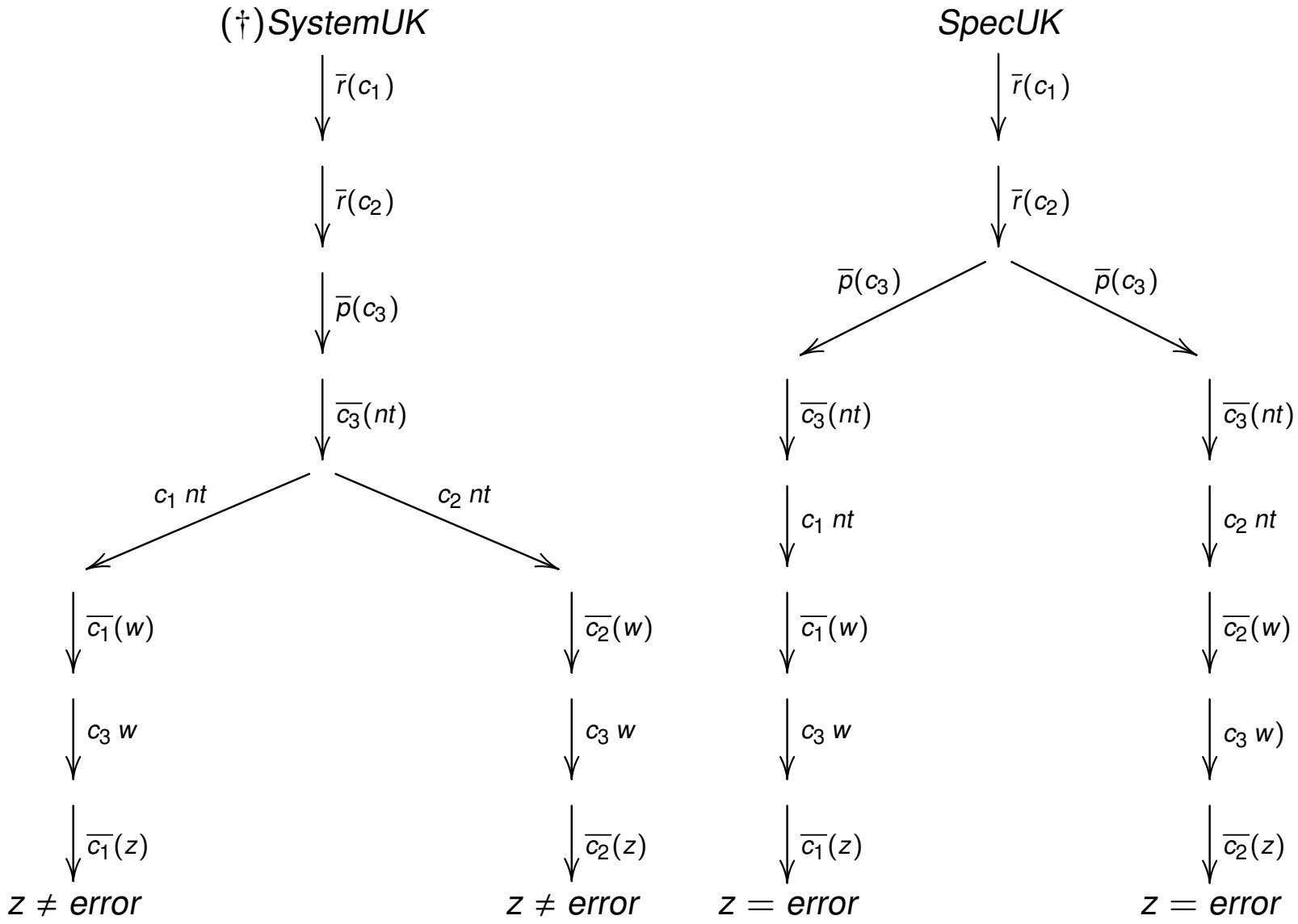
$$\mathit{SystemUK} \triangleq \quad !\nu ke.\nu km.!(\nu c.\overline{r}\langle c\rangle.\mathit{Reader}(c, ke, km) \mid \nu c.\overline{p}\langle c\rangle.\mathit{MainUK}(c, ke, km))$$

$$\mathit{SpecUK} \triangleq \quad !\nu ke.\nu km.(\nu c.\overline{r}\langle c\rangle.\mathit{Reader}(c, ke, km) \mid \nu c.\overline{p}\langle c\rangle.\mathit{MainUK}(c, ke, km))$$

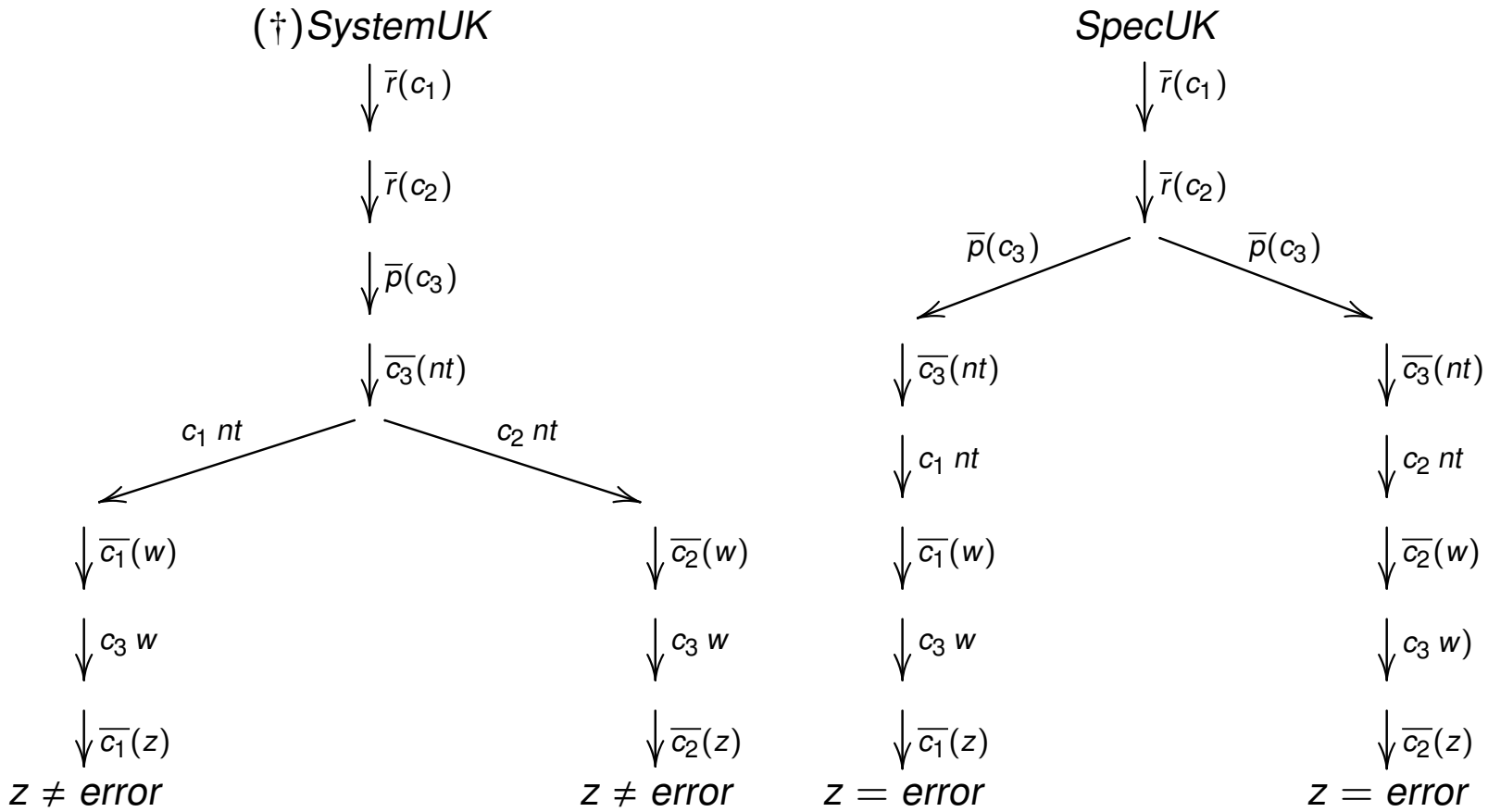
Theorem

$\mathit{SystemUK} \not\sim \mathit{SystemUK}'$.

Distinguishing Games Become Cleaner



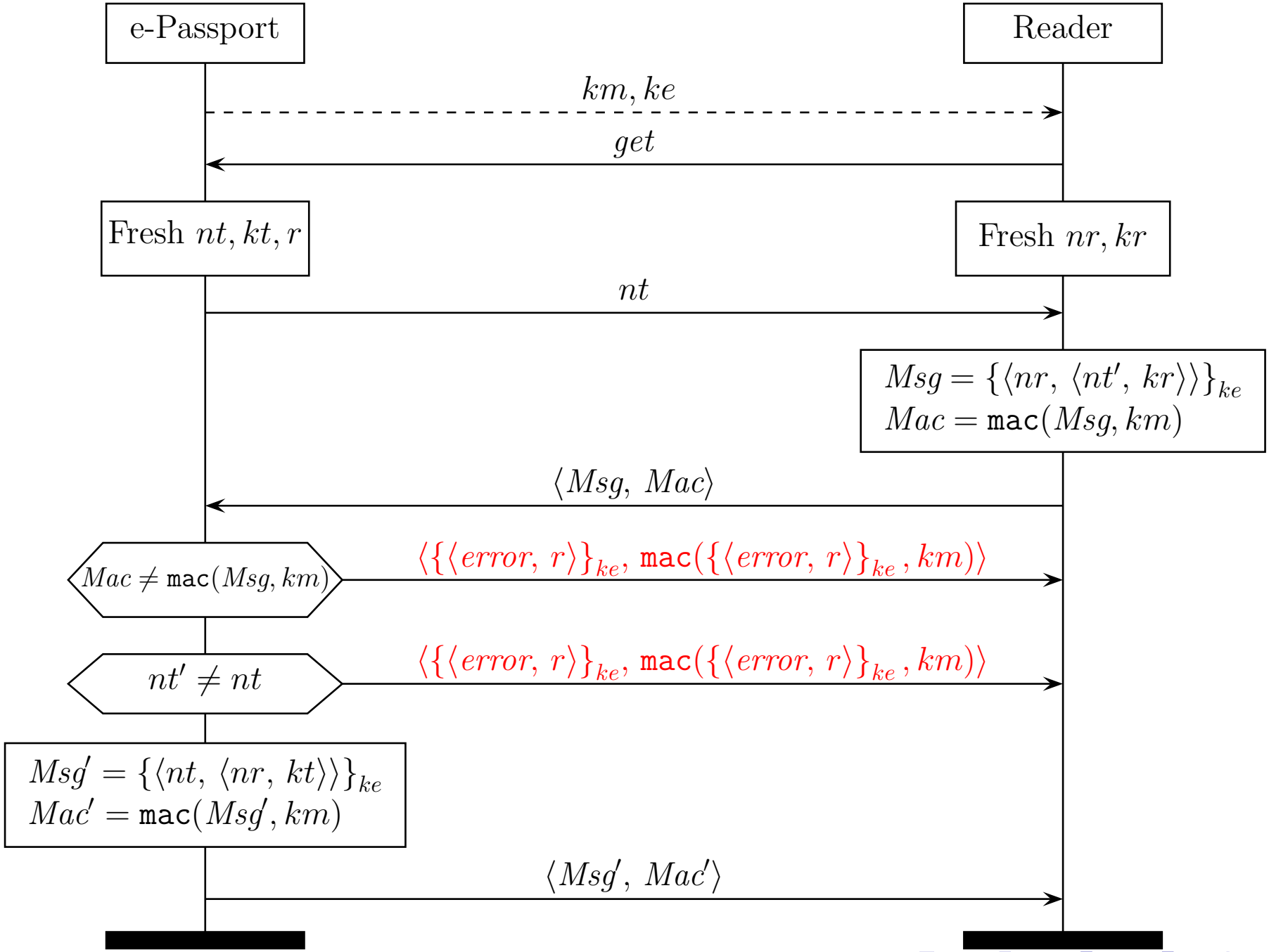
Distinguishing formula corresponding to game



$$\varphi \triangleq \langle \overline{r}(c_1) \rangle \langle \overline{r}(c_2) \rangle \langle \overline{p}(c_3) \rangle \langle \overline{c_3}(nt) \rangle (\langle c_1\ nt \rangle \langle \overline{c_1}(w) \rangle \langle c_3\ w \rangle \langle \overline{c_3}(z) \rangle (z \neq error) \wedge \langle c_2\ nt \rangle \langle \overline{c_2}(w) \rangle \langle c_3\ w \rangle \langle \overline{c_3}(z) \rangle (z \neq error))$$

$SystemUK \models \varphi$ $\quad$ $SpecUK \not\models \varphi$

Fix ICAO 9303 BAC Standard: Probabilistically Encrypt Error Message



Strong unlinkability of fixed BAC protocol, within scope of ICAO 9303

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

$$
\begin{aligned}
Reader(c, ke, km) \triangleq \quad & c(nt).\nu nr.\nu kr. \\
& \mathtt{let}\ m = \{\langle nr, \langle nt, kr\rangle\rangle\}_{ke}\ \mathtt{in} \\
& \overline{c}\langle m, \mathtt{mac}(\langle m, km\rangle)\rangle
\end{aligned}
$$

$$SystemOK \triangleq \quad !\nu ke.\nu km.!(\nu c.\overline{r}\langle c\rangle.Reader(c, ke, km) \mid \nu c.\overline{p}\langle c\rangle.MainOK(c, ke, km))$$

$$SpecOK \triangleq \quad !\nu ke.\nu km.(\nu c.\overline{r}\langle c\rangle.Reader(c, ke, km) \mid \nu c.\overline{p}\langle c\rangle.MainOK(c, ke, km))$$

Theorem

SystemOK $\sim$ *SpecOK.*

Lessons learned for verification

Should avoid mistaken claims (e.g., *SystemUK* $\approx$ *SpecUK* in Arapinis et al. 2010), by improving methods and tools for equivalence checking.

Our method:

- Reduce to equivalent strong bisimilarity problem, thereby avoiding image-finiteness issues.
- **Quasi-open bisimilarity** was used to find our attack quickly and systematically.
- **An intuitionistic modal logic** $\mathcal{FM}$ was used to confirm the attack.
- Finally we check the attack also holds under **classical assumptions**.

When unlinkability holds, construct a **quasi-open bisimulation** as a witness.

Privacy properties are subtle, so are more sensitive to different **equivalences** than security properties.

Conclusion: impact for society

Responsible disclosure: ICAO have been notified.

Manufacturers of **e-passport readers** should take responsibility.

Conclusion: impact for society

ICAO publicly confirm the vulnerability: “the described issue, which could be exploited for example at border controls or at other inspection system areas, would only allow adversaries to be able to know that somebody recently passed through a passport check– and even without opening their ePassport.” — office of the secretary general of ICAO