# Compositional Analysis of Protocol Equivalence in the Applied Pi-Calculus Using Quasi-Open Bisimilarity


Semyon Yurkov

uni.lu
UNIVERSITÉ DU LUXEMBOURG


STEP Seminar
17 November 2023


Luxembourg National Research Fund

Supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared.

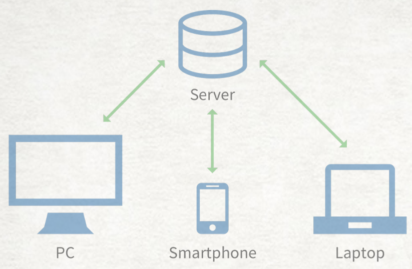
# PAPERS

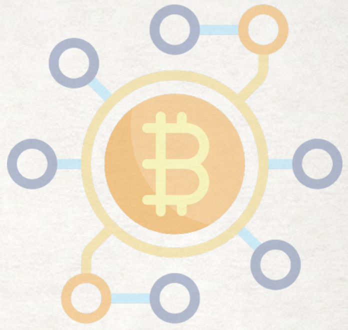
* HORNE, Ross; MAUW, Sjouke; YURKOV, Semen. When privacy fails, a formula describes an attack: A complete and compositional verification method for the applied Pi-calculus. *Theoretical Computer Science*, 2023, 959: 113842.

* HORNE, Ross; MAUW, Sjouke; YURKOV, Semen. Unlinkability of an improved key agreement protocol for EMV 2nd gen payments. In: *2022 IEEE 35th Computer Security Foundations Symposium (CSF)*.

Click on the title to view the article, both are downloadable.

# CRYPTOGRAPHIC PROTOCOLS



(Hi, It's) **Alice** →

← (Hi, It's) **Bob**

(Send BTC to) →

Symbolic verification: "Is my protocol designed correctly?"

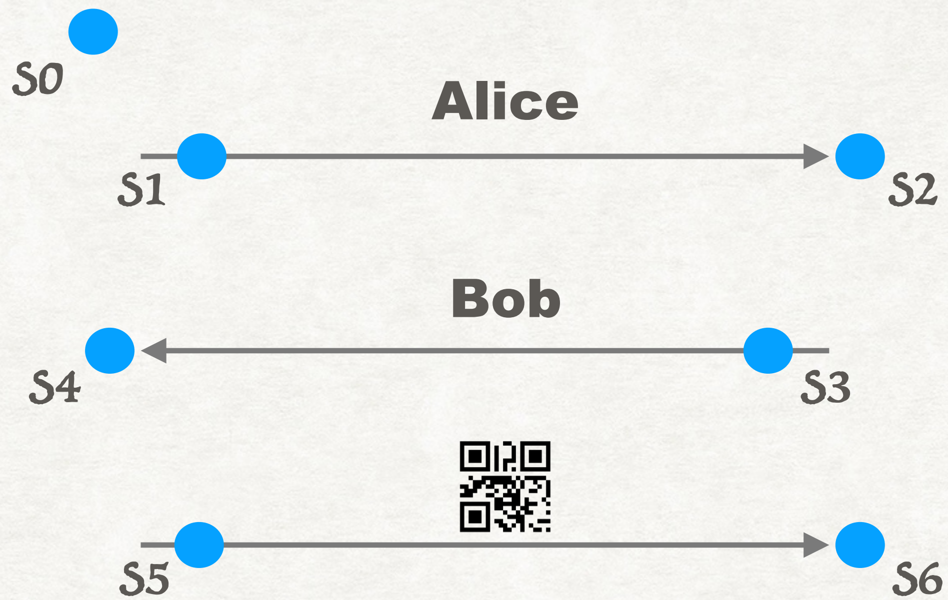
**Alice** →

← **Bob**

→

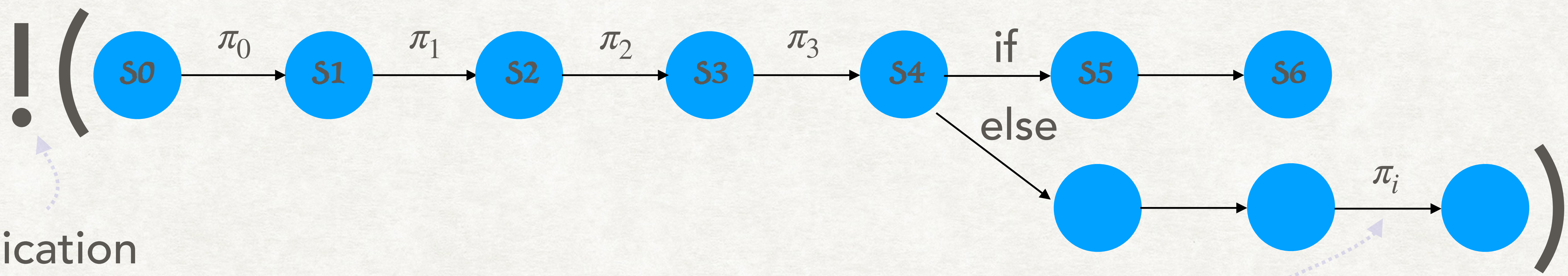
- Security property of *authentication* is not ensured.
- Privacy property of *unlinkability* is not ensured.

# PROTOCOL'S BEHAVIOUR = LABELLED TRANSITION SYSTEM = PROCESS




State =

- private values (keys, nonces)
- messages exposed to the environment
- available actions

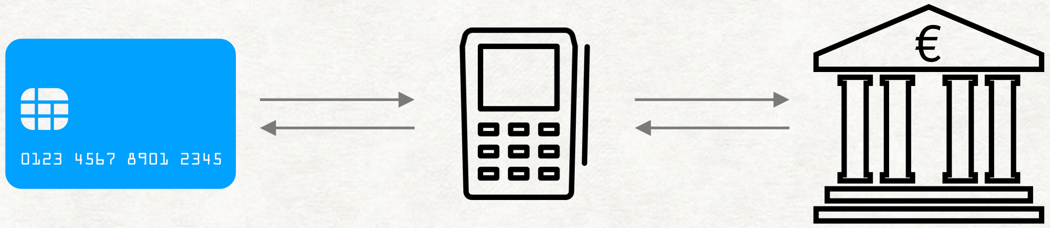


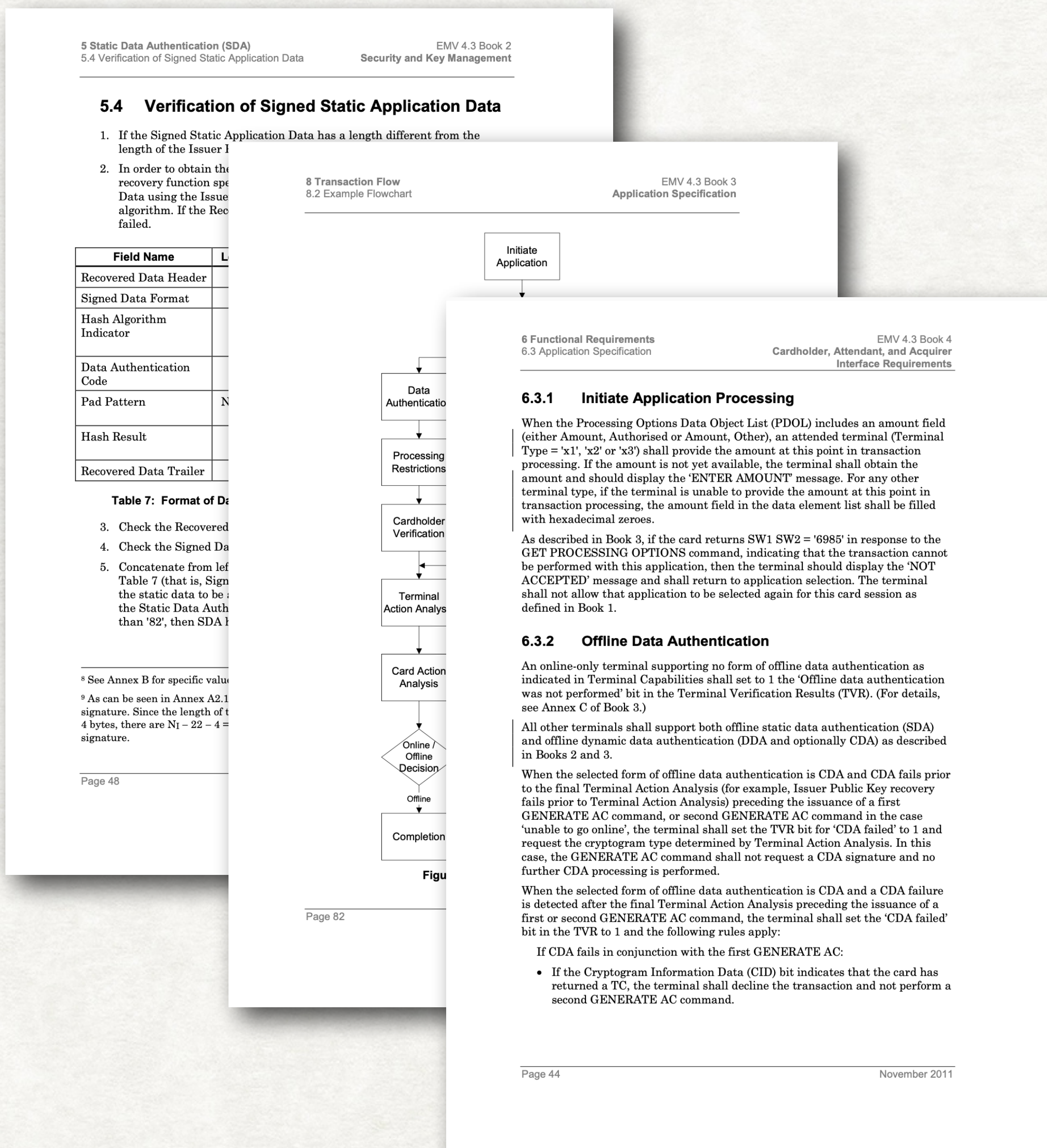

Replication
(infinitely many protocol sessions)

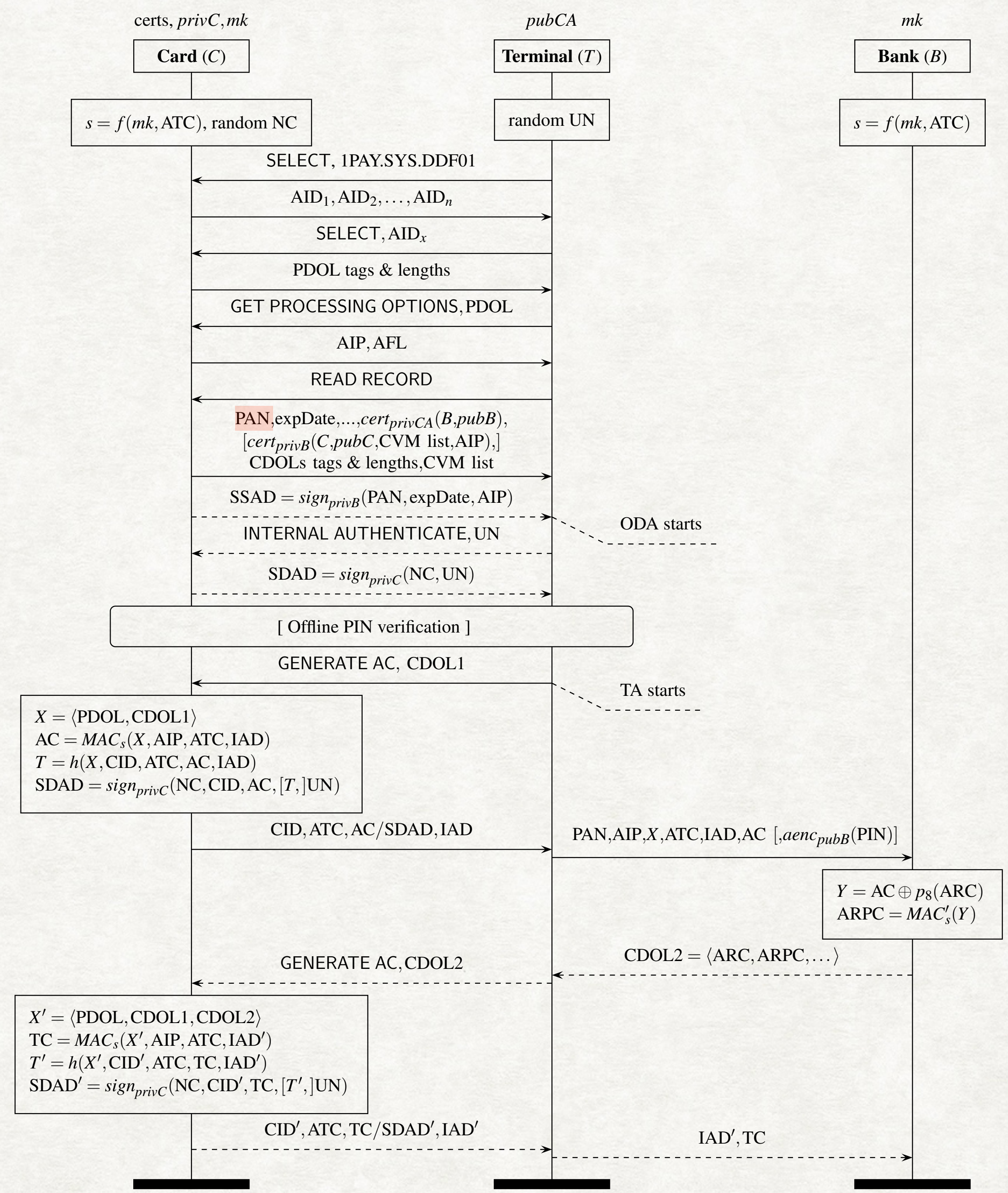
Label
(input / output / internal computation)

$$\nu \mathsf{ch} \,.\, \overline{out}\langle \mathsf{ch} \rangle \,.\, !\Big( \overline{\mathsf{ch}}\langle \mathsf{Alice} \rangle \,.\, \mathsf{ch}(x) \,.\, \mathsf{if}\ x = \mathsf{Bob}\ \mathsf{then}\ \nu \mathtt{QR} \,.\, \overline{\mathsf{ch}}\langle \mathtt{QR} \rangle \mid \mathsf{ch}(y) \,.\, \mathsf{if}\ y = \mathsf{Alice}\ \mathsf{then}\ \overline{\mathsf{ch}}\langle \mathsf{Bob} \rangle \,.\, \mathsf{ch}(z) \Big)$$

# EMV: AN EXAMPLE OF A REAL-WORLD PROTOCOL




*The EMV Standard: Break, Fix, Verify* David Basin, Ralf Sasse, and Jorge Toro-Pozo (S&P

$$\nu s.\overline{out}\langle \mathtt{pk}(s)\rangle.\Big(!\nu ch.\overline{card}\langle ch\rangle.C(ch, s, \ldots) \;\mid\; !ch.\overline{term}\langle ch\rangle.T(ch, \mathtt{pk}(s), \ldots) \;\mid\; !ch.\overline{card}\langle ch\rangle.B(ch \ldots)\Big)$$

# THE APPLIED PI-CALCULUS

Equational theory axiomatises cryptographic functions

| | | |
|---|---|---|
| $M, N, K ::= x$ | variable | |
| $\mid \mathrm{pk}(M)$ | public key | $\mathtt{fst}(\langle M, N\rangle) =_E M$ |
| $\mid \mathrm{h}(M)$ | hash | |
| $\mid \langle M, N\rangle$ | tuple | $\mathtt{snd}(\langle M, N\rangle) =_E N$ |
| $\mid \mathtt{aenc}(M, N)$ | asymmetric encryption | $\mathtt{adec}(\mathtt{aenc}(M, \mathrm{pk}(K)), K) =_E M$ |
| $\mid \mathtt{adec}(M, N)$ | asymmetric decryption | |
| $\mid \mathtt{fst}(M)$ | left | |
| $\mid \mathtt{snd}(M)$ | right | |

- free variables: x, y
- bound: z, w

## Syntax for processes

| | |
|---|---|
| $P, Q ::= 0$ | deadlock |
| $\mid \overline{M}\langle N\rangle.P$ | send |
| $\mid M(y).P$ | receive |
| $\mid [M = N]P$ | match |
| $\mid [M \neq N]P$ | mismatch |
| $\mid \nu x.P$ | new |
| $\mid P \mid Q$ | parallel |
| $\mid P + Q$ | choice |
| $\mid !P$ | replication |

## Transitions

$$\nu z.\overline{x}\langle z, y\rangle.z(w) \xrightarrow{\overline{x}(v)} \nu z.\left(\left\{{}^{\langle z,y\rangle}/_{v}\right\} \mid z(w)\right)$$

$$\nu z.\left(\left\{{}^{\langle z,y\rangle}/_{v}\right\} \mid z(w)\right) \xrightarrow{\mathtt{fst}(v)\ x} \nu z.\left(\left\{{}^{\langle z,y\rangle}/_{v}\right\} \mid 0\right)$$

States (extended processes) $\nu\vec{z}\,.\,(\sigma \mid P)$

private values (keys, nonces).(messages (and aliases!) exposed to the environment | available actions)

# OPEN EARLY LABELLED TRANSITION SYSTEM

LABELLED TRANSITION SYSTEM

$$\frac{M\sigma =_E K}{\vec{z}\colon \sigma \mid K(x).P \xrightarrow{M\,N} \sigma \mid P\left\{{}^{N\sigma}/_{x}\right\}}\ \textsc{Inp} \qquad \frac{x \# M, N, P, \sigma, \vec{z} \qquad M\sigma =_E K}{\vec{z}\colon \sigma \mid \overline{K}\langle N\rangle.P \xrightarrow{\overline{M}(x)} \left\{{}^{N}/_{x}\right\} \circ \sigma \mid P}\ \textsc{Out}$$

$$\frac{\vec{z}\colon \sigma \mid P \xrightarrow{\pi} A}{\vec{z}\colon \sigma \mid P + Q \xrightarrow{\pi} A}\ \textsc{Sum-l} \qquad \frac{\vec{z}\colon \sigma \mid Q \xrightarrow{\pi} A}{\vec{z}\colon \sigma \mid P + Q \xrightarrow{\pi} A}\ \textsc{Sum-r}$$

$$\frac{\vec{z}\colon \sigma \mid P \xrightarrow{\pi} A \qquad M =_E N}{\vec{z}\colon \sigma \mid [M = N]P \xrightarrow{\pi} A}\ \textsc{Mat} \qquad \frac{\vec{z}\colon \sigma \mid P \xrightarrow{\pi} A \qquad \vec{z} \models M \neq N}{\vec{z}\colon \sigma \mid [M \neq N]P \xrightarrow{\pi} A}\ \textsc{Mismatch}$$

$$\frac{\vec{z}, x\colon \sigma \mid P \xrightarrow{\pi} B \qquad x \# \vec{z}, \sigma, \mathrm{n}(\pi)}{\vec{z}\colon \sigma \mid \nu x.P \xrightarrow{\pi} \nu x.B}\ \textsc{Extrude} \qquad \frac{\vec{z}, x\colon A \xrightarrow{\pi} B \qquad x \# \vec{z}, \mathrm{n}(\pi)}{\vec{z}\colon \nu x.A \xrightarrow{\pi} \nu x.B}\ \textsc{Res}$$

$$\frac{\vec{z}\colon \sigma \mid P \xrightarrow{\pi} \nu\vec{x}.(\sigma \mid R) \qquad \vec{x} \cup \mathrm{bn}(\pi) \# Q}{\vec{z}\colon \sigma \mid P \mid Q \xrightarrow{\pi} \nu\vec{x}.(\sigma \mid R \mid Q)}\ \textsc{Par-l} \qquad \frac{\vec{z}\colon \sigma \mid Q \xrightarrow{\pi} \nu\vec{x}.(\sigma \mid R) \qquad \vec{x} \cup \mathrm{bn}(\pi) \# P}{\vec{z}\colon \sigma \mid P \mid Q \xrightarrow{\pi} \nu\vec{x}.(\sigma \mid P \mid R)}\ \textsc{Par-r}$$

$$\mathrm{n}(\pi) = \begin{cases} \mathrm{fv}(M) \cup \{x\} & \text{if } \pi = \overline{M}(x) \\ \mathrm{fv}(M) \cup \mathrm{fv}(N) & \text{if } \pi = M\,N \\ \emptyset & \text{otherwise} \end{cases} \qquad \mathrm{bn}(\pi) = \begin{cases} \{x\} & \text{if } \pi = \overline{M}(x) \\ \emptyset & \text{otherwise} \end{cases}$$

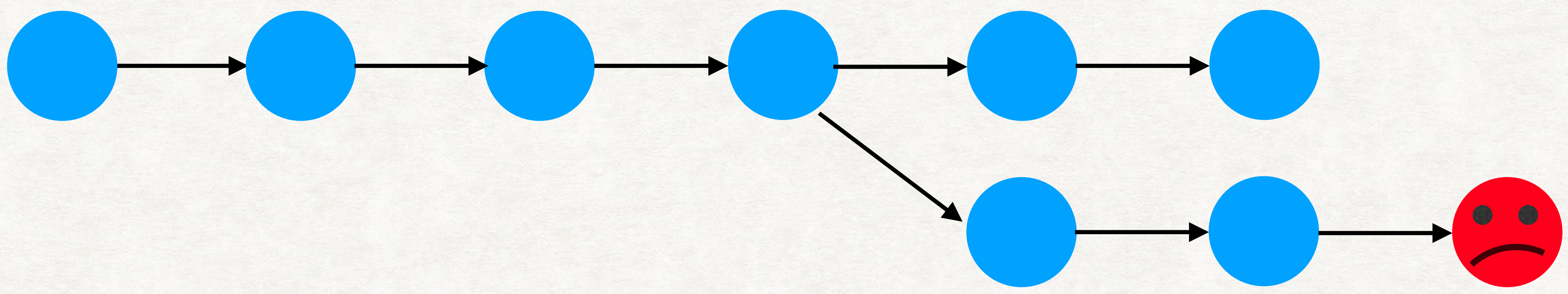
$$\frac{\vec{z}\colon \sigma \mid P \xrightarrow{\overline{M}(x)} \nu\vec{y}.\left(\left\{{}^{N}/_{x}\right\} \circ \sigma \mid P'\right) \qquad \vec{z}\colon \sigma \mid Q \xrightarrow{M\,N} \nu\vec{w}.(\sigma \mid Q') \qquad \{x\} \cup \vec{y} \# Q \qquad \vec{w} \# P, \vec{y}}{\vec{z}\colon \sigma \mid P \mid Q \xrightarrow{\tau} \nu\vec{y}, \vec{w}.(\sigma \mid P' \mid Q')}\ \textsc{Close-l}$$

$$\frac{\vec{z}\colon \sigma \mid P \xrightarrow{M\,N} \nu\vec{y}.(\sigma \mid P') \qquad \vec{z}\colon \sigma \mid Q \xrightarrow{\overline{M}(x)} \nu\vec{w}.\left(\left\{{}^{N}/_{x}\right\} \circ \sigma \mid Q'\right) \qquad \{x\} \cup \vec{w} \# P \qquad \vec{y} \# Q, \vec{w}}{\vec{z}\colon \sigma \mid P \mid Q \xrightarrow{\tau} \nu\vec{y}, \vec{w}.(\sigma \mid P' \mid Q')}\ \textsc{Close-r}$$

$$\frac{\vec{z}\colon \sigma \mid P \xrightarrow{\pi} \nu\vec{x}.(\sigma \mid Q) \qquad \vec{x} \cup \mathrm{bn}(\pi) \# P}{\vec{z}\colon \sigma \mid\, !P \xrightarrow{\pi} \nu\vec{x}.(\sigma \mid Q \mid\, !P)}\ \textsc{Rep-act}$$

$$\frac{\vec{z}\colon \sigma \mid P \xrightarrow{\overline{M}(x)} \nu\vec{y}.\left(\left\{{}^{N}/_{x}\right\} \circ \sigma \mid Q\right) \qquad \vec{z}\colon \sigma \mid P \xrightarrow{M\,N} \nu\vec{w}.(\sigma \mid R) \qquad \vec{y} \# P, \vec{w} \qquad \vec{w} \# P}{\vec{z}\colon \sigma \mid\, !P \xrightarrow{\tau} \nu\vec{y}, \vec{w}.(\sigma \mid Q \mid R \mid\, !P)}\ \textsc{Rep-close}$$

# REACHABILITY (SECURITY)



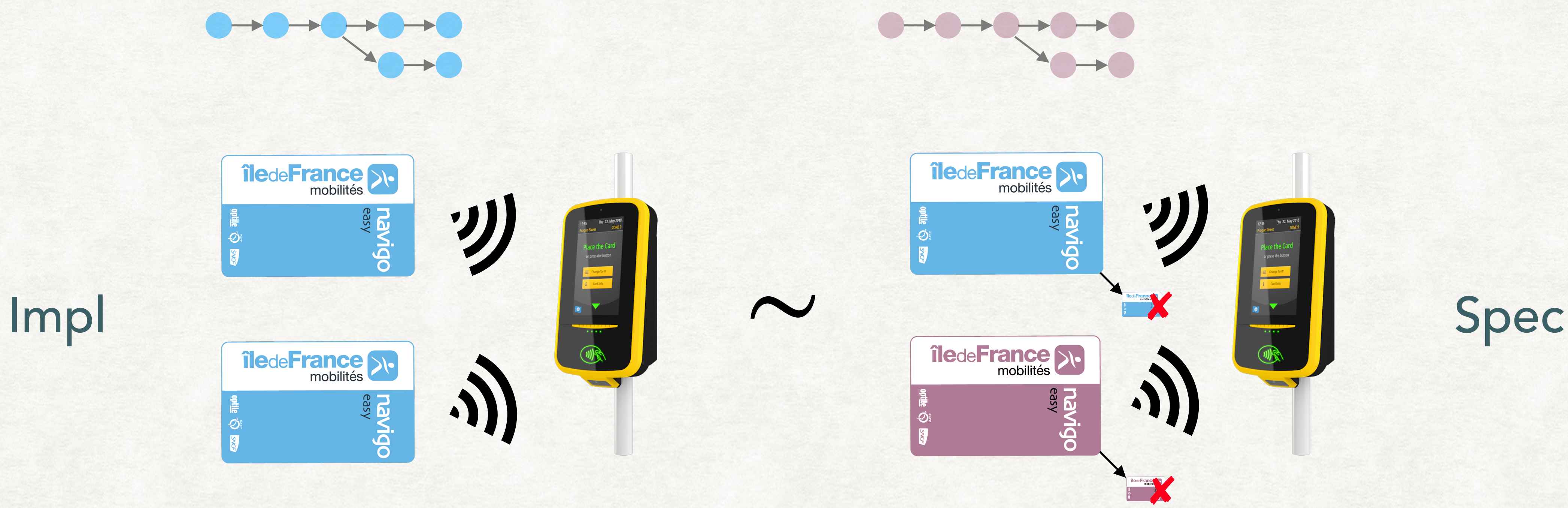
An attacker interacting with the system cannot force the system to reach a "bad" state where a property (***authentication***, *secrecy*) is violated.

* There is a powerful default (Dolev-Yao) attacker capable of: intercepting, blocking, modifying or injecting messages.

* Well-developed tool support

— ProVerif, Tamarin

# INDISTINGUISHABILITY (PRIVACY)




An attacker interacting with the system cannot distinguish between the idealised system Spec, where the target property (***unlinkability***, *anonymity*) definitely holds, and the real-world system Impl.

- No default attacker (no default $\sim$ )
- Limited tool support

— DeepSec, ProVerif

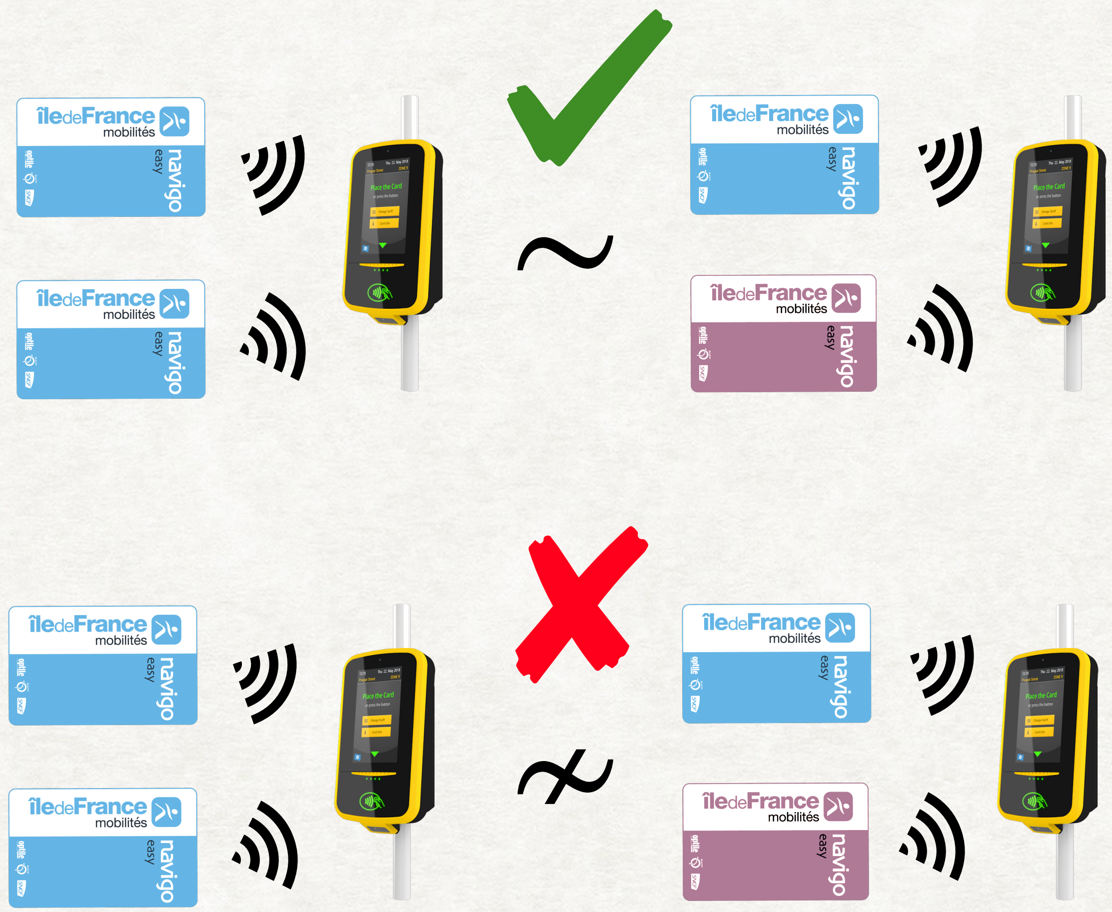
# RESEARCH QUESTIONS

***Q1: Can we identify the requirements for an equivalence notion suitable for modelling indistinguishability properties of security protocols?***

***Q2: Can we identify a canonical equivalence notion satisfying the identified demands?***

***Q3: Can we reason effectively about protocols using the identified equivalence?***

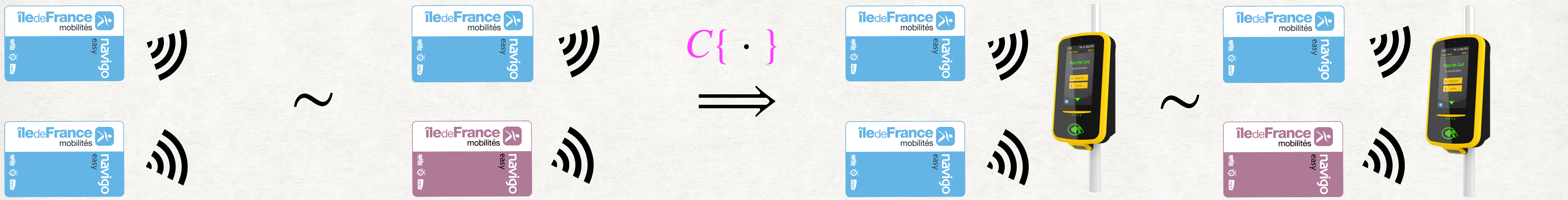
# REQUIREMENT 1: CLEAR VERIFICATION OUTCOME




$\text{Impl} \not\models \phi$ $\text{Spec} \models \phi$

**R1**: Whenever the property fails there is a formula $\phi$ describing a testable attack.

# REQUIREMENT 2: CONGRUENCE

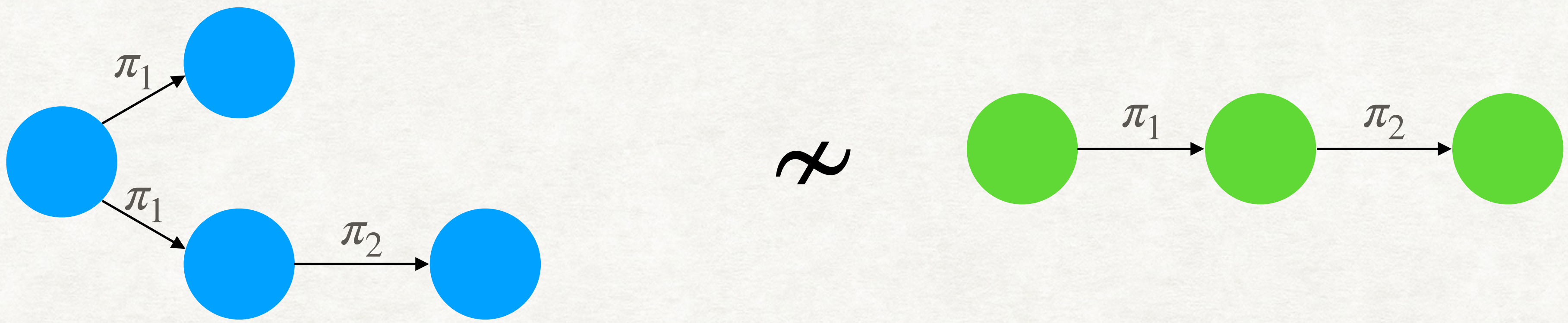



Small_Impl $\sim$ Small_Spec $\Longrightarrow$ $C\{$Small_Impl$\}$ = Impl $\sim$ $C\{$Small_Spec$\}$ = Spec

**R2**: $\sim$ should be a congruence relation.

**BONUS**: When possible, we can reduce the amount of work needed for verification!

# REQUIREMENT 3: BISIMILARITY




**R3**: Attacker should be able to make decisions *dynamically*, during the execution.

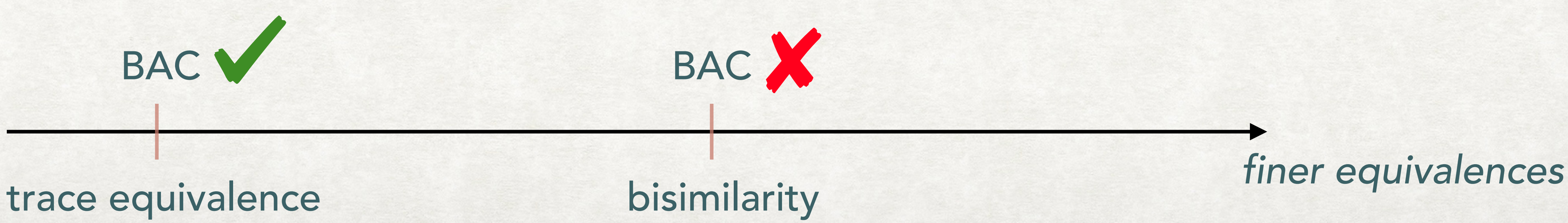
**EVIDENCE**:

- 2016: The (*correct !*) proof that the BAC protocol used in biometric passports is unlinkable in the trace equivalence-based model.

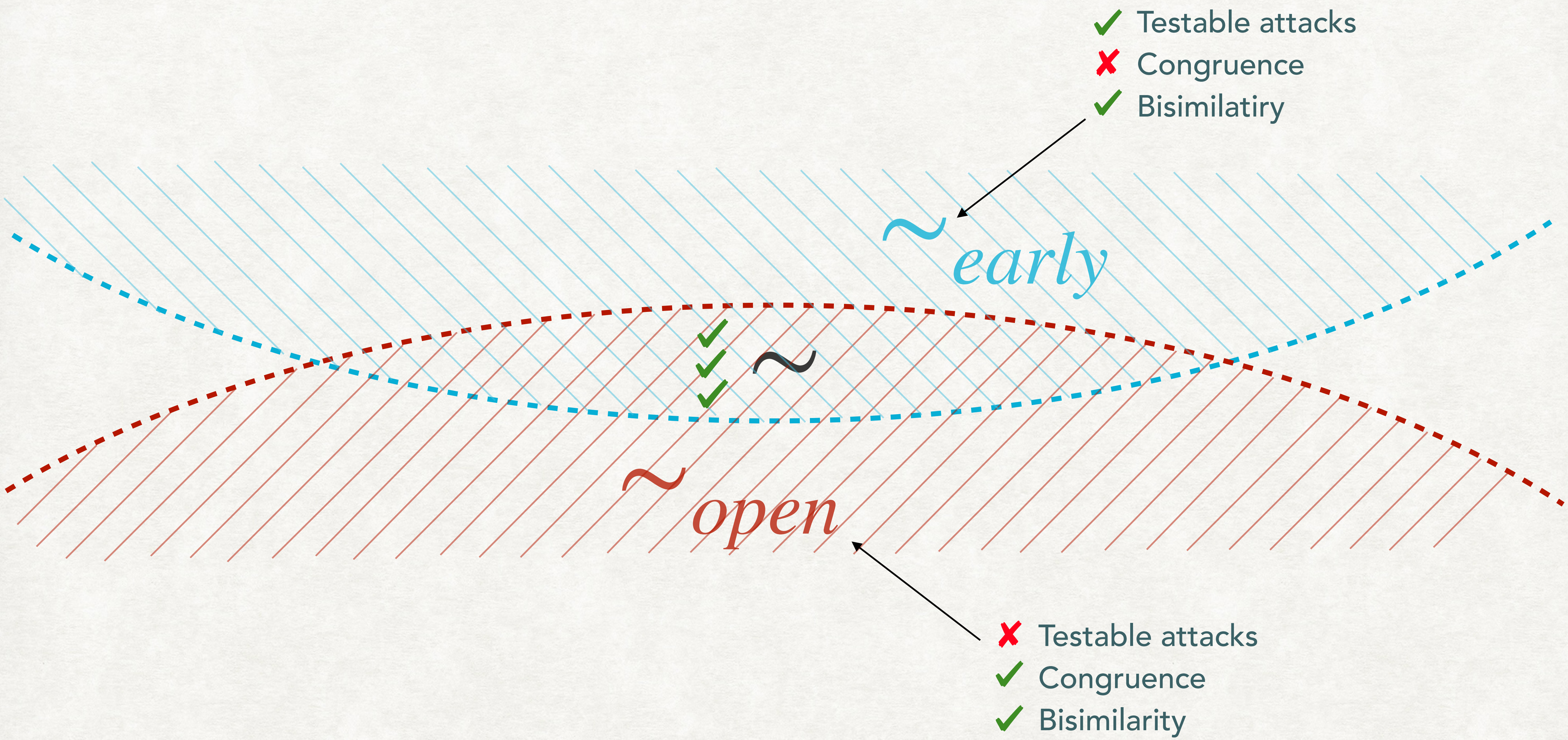
L. Hirschi, D. Baelde, and S. Delaune. A method for verifying privacy-type properties: the unbounded case (S&P).

- 2019: A (*practical !*) attack has been discovered employing the bisimilarity-based model.

I. Filimonov, R. Horne, S. Mauw, and Z. Smith. Breaking unlinkability of the ICAO 9303 standard for e-passports using bisimilarity (ESORICS).

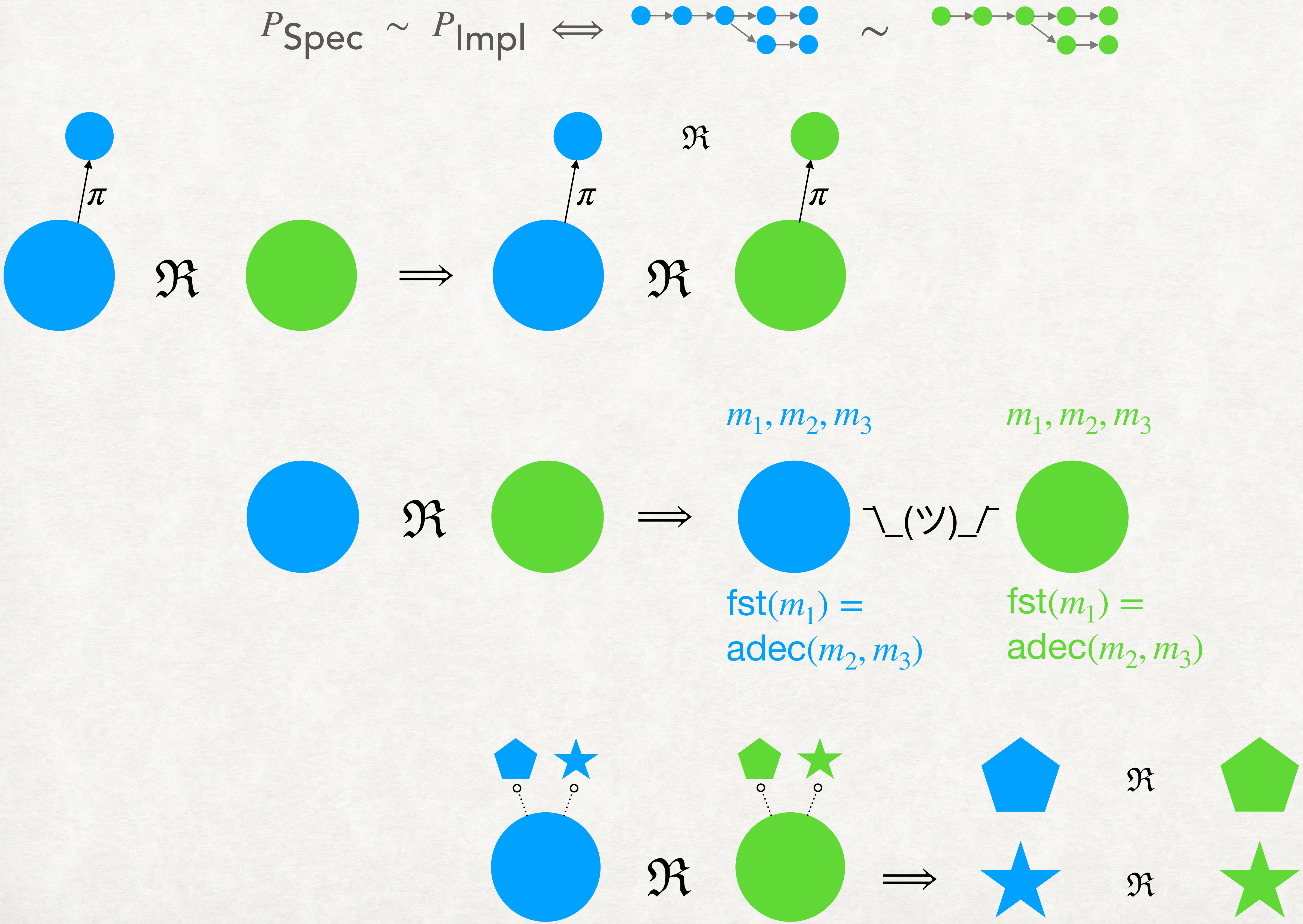


# QUASI-OPEN BISIMILARITY

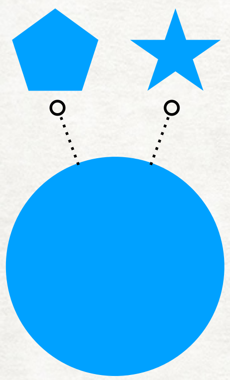



~ **quasi-open bisimilarity**: the coarsest bisimilarity congruence for the applied pi-calculus

# QUASI-OPEN BISIMILARITY



# III – MANIPULATING FREE VARIABLES



**Definition 4** (open). *A relation over extended processes* $\mathfrak{R}$ *is open whenever we have that if* $\nu\vec{x}.(\sigma \mid P) \;\mathfrak{R}\; \nu\vec{y}.(\theta \mid Q)$ *and there exist variables* $\vec{z}$ *and idempotent substitution* $\rho$ *such that:* $\vec{z} \# \sigma, P, \theta, Q$ *and* $\rho \# \vec{x}, \vec{y}, \mathrm{dom}(\sigma), \mathrm{dom}(\theta)$, *we have*

$$\nu\vec{z},\vec{x}.(\sigma \circ \rho \mid P\rho) \;\mathfrak{R}\; \nu\vec{z},\vec{y}.(\theta \circ \rho \mid Q\rho)$$

In the context of the definition above, we say that the extended process $A \triangleq \nu\vec{x}.(\sigma \mid P)$ *can access* the extended process $A' \triangleq \nu\vec{z},\vec{x}.(\sigma \circ \rho \mid P\rho)$ by the environment extension $\nu\vec{z}.\rho$, written as $A \sqsubseteq_{\nu\vec{z}.\rho} A'$ via $\nu\vec{z}.\rho$ if $\vec{z} \# \sigma, P$ and $\rho \# \vec{x}, \mathrm{dom}(\sigma)$.

Monotonicity lemma: if a transition $\pi$ available from the extended process *A*, it is always available in any accessible state *A'*, however accessibility may enable new transitions, not available in the original state A.

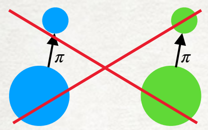
$[x \neq z]a(y).[x = y]\pi$ cannot act, since there is no evidence that *x* and *z* are different

but we can access and fix “the universe” where x and z ARE different

$$[x \neq z]a(y).[x = y]\pi \sqsubseteq_{\nu n.\{^n/_x\}} \nu n.(\{^n/_x\} \mid [n \neq z]a(y).[n = y]\pi) \xrightarrow{ax} \nu n.(\{^n/_x\} \mid [n = n]\pi)$$

$$\frac{\vec{z}\colon \sigma \mid P \xrightarrow{\pi} A \qquad M =_E N}{\vec{z}\colon \sigma \mid [M = N]P \xrightarrow{\pi} A}\;\textsc{Mat} \qquad \frac{\vec{z}\colon \sigma \mid P \xrightarrow{\pi} A \qquad \vec{z} \models M \neq N}{\vec{z}\colon \sigma \mid [M \neq N]P \xrightarrow{\pi} A}\;\textsc{Mismatch}$$

# ATTACK EXAMPLES



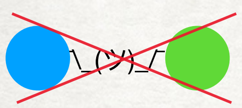
$$\nu z.\overline{x}\langle\langle z,y\rangle\rangle.z(w) \not\approx \nu z.\overline{x}\langle\langle z,y\rangle\rangle$$

$$\nu z.\overline{x}\langle z,y\rangle.z(w) \xrightarrow{\overline{x}(v)} \nu z.\left(\left\{{}^{\langle z,y\rangle}/_{v}\right\} \mid z(w)\right) \xrightarrow{\mathtt{fst}(v)\,w} \nu z.\left(\left\{{}^{\langle z,y\rangle}/_{v}\right\} \mid 0\right)$$

$$\nu z.\overline{x}\langle z,y\rangle \xrightarrow{\overline{x}(v)} \nu z.\left(\left\{{}^{\langle z,y\rangle}/_{v}\right\} \mid 0\right)$$

$$\langle\overline{a}(u)\rangle\langle\mathtt{fst}(u)\,w\rangle\mathtt{tt}$$

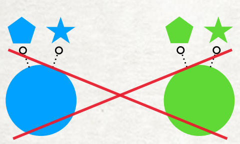
$$[\overline{a}(u)]\,[\mathtt{fst}(u)\,w]\,\mathtt{ff}$$




$$\nu m,n.\overline{a}\langle m\rangle.\overline{a}\langle n\rangle \not\approx \nu n.\overline{a}\langle n\rangle.\overline{a}\langle \mathtt{h}(n)\rangle$$

$$\langle\overline{a}(u)\rangle\langle\overline{a}(v)\rangle(v \neq \mathtt{h}(u))$$

$$[\overline{a}(u)]\,[\overline{a}(v)]\,(v = \mathtt{h}(u))$$



$$\nu x.\overline{a}\langle\mathtt{aenc}(x,z)\rangle \not\approx \nu x.\overline{a}\langle\mathtt{aenc}(\langle x,y\rangle,z)\rangle$$

under $\left\{{}^{\mathtt{pk}(w)}/_{z}\right\}$ we can reach two states that we can distinguish, i.e.

$$\nu x.\left(\left\{{}^{\mathtt{aenc}(x,z)}/_{v}\right\} \mid 0\right)\left\{{}^{\mathtt{pk}(w)}/_{z}\right\}$$

~~¯_(ツ)_/¯~~

$$\nu x.\left(\left\{{}^{\mathtt{aenc}(\langle x,y\rangle,z)}/_{v}\right\} \mid 0\right)\left\{{}^{\mathtt{pk}(w)}/_{z}\right\}$$

$$[\overline{a}(u)]\,(\mathtt{snd}(\mathtt{adec}(u,w)) \neq y)$$

$$\langle\overline{a}(u)\rangle(z = \mathtt{pk}(w) \supset \mathtt{snd}(\mathtt{adec}(u,w)) = y)$$

# QASI-OPEN BIMISILARITY IS THE COARSEST BISIMILARITY CONGRUENCE

**Theorem 3** (contexts). *If $P \sim Q$ then for all contexts $\mathcal{C}\{\cdot\}$, we have $\mathcal{C}\{P\} \sim \mathcal{C}\{Q\}$.*

**Theorem 5.** *Quasi-open bisimilarity coincides with open barbed bisimilarity.*

We say process $P$ has *barb* $M$, written $P{\downarrow}M$, whenever, for some $A$, $P \xrightarrow{\overline{M}(z)} A$, or $P \xrightarrow{M\,N} A$, that is a barb represents the ability to observe an input or output action on a channel.

**Definition 8** (open barbed bisimilarity). *An open barbed bisimulation $\mathfrak{R}$ is a symmetric relation over processes such that whenever $A \mathrel{\mathfrak{R}} B$ holds the following hold:*

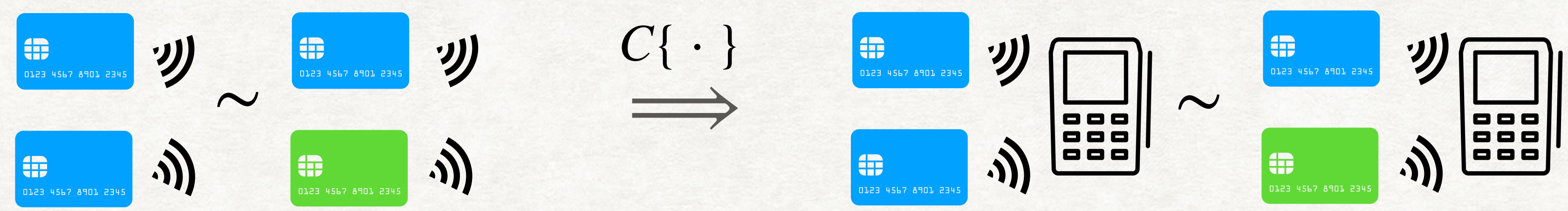
- *For all contexts $\mathcal{C}\{\,\cdot\,\}$, $\mathcal{C}\{A\} \mathrel{\mathfrak{R}} \mathcal{C}\{B\}$.*
- *If $A{\downarrow}M$ then $B{\downarrow}M$.*
- *If $A \xrightarrow{\tau} A'$, there exists $B'$ such that $B \xrightarrow{\tau} B'$ and $A' \mathrel{\mathfrak{R}} B'$ holds.*

*Processes $A$ and $B$ are open barbed bisimilar whenever there exists an open barbed bisimulation $\mathfrak{R}$ such that $A \mathrel{\mathfrak{R}} B$.*

OBB is defined to be a congruence and defined independently of the content of the messages sent and received. Due to the independence of the information on the labels, open barbed bisimilarity applies to any language.

# CONGRUENCE ENABLES COMPOSITIONAL REASONING

Lemma:




Proof.

$$C\{\ \cdot\ \} \triangleq \nu out.\Big(\ \{\ \cdot\ \} \mid out(pks).\overline{out'}\langle pks\rangle.!\nu ch_t.\overline{term}\langle ch_t\rangle.T(pks, ch_t)\Big)$$

$\blacksquare$

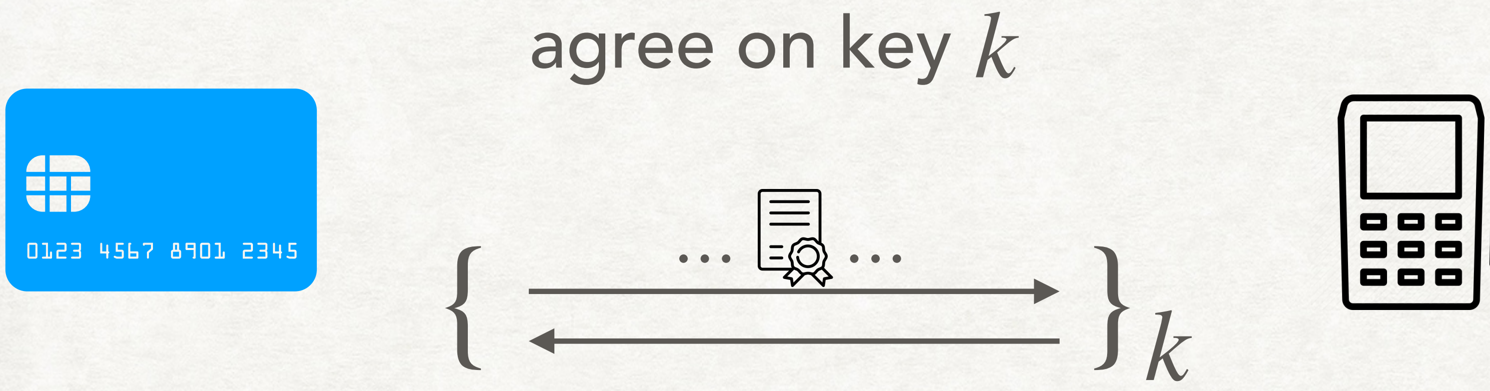
**A CARD CAN PARTICIPATE IN MANY SESSIONS**

**A CARD CAN PARTICIPATE IN ONE SESSION AT MOST**

$$\text{Impl} \triangleq \nu s.\Big( !\nu c.\ !\nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \mid \overline{out}\langle \mathtt{pk}(s)\rangle.\ \sout{ch_t.\overline{term}\langle ch_t\rangle.T(\mathtt{pk}(s), ch_t)}\Big) \sim \nu s.\Big( !\nu c.\ \nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \mid \overline{out}\langle \mathtt{pk}(s)\rangle.\ \sout{ch_t.\overline{term}\langle ch_t\rangle.T(\mathtt{pk}(s), ch_t)}\Big) \triangleq \text{Spec}$$

$$\text{Small\_Impl} \triangleq \nu s.\ \overline{out}\langle \mathtt{pk}(s)\rangle.\ !\nu c.\ !\nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \sim \nu s.\ \overline{out}\langle \mathtt{pk}(s)\rangle.\ !\nu c.\ \nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \triangleq \text{Small\_Spec}$$

# AN EXAMPLE OF THE ATTACK ON A REAL-WORLD PROTOCOL



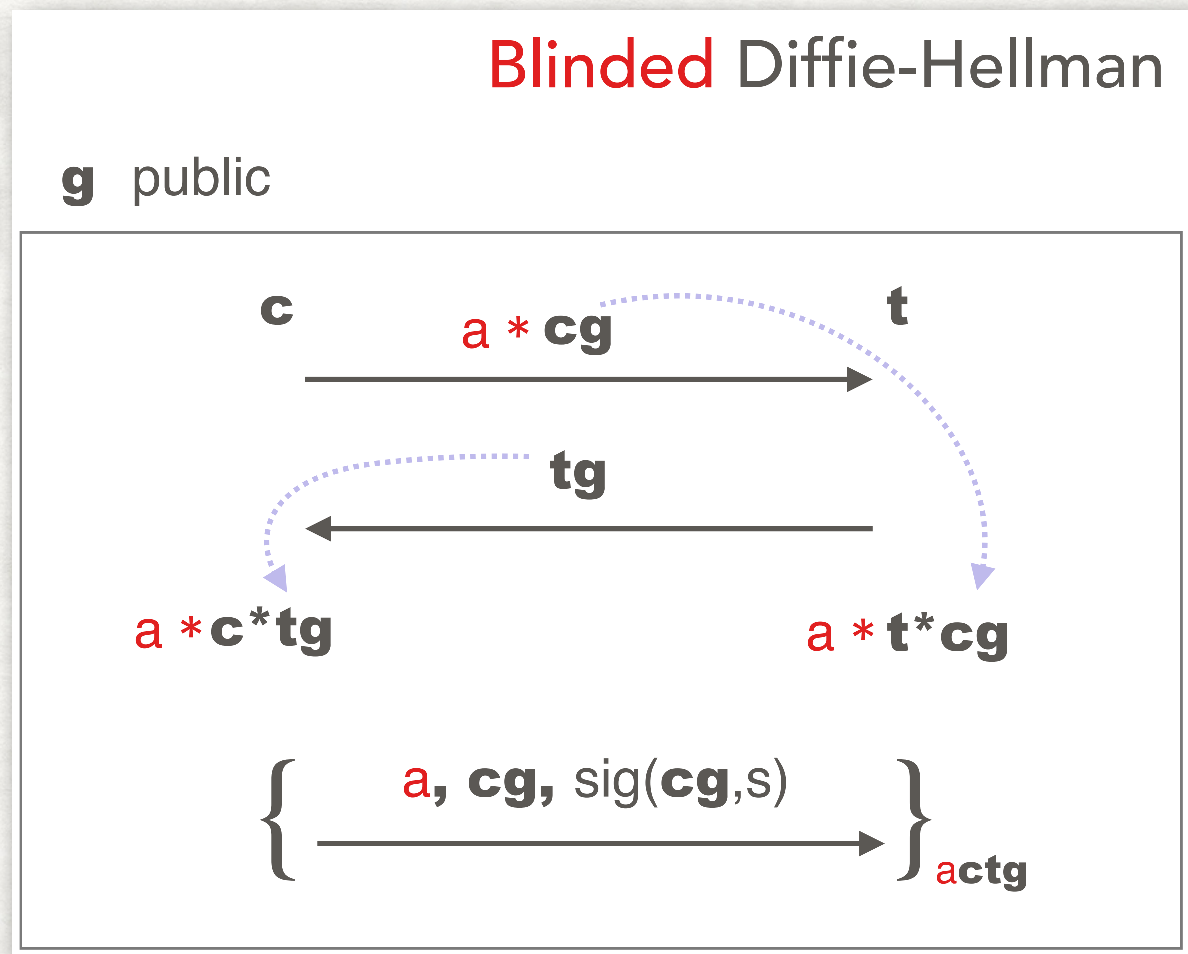

Attack scheme:

1. An active attacker powers up the card
2. Establishes a symmetric key $k$ with the card
3. Obtains the long-term identity

2012: "Blinded Diffie-Hellman RFC", EMVCo LLC

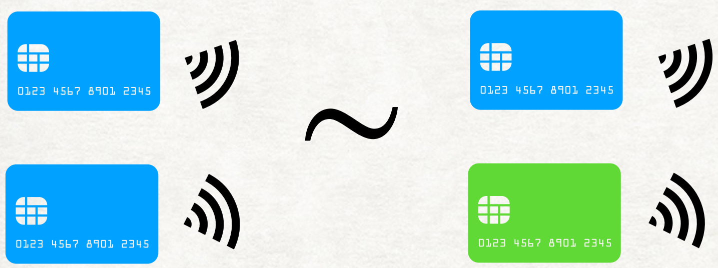
- provide authentication of the card by the terminal
- protect against eavesdropping and card tracking.

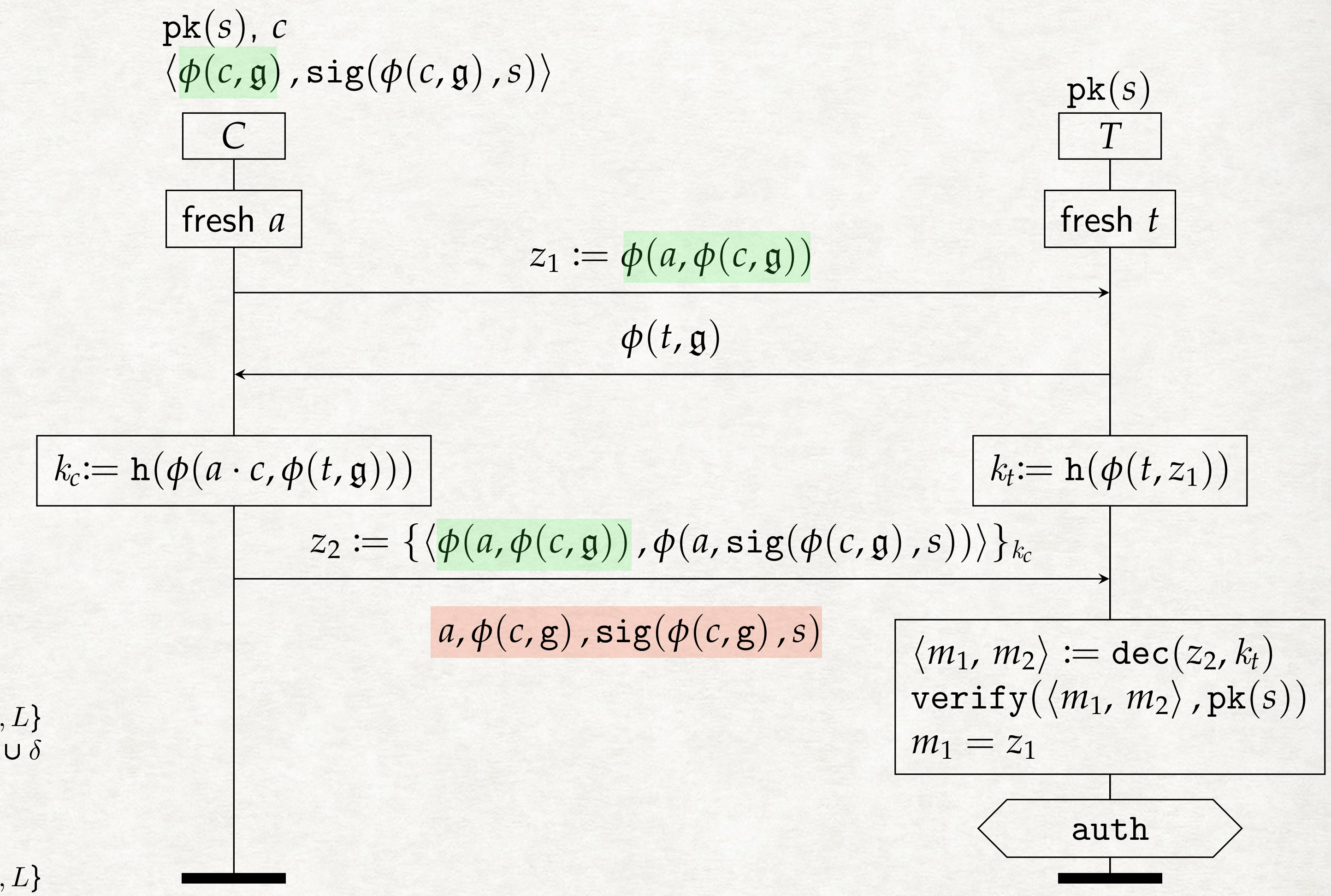

$$\phi = \begin{array}{l} \langle \overline{out}(pk_s) \rangle \\ \langle \overline{card}(u_1) \rangle \langle \overline{u_1}(v_1) \rangle \langle u_1\, \phi(y_1, \mathrm{g}) \rangle \langle \overline{u_1}(w_1) \rangle \\ \langle \overline{card}(u_2) \rangle \langle \overline{u_2}(v_2) \rangle \langle u_2\, \phi(y_2, \mathrm{g}) \rangle \langle \overline{u_2}(w_2) \rangle \\ (\mathtt{snd}(\mathtt{dec}(w_1, \mathtt{h}(\phi(y_1, v_1)))) = \mathtt{snd}(\mathtt{dec}(w_2, \mathtt{h}(\phi(y_2, v_2))))) \end{array}$$



# A PROOF OF PRIVACY OF A CORRECT PROTOCOL

Verheul condition: $\phi(a, \mathtt{sig}(M, s)) =_E \mathtt{sig}(\phi(a, M), s)$




Since we can present a relation between the states of  and  that satisfies the definition of quasi-open bisimilarity.

$$UPD_{\text{spec}} \ \mathfrak{R} \ UPD_{\text{impl}}$$

$$UPD^{\Psi}_{\text{spec}}(\vec{Y}) \triangleq \nu s, c_1, \cdots, c_L, ch_1, \cdots, ch_L, a_{l_1}, \cdots, a_{l_K}.(\sigma \mid C_1 \mid \cdots \mid C_L \mid !\nu c.\nu ch.\overline{card}\langle ch\rangle.C_{\text{upd}}(s, c, ch))$$

$$\mathfrak{R}$$

$$UPD^{\Psi,\Omega}_{\text{impl}}(\vec{Y}) \triangleq \nu s, c_1, \cdots, c_D, ch_1, \cdots, ch_L, a_{l_1}, \cdots, a_{l_K}.(\theta \mid \cdots \mid C^d_l \mid \cdots \mid !\nu ch.\overline{card}\langle ch\rangle.C_{\text{upd}}(s, c_d, ch) \mid !\nu c.!\nu ch.\overline{card}\langle ch\rangle.C_{\text{upd}}((s, ch, c)))$$

$$C_l = \begin{cases} \mathcal{E}^l(ch_l) & \text{if } l \in \alpha \\ \mathcal{F}^l(ch_l, a_l) & \text{if } l \in \beta \\ \mathcal{G}^l(ch_l, a_l, Y_l\sigma) & \text{if } l \in \gamma \\ \mathcal{H}^l & \text{if } l \in \delta \end{cases}$$

$$C^d_l = \begin{cases} \mathcal{E}^d(ch_l) & \text{if } l \in \zeta^d \cap \alpha \\ \mathcal{F}^d(ch_l, a_l) & \text{if } l \in \zeta^d \cap \beta \\ \mathcal{G}^d(ch_l, a_l, Y_l\theta) & \text{if } l \in \zeta^d \cap \gamma \\ \mathcal{H}^d & \text{if } l \in \zeta^d \cap \delta \end{cases}$$

$$\begin{array}{ll} pk_s\sigma = \mathrm{pk}(s) & \\ u_l\sigma = ch_l & \text{if } l \in \{1, \cdots, L\} \\ v_l\sigma = \phi(a_l, \phi(c_l, \mathrm{g})) & \text{if } l \in \beta \cup \gamma \cup \delta \\ w_l\sigma = m^l(a_l, Y_l\sigma) & \text{if } l \in \delta \end{array}$$

$$\begin{array}{ll} pk_s\theta = \mathrm{pk}(s) & \\ u_l\theta = ch_l & \text{if } l \in \{1, \cdots, L\} \\ v_l\theta = \phi(a_l, \phi(c_d, \mathrm{g})) & \text{if } l \in \zeta^d \cap (\beta \cup \gamma \cup \delta) \\ w_l\theta = m^d(a_l, Y_l\theta) & \text{if } l \in \zeta^d \cap \delta \end{array}$$

$$\Psi := \{\alpha, \beta, \gamma, \delta\}, \ \ \Omega := \{\zeta^1, \cdots, \zeta^D\} \text{ are partitions of } \{1, \cdots, L\}$$

$$K := |\beta \cup \gamma \cup \delta| \quad l_1, \cdots, l_K \in \beta \cup \gamma \cup \delta$$

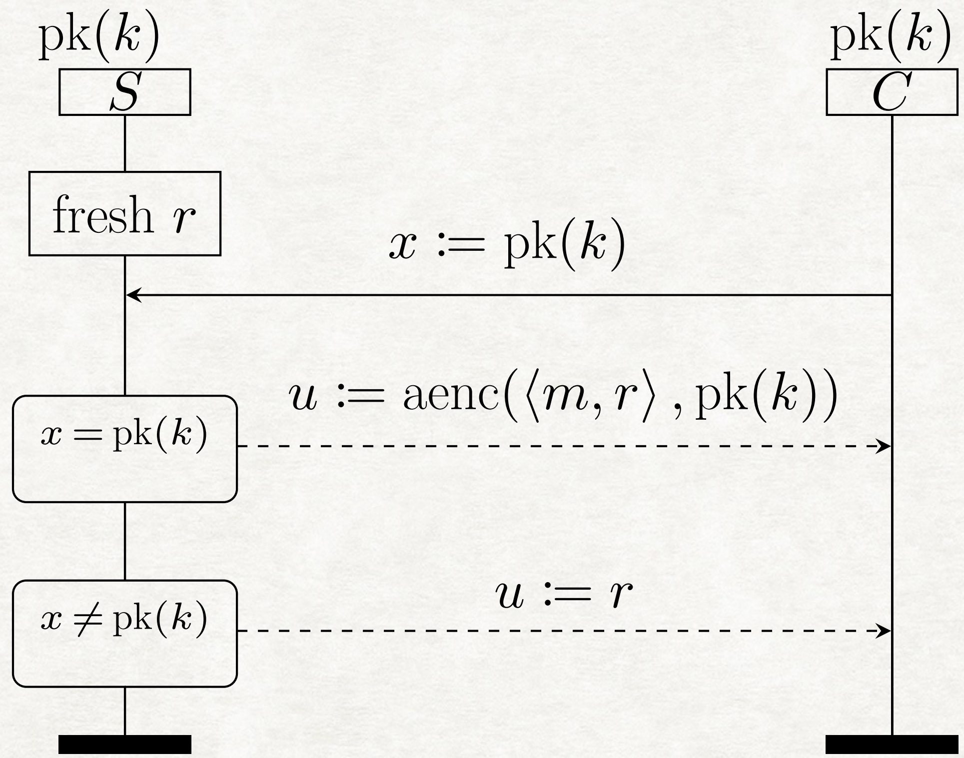
$$pk_s, u_l, v_l, w_l \ \# \ \{card, s\} \cup \{c_l, ch_l, a_l | l \in \{1, \cdots, L\}\}$$

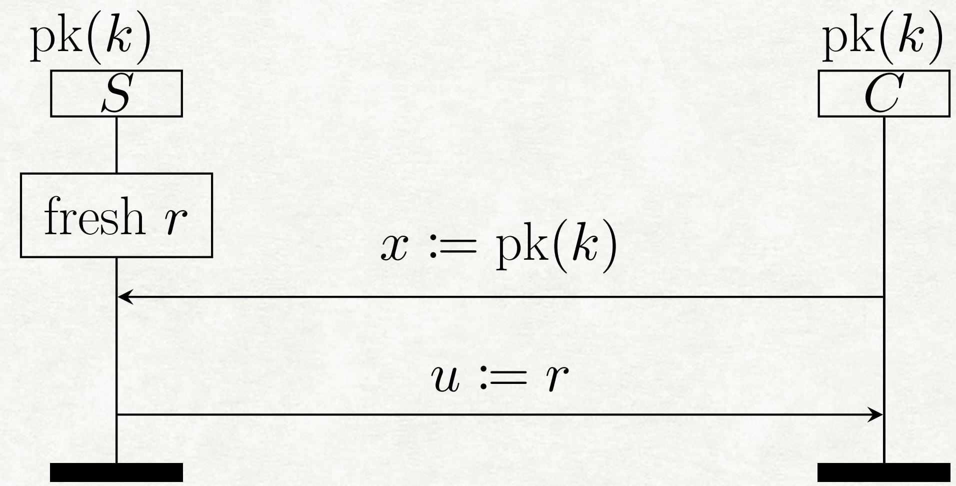
$$Y_l \ \# \ \{s\} \cup \{c_l, ch_l, a_l | l \in \{1, \cdots, L\}\}$$

$$\mathrm{fv}(Y_l) \cap (\{v_i | i \in \alpha\} \cup \{w_i | i \in \alpha \cup \beta \cup \gamma \cup \{l\}\}) = \varnothing$$

- Defining a relation (hard)
- Verify it is a quasi-open bisimulation (less hard)

# A FINER CONGRUENCE CALLED **OPEN BISIMILARITY*** IS TOO FINE




$$\nu k.\bar{s}\langle \mathtt{pk}(k)\rangle.!\ \nu a.\bar{c}\langle a\rangle.a(x).\nu r.\ \mathtt{if}\ x = \mathtt{pk}(k)\ \mathtt{then}\ \bar{a}\langle \mathtt{aenc}(\langle m,r\rangle, \mathtt{pk}(k))\rangle\ \mathtt{else}\ \bar{a}\langle r\rangle$$

$\sim$

$\not\sim_o$

$$\nu k.\bar{s}\langle \mathtt{pk}(k)\rangle.!\nu a.\bar{c}\langle a\rangle.a(x).\nu r.\bar{a}\langle r\rangle$$

For q-o.b. we have already decided about the input – it is some *N* that could or could not be pk(*k*), hence we can always proceed

For o.b. we are not ready yet to proceed from the reachable state below: the input x is not yet instantiated

$$\nu k, a_1, r_1.\left( \left\{ {}^{\mathtt{pk}(k),a_1}/_{u,v} \right\} \mid \quad \mathtt{if}\ x = \mathtt{pk}(k)\ \mathtt{then}\ \overline{a_1}\langle \mathtt{aenc}(\langle m,r_1\rangle, \mathtt{pk}(k))\rangle\ \mathtt{else}\ \overline{a_1}\langle r_1\rangle\right)$$

$$\nu k,a,r.\left( \left\{ {}^{\mathtt{pk}(k),a}/_{u,v} \right\} \mid \mathtt{if}\ N\left\{ {}^{\mathtt{pk}(k),a}/_{u,v} \right\} = \mathtt{pk}(k)\ \mathtt{then}\ \bar{a}\langle \mathtt{aenc}(\langle m,r\rangle, \mathtt{pk}(k))\rangle\ \mathtt{else}\ \bar{a}\langle r\rangle\right)$$

*HORNE, Ross; MAUW, Sjouke. Discovering ePassport vulnerabilities using bisimilarity. *Logical Methods in Computer Science*, 2021.

# RETURNING TO RESEARCH QUESTIONS

***Q1: Can we identify the requirements for an equivalence notion suitable for modelling indistinguishability properties of security protocols?***

*R1, R2, R3.*

***Q2: Can we identify a canonical equivalence notion satisfying the identified demands?***

*Quasi-open bisimilarity.*

***Q3: Can we reason effectively about protocols using the identified equivalence?***

*Even complex protocols can be analysed, compositionality allows to reduce the amount of work, direction for future work is an automated proof certificate (formula $\phi$ /q-o. bisimulation $\mathcal{R}$) verifier.*


LUXEMBOURG
LET'S MAKE IT HAPPEN
uni.lu
UNIVERSITÉ DU LUXEMBOURG
ALL

Thank you!