

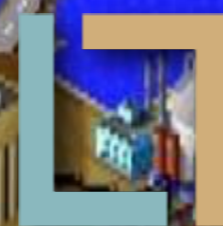


COMPOSITIONAL ANALYSIS OF PROTOCOL EQUIVALENCE IN THE APPLIED PI-CALCULUS USING QUASI-OPEN BISIMILARITY



Semyon Yurkov

STEP Seminar
17 November 2023



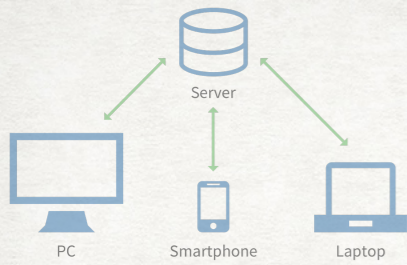
Luxembourg National
Research Fund

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



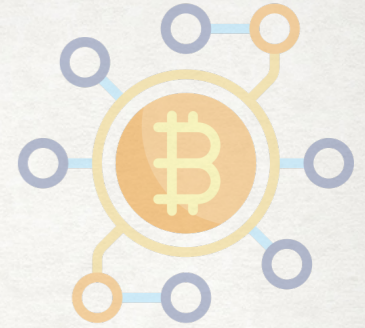
(Hi, It's) **Alice**



(Hi, It's) **Bob**



(Send BTC to)



Symbolic verification: "Is my protocol designed correctly?"



Alice

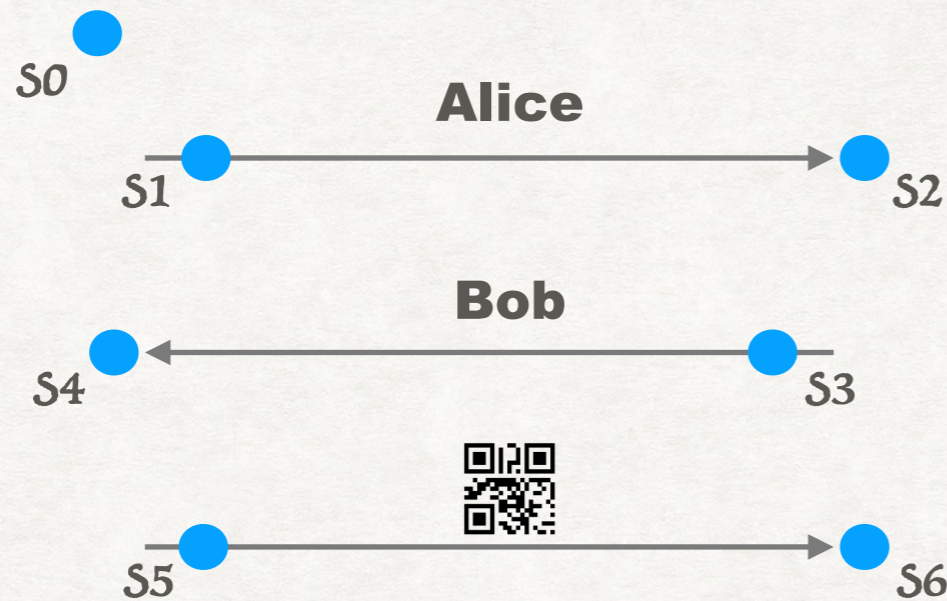


Bob

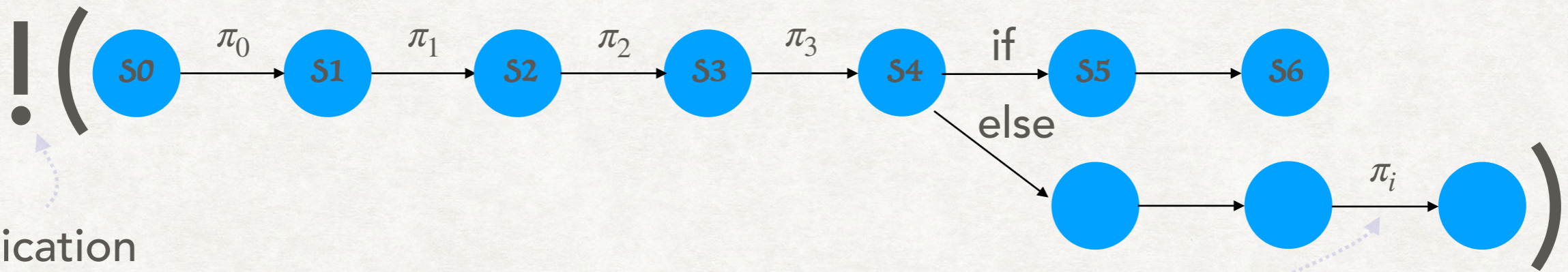


- Security property of *authentication* is not ensured.
- Privacy property of *unlinkability* is not ensured.

PROTOCOL'S BEHAVIOUR = LABELLED TRANSITION SYSTEM = PROCESS



State =
 + private values (keys, nonces)
 + messages exposed to the environment
 + available actions

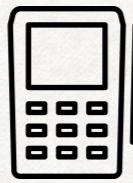
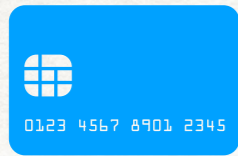


Replication
 (infinitely many protocol sessions)

Label
 (input / output / internal computation)

$$\nu ch . \overline{out}\langle ch \rangle . ! \left(\overline{ch}\langle Alice \rangle . ch(x) . \text{if } x = \text{Bob} \text{ then } \nu QR . \overline{ch}\langle QR \rangle \mid ch(y) . \text{if } y = \text{Alice} \text{ then } \overline{ch}\langle Bob \rangle . ch(z) \right)$$

EMV: AN EXAMPLE OF A REAL-WORLD PROTOCOL



5 Static Data Authentication (SDA)
5.4 Verification of Signed Static Application Data

5.4 Verification of Signed Static Application Data

1. If the Signed Static Application Data has a length different from the length of the Issuer I
2. In order to obtain the recovery function sp Data using the Issue algorithm. If the Rec failed.

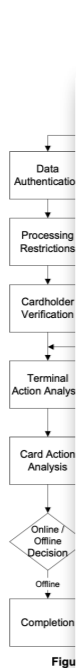
Field Name	L
Recovered Data Header	
Signed Data Format	
Hash Algorithm Indicator	
Data Authentication Code	
Pad Pattern	N
Hash Result	
Recovered Data Trailer	

Table 7: Format of D

3. Check the Recovered
4. Check the Signed Da
5. Concatenate from left Table 7 (that is, Sign the static data to be the Static Data Auth than '82', then SDA1

* See Annex B for specific value
* As can be seen in Annex A2.1 signature. Since the length of t 4 bytes, there are $N_1 - 22 - 4 =$ signature.

8 Transaction Flow
8.2 Example Flowchart



EMV 4.3 Book 2
Security and Key Management

EMV 4.3 Book 3
Application Specification

EMV 4.3 Book 4
Cardholder, Attendant, and Acquirer
Interface Requirements

6.3.1 Initiate Application Processing

When the Processing Options Data Object List (PDOL) includes an amount field (either Amount, Authorised or Amount, Other), an attended terminal (Terminal Type = 'x1', 'x2' or 'x3') shall provide the amount at this point in transaction processing. If the amount is not yet available, the terminal shall obtain the amount and should display the 'ENTER AMOUNT' message. For any other terminal type, if the terminal is unable to provide the amount at this point in transaction processing, the amount field in the data element list shall be filled with hexadecimal zeroes.

As described in Book 3, if the card returns SW1 SW2 = '6985' in response to the GET PROCESSING OPTIONS command, indicating that the transaction cannot be performed with this application, then the terminal should display the 'NOT ACCEPTED' message and shall return to application selection. The terminal shall not allow that application to be selected again for this card session as defined in Book 1.

6.3.2 Offline Data Authentication

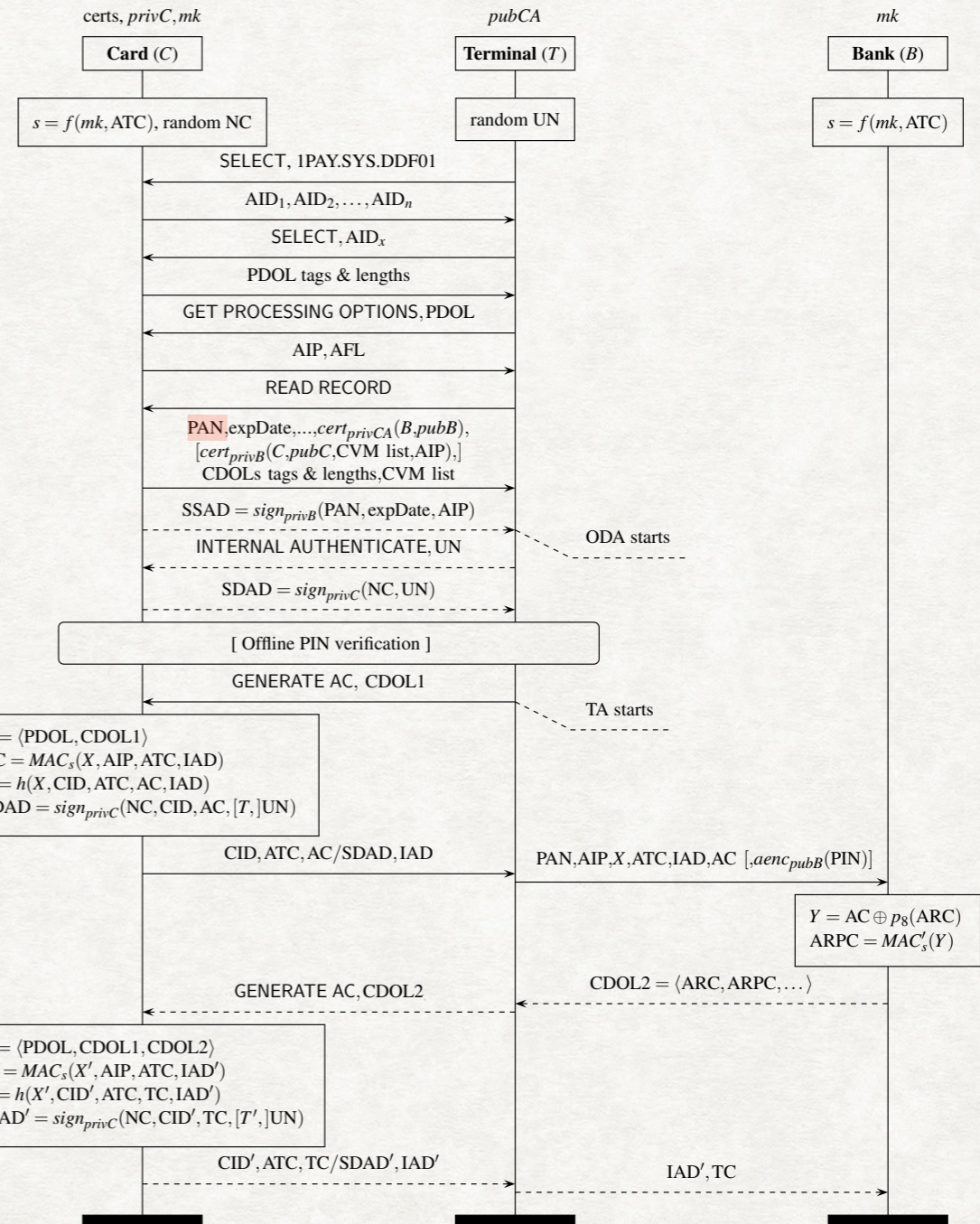
An online-only terminal supporting no form of offline data authentication as indicated in Terminal Capabilities shall set to 1 the 'Offline data authentication was not performed' bit in the Terminal Verification Results (TVR). (For details, see Annex C of Book 3.)

All other terminals shall support both offline static data authentication (SDA) and offline dynamic data authentication (DDA and optionally CDA) as described in Books 2 and 3.

When the selected form of offline data authentication is CDA and CDA fails prior to the final Terminal Action Analysis (for example, Issuer Public Key recovery fails prior to Terminal Action Analysis) preceding the issuance of a first GENERATE AC command, or second GENERATE AC command in the case 'unable to go online', the terminal shall set the TVR bit for 'CDA failed' to 1 and request the cryptogram type determined by Terminal Action Analysis. In this case, the GENERATE AC command shall not request a CDA signature and no further CDA processing is performed.

When the selected form of offline data authentication is CDA and a CDA failure is detected after the final Terminal Action Analysis preceding the issuance of a first or second GENERATE AC command, the terminal shall set the 'CDA failed' bit in the TVR to 1 and the following rules apply:

- If CDA fails in conjunction with the first GENERATE AC:
 - If the Cryptogram Information Data (CID) bit indicates that the card has returned a TC, the terminal shall decline the transaction and not perform a second GENERATE AC command.



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

$vs. \overline{out} \langle pk(s) \rangle . \left(!vch. \overline{card} \langle ch \rangle . C(ch, s, \dots) \mid !ch. \overline{term} \langle ch \rangle . T(ch, pk(s), \dots) \mid !ch. \overline{card} \langle ch \rangle . B(ch, \dots) \right)$

THE APPLIED PI-CALCULUS

Equational theory axiomatises cryptographic functions

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

Syntax for processes

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

Transitions

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

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

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

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

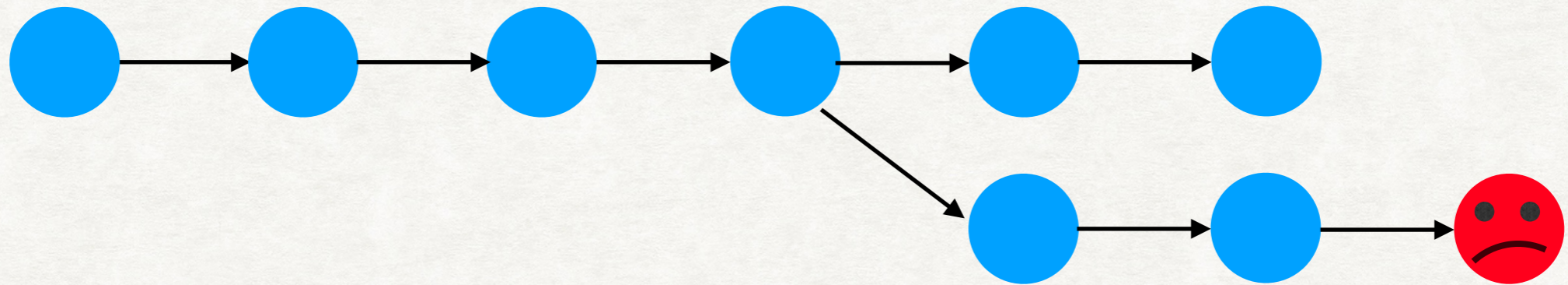
private values (keys, nonces).(messages (and aliases!) exposed to the environment | available actions)

OPEN EARLY LABELLED TRANSITION SYSTEM

LABELLED TRANSITION SYSTEM

$$\begin{array}{c}
 \frac{M\sigma =_E K}{\vec{z}: \sigma \mid K(x).P \xrightarrow{MN} \sigma \mid P\{N\sigma/x\}} \text{INP} \qquad \frac{x \# M, N, P, \sigma, \vec{z} \quad M\sigma =_E K}{\vec{z}: \sigma \mid \bar{K}\langle N \rangle.P \xrightarrow{\bar{M}(x)} \{N/x\} \circ \sigma \mid P} \text{OUT} \\
 \\
 \frac{\vec{z}: \sigma \mid P \xrightarrow{\pi} A}{\vec{z}: \sigma \mid P + Q \xrightarrow{\pi} A} \text{SUM-L} \qquad \frac{\vec{z}: \sigma \mid Q \xrightarrow{\pi} A}{\vec{z}: \sigma \mid P + Q \xrightarrow{\pi} A} \text{SUM-R} \\
 \\
 \frac{\vec{z}: \sigma \mid P \xrightarrow{\pi} A \quad M =_E N}{\vec{z}: \sigma \mid [M = N]P \xrightarrow{\pi} A} \text{MAT} \qquad \frac{\vec{z}: \sigma \mid P \xrightarrow{\pi} A \quad \vec{z} \models M \neq N}{\vec{z}: \sigma \mid [M \neq N]P \xrightarrow{\pi} A} \text{MISMATCH} \\
 \\
 \frac{\vec{z}, x: \sigma \mid P \xrightarrow{\pi} B \quad x \# \vec{z}, \sigma, n(\pi)}{\vec{z}: \sigma \mid \nu x.P \xrightarrow{\pi} \nu x.B} \text{EXTRUDE} \qquad \frac{\vec{z}, x: A \xrightarrow{\pi} B \quad x \# \vec{z}, n(\pi)}{\vec{z}: \nu x.A \xrightarrow{\pi} \nu x.B} \text{RES} \\
 \\
 \frac{\vec{z}: \sigma \mid P \xrightarrow{\pi} \nu \vec{x}.(\sigma \mid R) \quad \vec{x} \cup \text{bn}(\pi) \# Q}{\vec{z}: \sigma \mid P \mid Q \xrightarrow{\pi} \nu \vec{x}.(\sigma \mid R \mid Q)} \text{PAR-L} \qquad \frac{\vec{z}: \sigma \mid Q \xrightarrow{\pi} \nu \vec{x}.(\sigma \mid R) \quad \vec{x} \cup \text{bn}(\pi) \# P}{\vec{z}: \sigma \mid P \mid Q \xrightarrow{\pi} \nu \vec{x}.(\sigma \mid P \mid R)} \text{PAR-R} \\
 \\
 n(\pi) = \begin{cases} \text{fv}(M) \cup \{x\} & \text{if } \pi = \bar{M}(x) \\ \text{fv}(M) \cup \text{fv}(N) & \text{if } \pi = MN \\ \emptyset & \text{otherwise} \end{cases} \qquad \text{bn}(\pi) = \begin{cases} \{x\} & \text{if } \pi = \bar{M}(x) \\ \emptyset & \text{otherwise} \end{cases} \\
 \\
 \frac{\vec{z}: \sigma \mid P \xrightarrow{\bar{M}(x)} \nu \vec{y}.(\{N/x\} \circ \sigma \mid P') \quad \vec{z}: \sigma \mid Q \xrightarrow{MN} \nu \vec{w}.(\sigma \mid Q') \quad \{x\} \cup \vec{y} \# Q \quad \vec{w} \# P, \vec{y}}{\vec{z}: \sigma \mid P \mid Q \xrightarrow{\tau} \nu \vec{y}, \vec{w}.(\sigma \mid P' \mid Q')} \text{CLOSE-L} \\
 \\
 \frac{\vec{z}: \sigma \mid P \xrightarrow{MN} \nu \vec{y}.(\sigma \mid P') \quad \vec{z}: \sigma \mid Q \xrightarrow{\bar{M}(x)} \nu \vec{w}.(\{N/x\} \circ \sigma \mid Q') \quad \{x\} \cup \vec{w} \# P \quad \vec{y} \# Q, \vec{w}}{\vec{z}: \sigma \mid P \mid Q \xrightarrow{\tau} \nu \vec{y}, \vec{w}.(\sigma \mid P' \mid Q')} \text{CLOSE-R} \\
 \\
 \frac{\vec{z}: \sigma \mid P \xrightarrow{\pi} \nu \vec{x}.(\sigma \mid Q) \quad \vec{x} \cup \text{bn}(\pi) \# P}{\vec{z}: \sigma \mid !P \xrightarrow{\pi} \nu \vec{x}.(\sigma \mid Q \mid !P)} \text{REP-ACT} \\
 \\
 \frac{\vec{z}: \sigma \mid P \xrightarrow{\bar{M}(x)} \nu \vec{y}.(\{N/x\} \circ \sigma \mid Q) \quad \vec{z}: \sigma \mid P \xrightarrow{MN} \nu \vec{w}.(\sigma \mid R) \quad \vec{y} \# P, \vec{w} \quad \vec{w} \# P}{\vec{z}: \sigma \mid !P \xrightarrow{\tau} \nu \vec{y}, \vec{w}.(\sigma \mid Q \mid R \mid !P)} \text{REP-CLOSE}
 \end{array}$$

REACHABILITY (SECURITY)

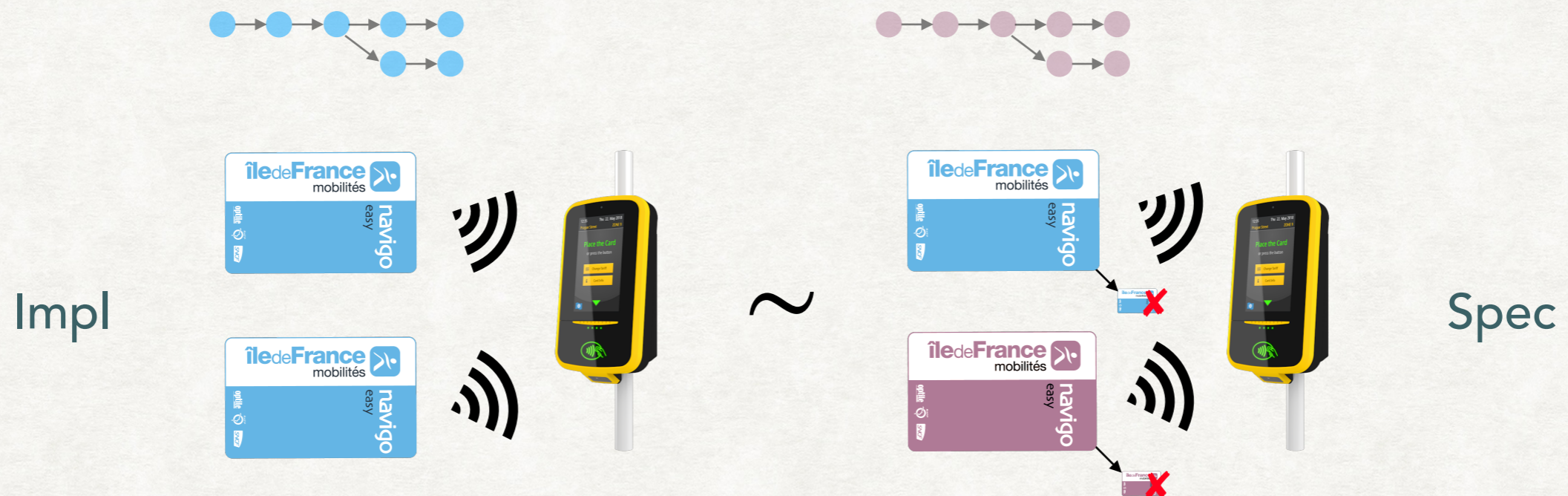


An attacker interacting with the system cannot force the system to reach a “bad” state where a property (authentication, secrecy) is violated.

- * 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 ~)

- Limited tool support

— DeepSec, ProVerif

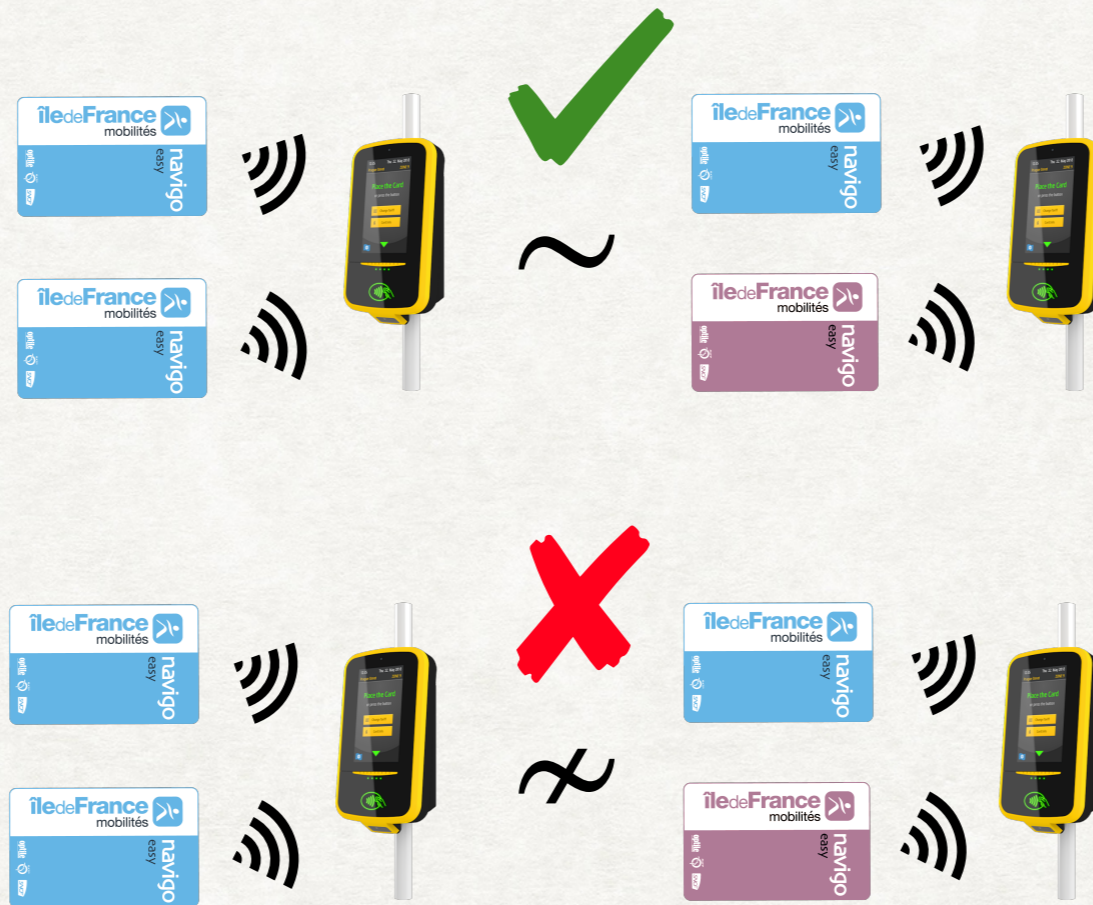
RESEARCH QUESTIONS

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

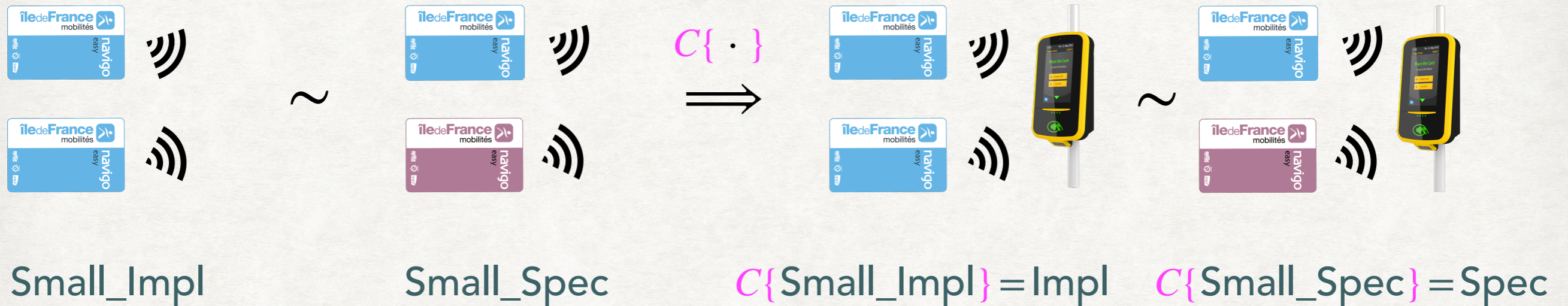


$\text{Impl} \not\models \phi$

$\text{Spec} \models \phi$

R1: Whenever the property fails there is a formula ϕ describing a testable attack.

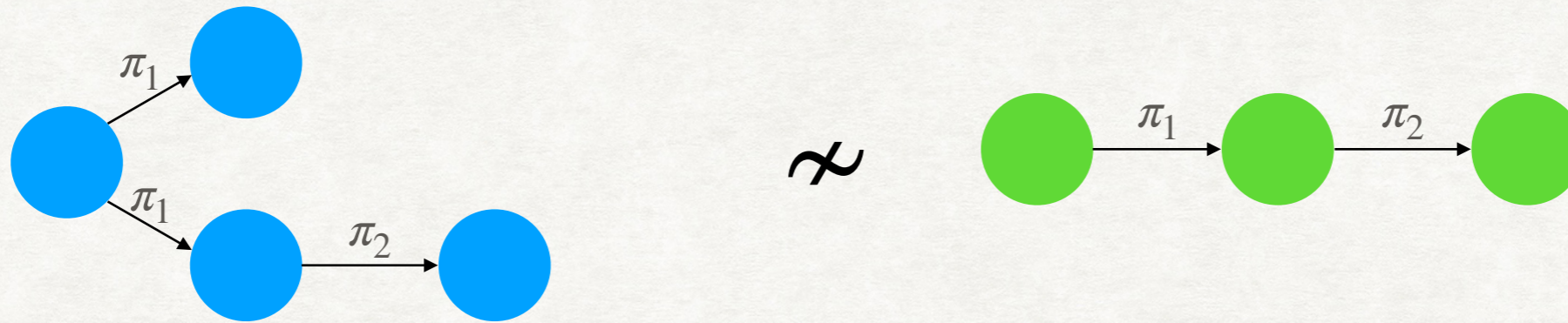
REQUIREMENT 2: CONGRUENCE



R2: \sim should be a congruence relation.

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

REQUIREMENT 3: BISIMILARITY



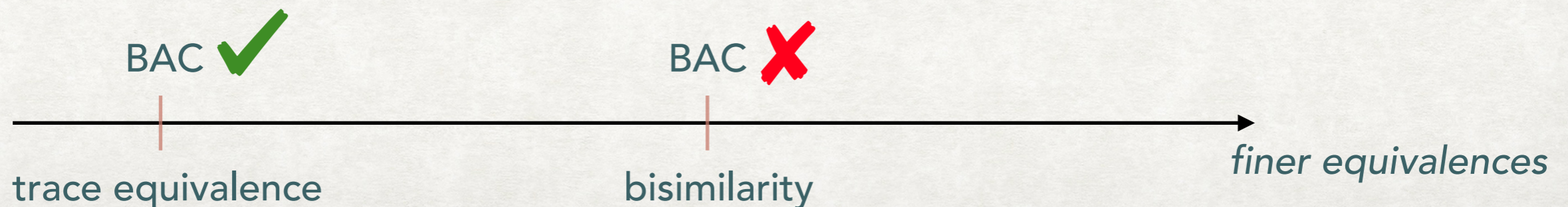
R3: Attacker should be able to make decisions *dynamically*, during the execution.

EVIDENCE:

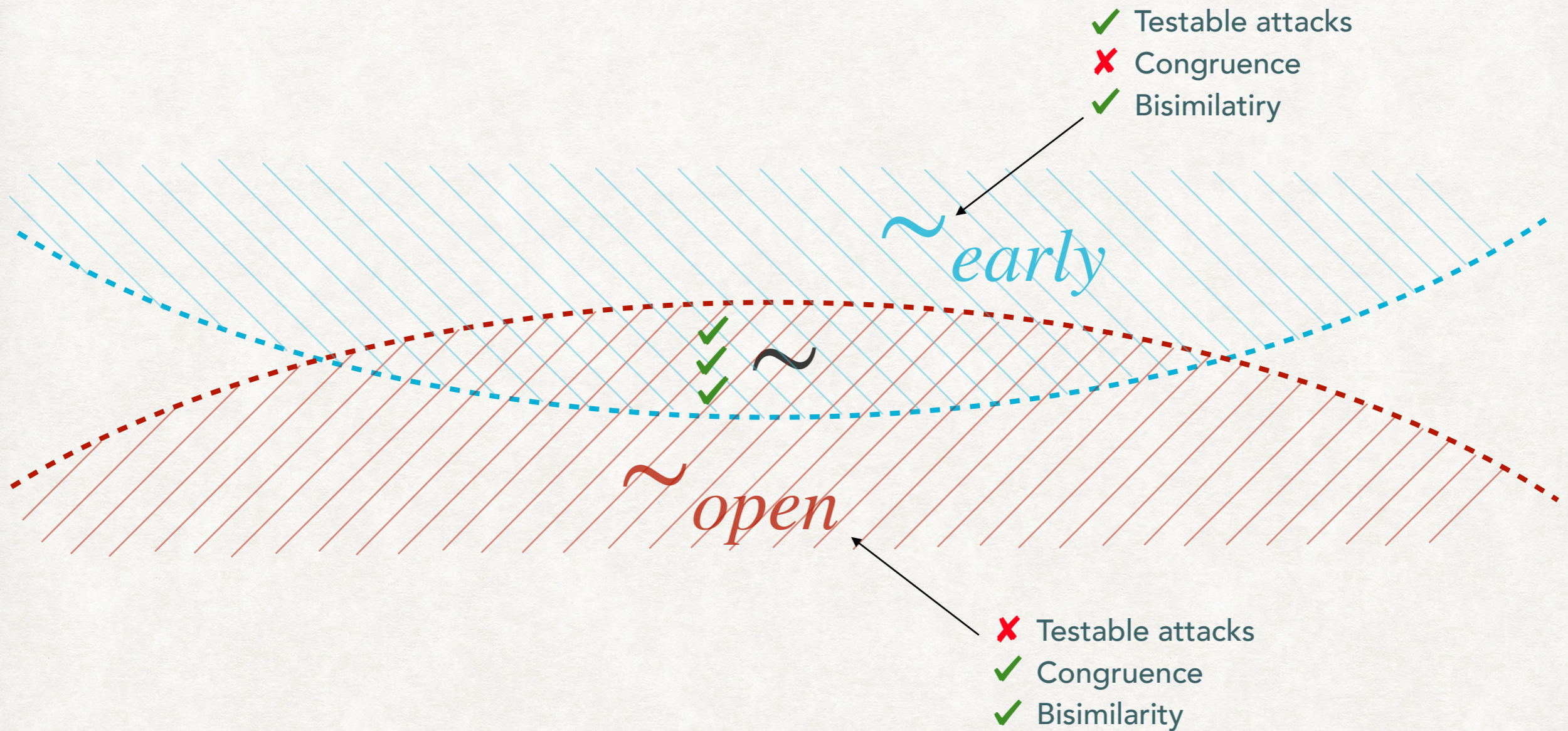
- 2016: The (*correct* !) proof that the BAC protocol used in biometric passports is unlinkable in the trace equivalence-based model.
- 2019: A (*practical* !) attack has been discovered employing the bisimilarity-based model.

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

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



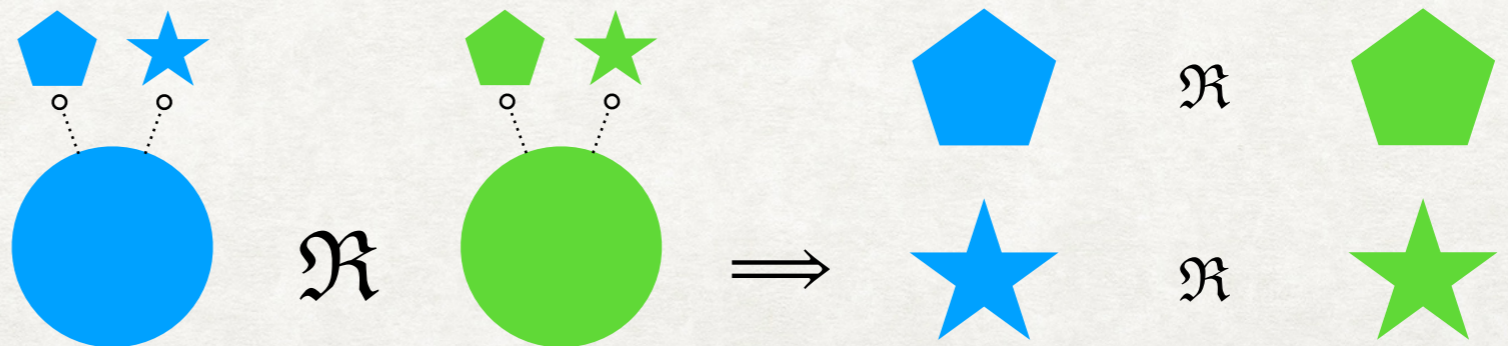
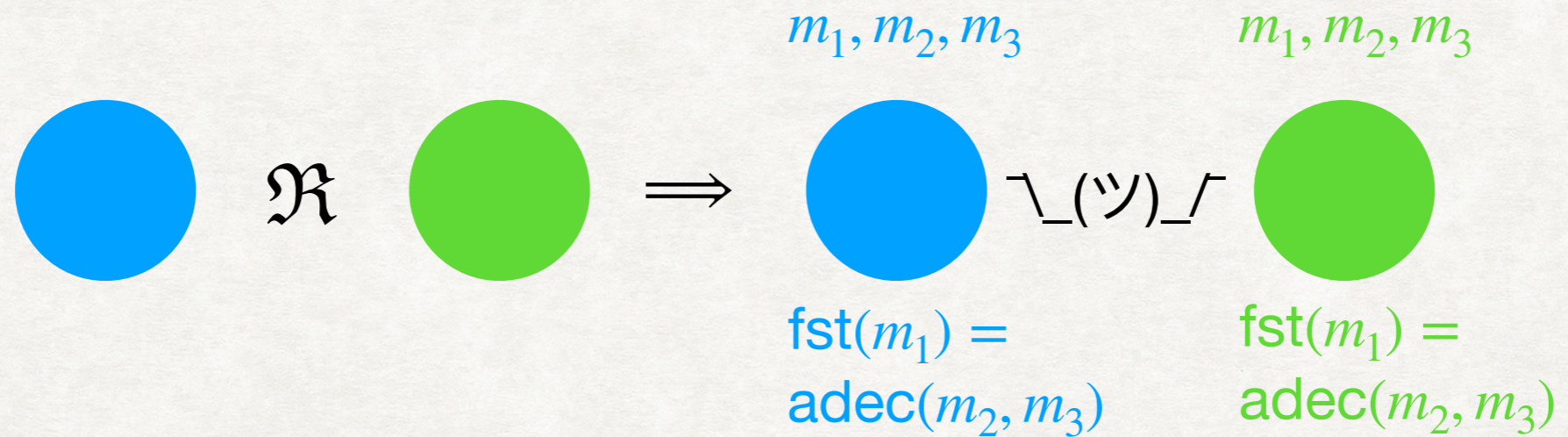
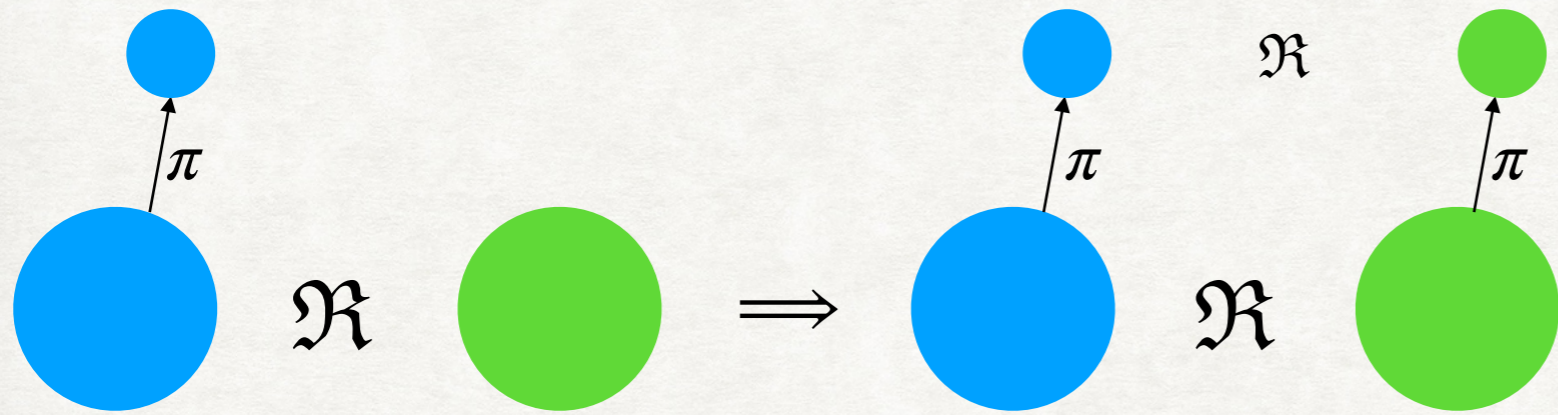
QUASI-OPEN BISIMILARITY



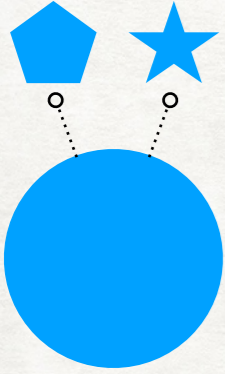
\sim quasi-open bisimilarity: the coarsest bisimilarity congruence for the applied pi-calculus

QUASI-OPEN BISIMILARITY

$$P_{\text{Spec}} \sim P_{\text{Impl}} \iff \begin{array}{c} \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \\ \searrow \\ \end{array} \sim \begin{array}{c} \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet \\ \searrow \\ \end{array}$$



III – MANIPULATING FREE VARIABLES



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

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

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

Monotonicity lemma: if a transition π 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 .

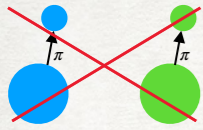
$[x \neq z]a(y).[x = y]\pi$ cannot act, since there is no evidence that x and z are different

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

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

$$\frac{\vec{z}:\sigma \mid P \xrightarrow{\pi} A \quad M =_E N}{\vec{z}:\sigma \mid [M = N]P \xrightarrow{\pi} A} \text{MAT} \quad \frac{\vec{z}:\sigma \mid P \xrightarrow{\pi} A \quad \vec{z} \models M \neq N}{\vec{z}:\sigma \mid [M \neq N]P \xrightarrow{\pi} A} \text{MISMATCH}$$

ATTACK EXAMPLES



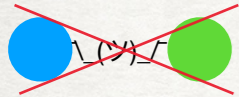
$$\nu z. \bar{x} \langle \langle z, y \rangle \rangle. z(w) \not\sim \nu z. \bar{x} \langle \langle z, y \rangle \rangle$$

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

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

$$\langle \bar{a}(u) \rangle \langle \text{fst}(u) w \rangle \mathbf{tt}$$

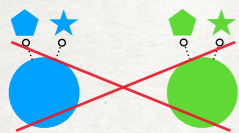
$$[\bar{a}(u)] [\text{fst}(u) w] \mathbf{ff}$$



$$\nu m, n. \bar{a} \langle m \rangle. \bar{a} \langle n \rangle \not\sim \nu n. \bar{a} \langle n \rangle. \bar{a} \langle h(n) \rangle$$

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

$$[\bar{a}(u)] [\bar{a}(v)] (v = h(u))$$



$$\nu x. \bar{a} \langle \text{aenc}(x, z) \rangle \not\sim \nu x. \bar{a} \langle \text{aenc}(\langle x, y \rangle, z) \rangle$$

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

$$\nu x. \left(\left\{ \text{aenc}(x, z) / v \right\} \mid 0 \right) \left\{ \text{pk}(w) / z \right\} \quad \not\sim \quad \nu x. \left(\left\{ \text{aenc}(\langle x, y \rangle, z) / v \right\} \mid 0 \right) \left\{ \text{pk}(w) / z \right\}$$

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

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

QASI-OPEN BIMISILARITY IS THE COARSEST BISIMILARITY CONGRUENCE

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

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 , $P \xrightarrow{\bar{M}(z)} A$, or $P \xrightarrow{MN} A$, 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 $A \mathfrak{R} B$ holds the following hold:*

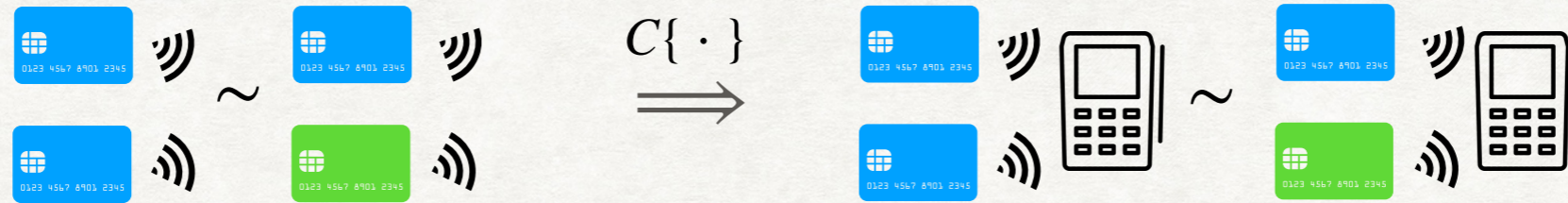
- *For all contexts $C\{\cdot\}$, $C\{A\} \mathfrak{R} C\{B\}$.*
- *If $A \downarrow M$ then $B \downarrow M$.*
- *If $A \xrightarrow{\tau} A'$, there exists B' such that $B \xrightarrow{\tau} B'$ and $A' \mathfrak{R} B'$ holds.*

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

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.

$$C\{\cdot\} \triangleq \nu out. \left(\{\cdot\} \mid out(pk_s). \overline{out'} \langle pk_s \rangle . !vch_t. \overline{term} \langle ch_t \rangle . T(pk_s, ch_t) \right)$$



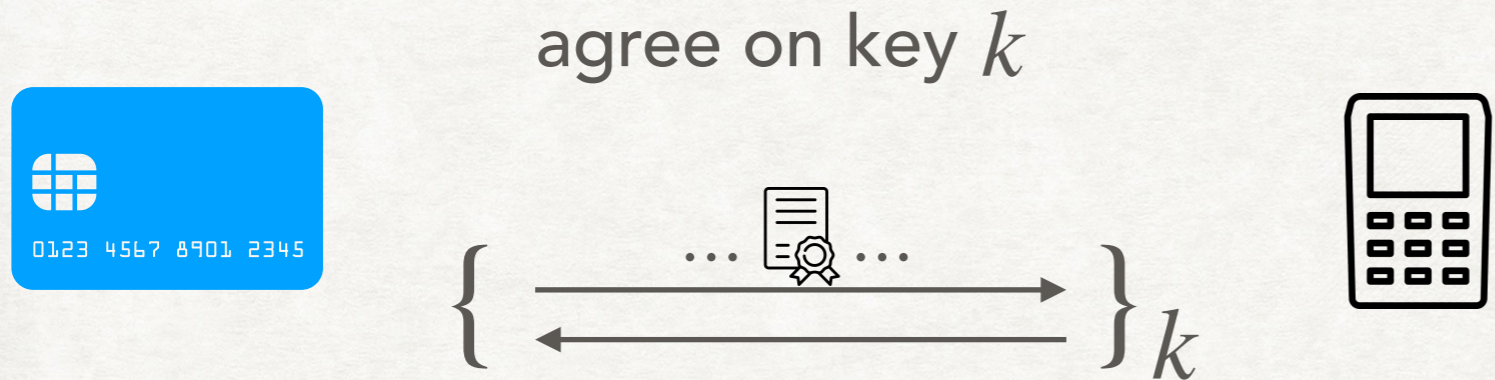
**A CARD CAN PARTICIPATE
IN MANY SESSIONS**

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

$$\text{Impl} \triangleq \nu s. \left(\begin{array}{l} !vc. \\ !vch_c. \overline{card} \langle ch_c \rangle . C(s, c, ch_c) \mid \\ \overline{out} \langle pk(s) \rangle . \\ \overline{ch_t}. \overline{term} \langle ch_t \rangle . T(pk(s), ch_t) \end{array} \right) \sim \nu s. \left(\begin{array}{l} !vc. \\ vch_c. \overline{card} \langle ch_c \rangle . C(s, c, ch_c) \mid \\ \overline{out} \langle pk(s) \rangle . \\ \overline{ch_t}. \overline{term} \langle ch_t \rangle . T(pk(s), ch_t) \end{array} \right) \triangleq \text{Spec}$$

$$\text{Small_Impl} \triangleq \nu s. \left(\begin{array}{l} \overline{out} \langle pk(s) \rangle . \\ !vc. \\ !vch_c. \overline{card} \langle ch_c \rangle . C(s, c, ch_c) \end{array} \right) \sim \nu s. \left(\begin{array}{l} \overline{out} \langle pk(s) \rangle . \\ !vc. \\ vch_c. \overline{card} \langle ch_c \rangle . C(s, c, ch_c) \end{array} \right) \triangleq \text{Small_Spec}$$

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

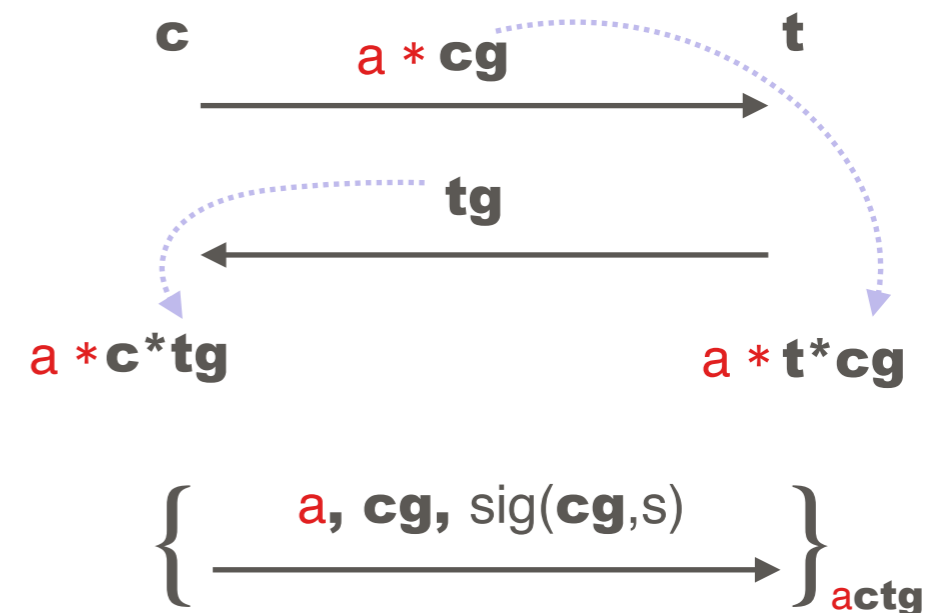
- provide authentication of the card by the terminal
- protect against eavesdropping and card tracking.



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

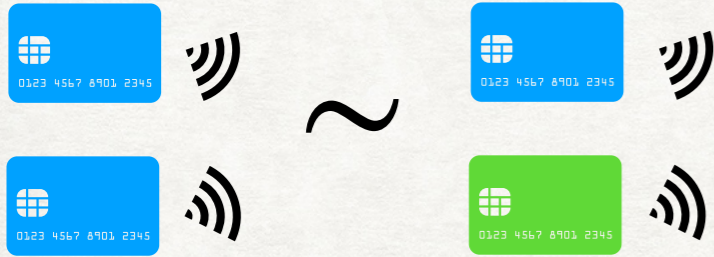
Blinded Diffie-Hellman

g public



A PROOF OF PRIVACY OF A CORRECT PROTOCOL

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

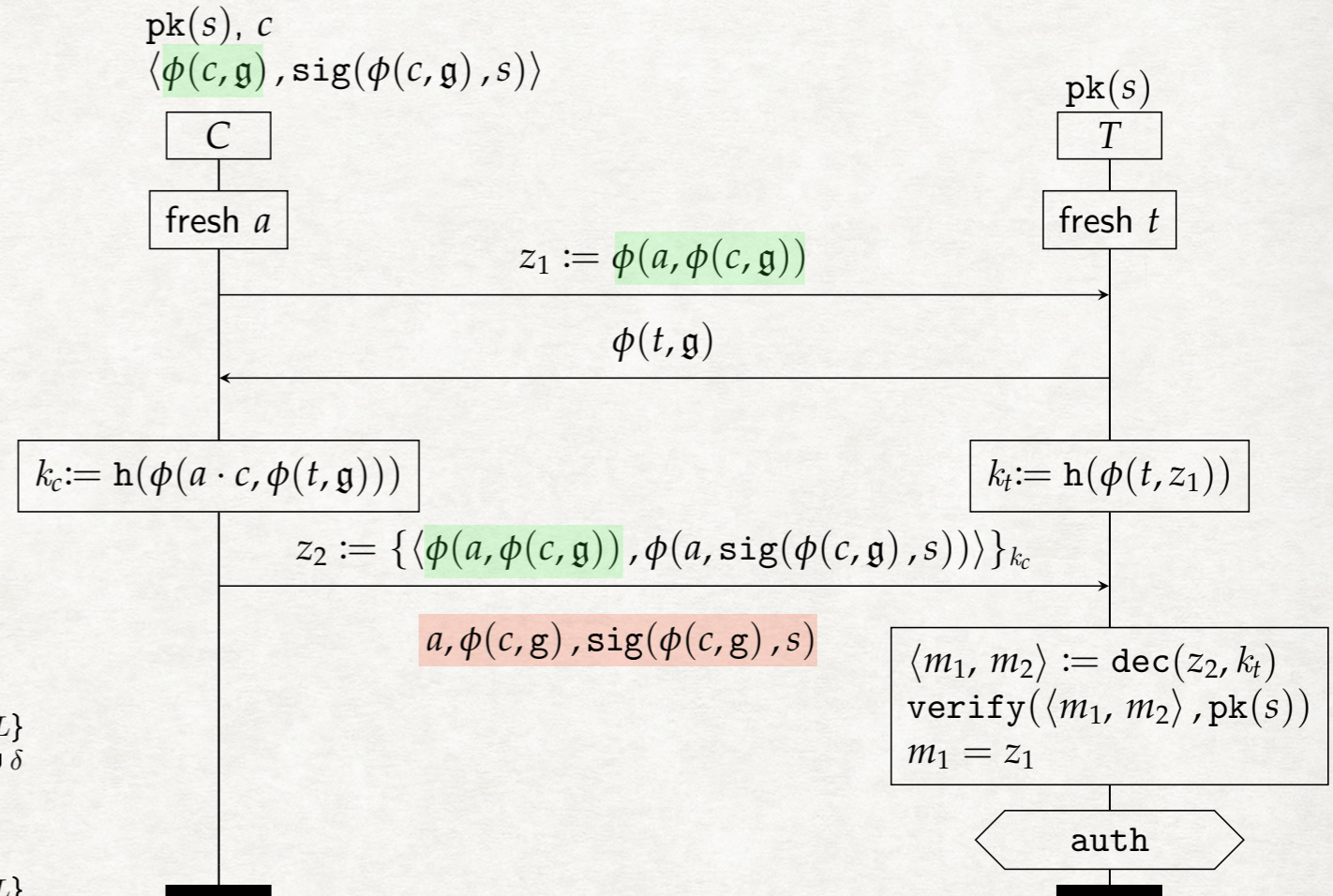


Since we can present a relation between the states of and that satisfies the definition of quasi-open bisimilarity.

$$\begin{aligned}
 &UPD_{\text{spec}} \mathfrak{R} UPD_{\text{impl}} \\
 &UPD_{\text{spec}}^{\Psi}(\vec{Y}) \triangleq \nu s, c_1, \dots, c_L, ch_1, \dots, ch_L, \\
 &a_{l_1}, \dots, a_{l_K} \cdot (\sigma \\
 &| C_1 | \dots | C_L \\
 &| !\nu c. \overline{\nu ch. card}\langle ch \rangle. C_{\text{upd}}(s, c, ch)) \\
 &\mathfrak{R} \\
 &UPD_{\text{impl}}^{\Psi, \Omega}(\vec{Y}) \triangleq \nu s, c_1, \dots, c_D, ch_1, \dots, ch_L, \\
 &a_{l_1}, \dots, a_{l_K} \cdot (\theta \\
 &| \dots | C_l^d | \dots | !\nu ch. \overline{\nu ch. card}\langle ch \rangle. C_{\text{upd}}(s, c_d, ch) \\
 &| !\nu c. !\nu ch. \overline{\nu ch. card}\langle ch \rangle. C_{\text{upd}}((s, ch, c))) \\
 &C_l = \begin{cases} \mathcal{E}^l(ch_l) & \text{if } l \in \alpha \\ \mathcal{F}^l(ch_l, a_l) & \text{if } l \in \beta \\ \mathcal{G}^l(ch_l, a_l, Y_l \sigma) & \text{if } l \in \gamma \\ \mathcal{H}^l & \text{if } l \in \delta \end{cases} \\
 &C_l^d = \begin{cases} \mathcal{E}^d(ch_l) & \text{if } l \in \zeta^d \cap \alpha \\ \mathcal{F}^d(ch_l, a_l) & \text{if } l \in \zeta^d \cap \beta \\ \mathcal{G}^d(ch_l, a_l, Y_l \theta) & \text{if } l \in \zeta^d \cap \gamma \\ \mathcal{H}^d & \text{if } l \in \zeta^d \cap \delta \end{cases}
 \end{aligned}$$

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

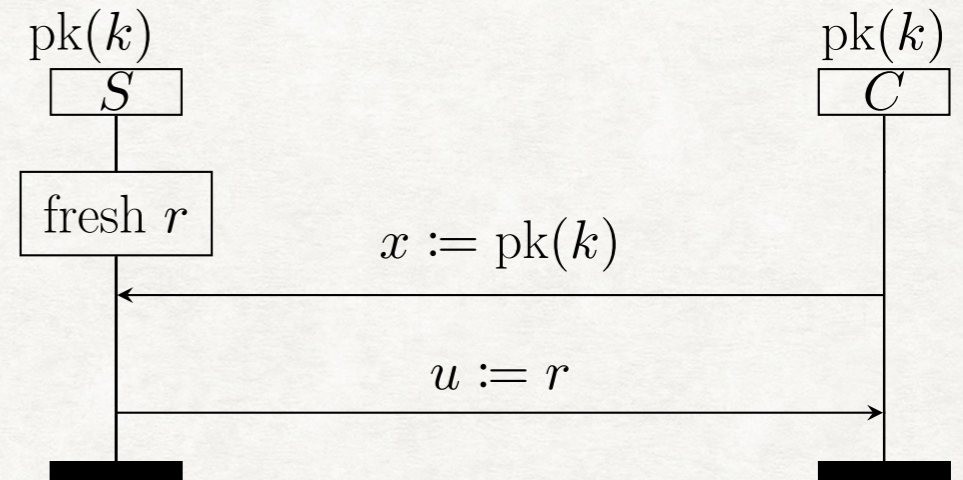
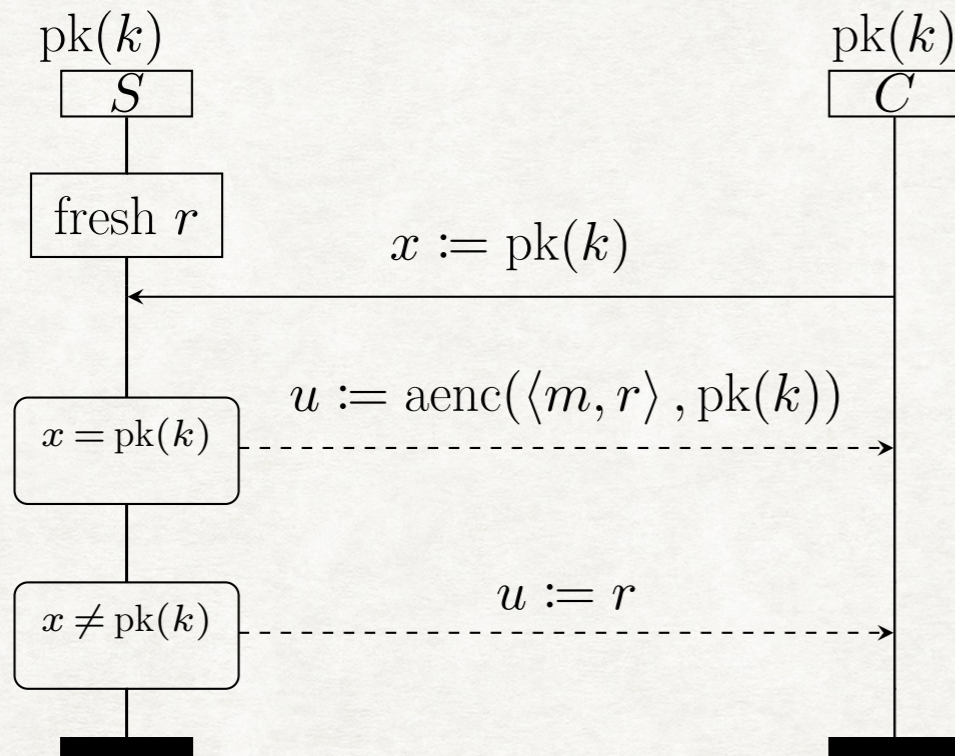
$$\begin{aligned}
 &\Psi := \{\alpha, \beta, \gamma, \delta\}, \quad \Omega := \{\zeta^1, \dots, \zeta^D\} \text{ are partitions of } \{1, \dots, L\} \\
 &K := |\beta \cup \gamma \cup \delta| \quad l_1, \dots, l_K \in \beta \cup \gamma \cup \delta \\
 &pk_s, u_l, v_l, w_l \# \{card, s\} \cup \{c_l, ch_l, a_l \mid l \in \{1, \dots, L\}\} \\
 &Y_l \# \{s\} \cup \{c_l, ch_l, a_l \mid l \in \{1, \dots, L\}\} \\
 &fv(Y_l) \cap (\{v_i \mid i \in \alpha\} \cup \{w_i \mid i \in \alpha \cup \beta \cup \gamma \cup \{l\}\}) = \emptyset
 \end{aligned}$$



✿ Defining a relation (hard)

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

A FINER CONGRUENCE CALLED OPEN BISIMILARITY* IS TOO FINE



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

\approx_0

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

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

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

$\nu k, a_1, r_1. \left(\left\{ pk(k), a_1 / u, v \right\} \mid \text{if } x = pk(k) \text{ then } \bar{a}_1\langle aenc(\langle m, r_1 \rangle, pk(k)) \rangle \text{ else } \bar{a}_1\langle r_1 \rangle \right)$

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

*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 ϕ / q-o. bisimulation \mathcal{R}) verifier.

LU  EMBOURG

LET'S MAKE IT HAPPEN



UNIVERSITÉ DU
LUXEMBOURG



Thank you!