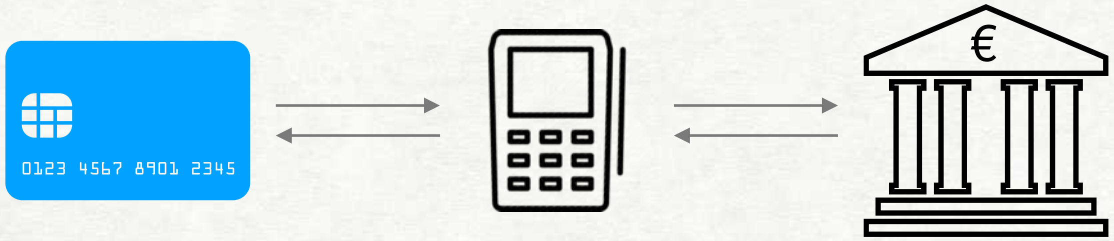
# Analysis of Smartcard-based Payment Protocols in the Applied pi-calculus using Quasi-Open Bisimilarity

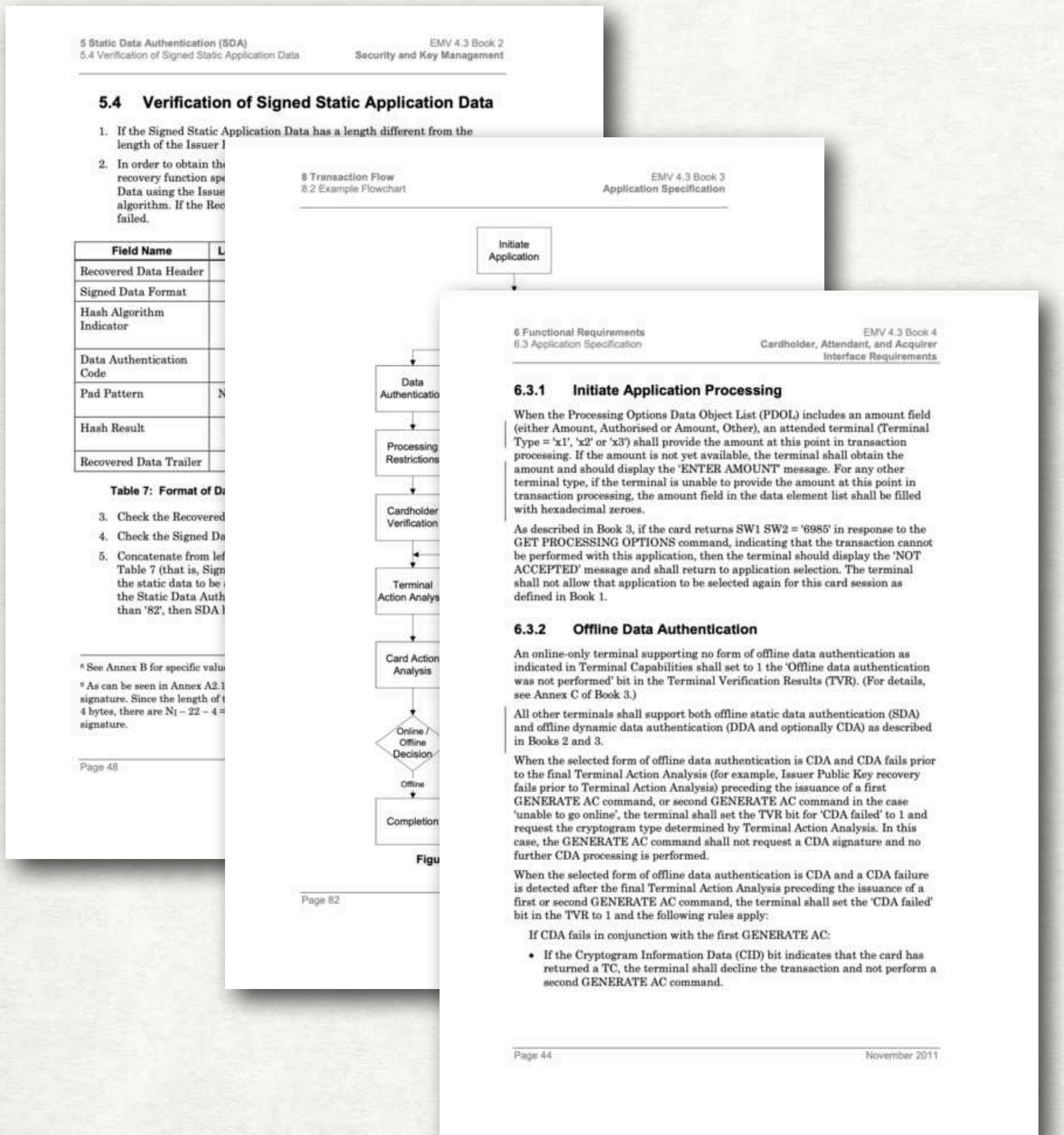
Semyon Yurkov

15 June 2023

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

# VERIFICATION: IS MY PROTOCOL DESIGNED CORRECTLY?



5 Static Data Authentication (SDA)
5.4 Verification of Signed Static Application Data
EMV 4.3 Book 2
Security and Key Management

**5.4 Verification of Signed Static Application Data**

8 Transaction Flow
8.2 Example Flowchart
EMV 4.3 Book 3
Application Specification

6 Functional Requirements
6.3 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.

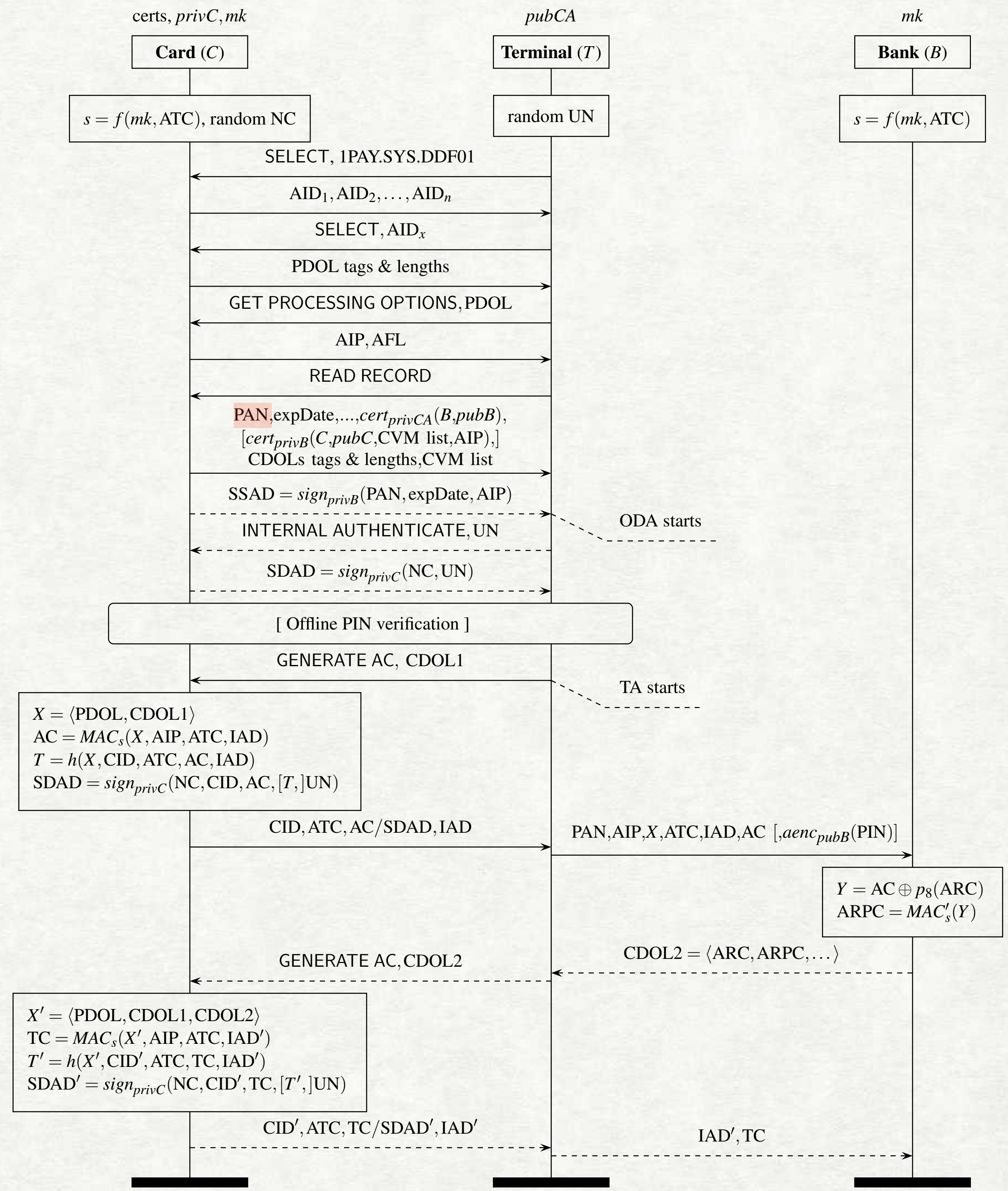
When the selected form of offline data authentication is CDA and CDA fails prior to the final Terminal Action Analysis (for example, Issuer Public Key recovery fails prior to Terminal Action Analysis) preceding the issuance of a first GENERATE AC command, or second GENERATE AC command in the case 'unable 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.

Page 44 November 2011

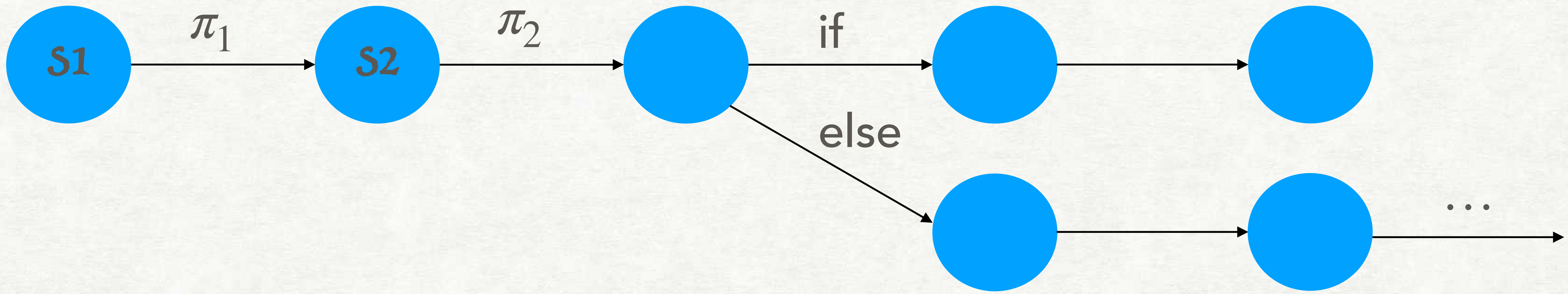



*The EMV Standard: Break, Fix, Verify* David Basin, Ralf Sasse, and Jorge Toro-Pozo (S&P 2021)

# OVERVIEW

- Modelling privacy-like properties of cryptographic protocols.
- Quasi-open bisimilarity for the applied pi-calculus: formalising privacy.
- UBDH: an unlinkable key agreement for smart card payments.
- UTX: an unlinkable smart card payment protocol.

# PROTOCOL'S BEHAVIOUR = LABELLED TRANSITION SYSTEM = PROCESS



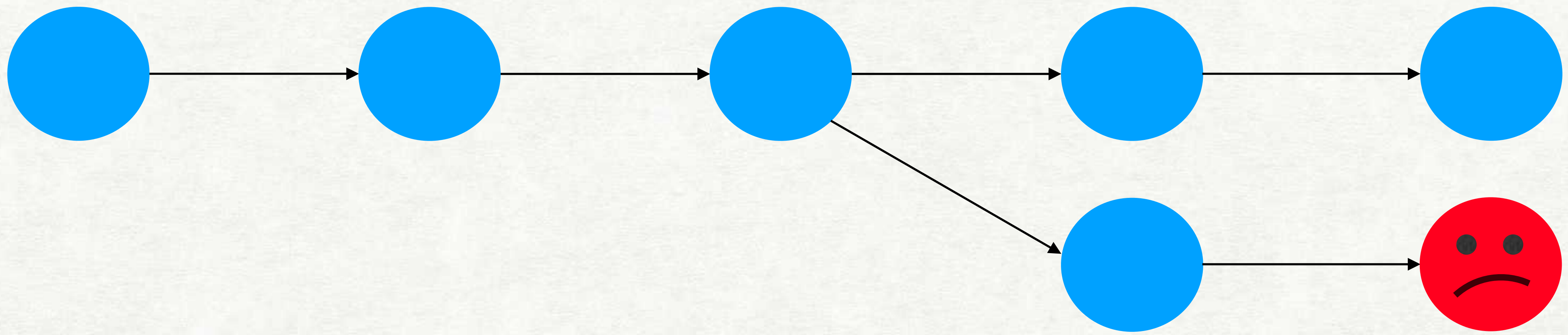

- private values (keys, nonces)
- messages exposed to the environment
- available actions

$\pi$

- input / output / internal computation

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

# REACHABILITY (SECURITY)



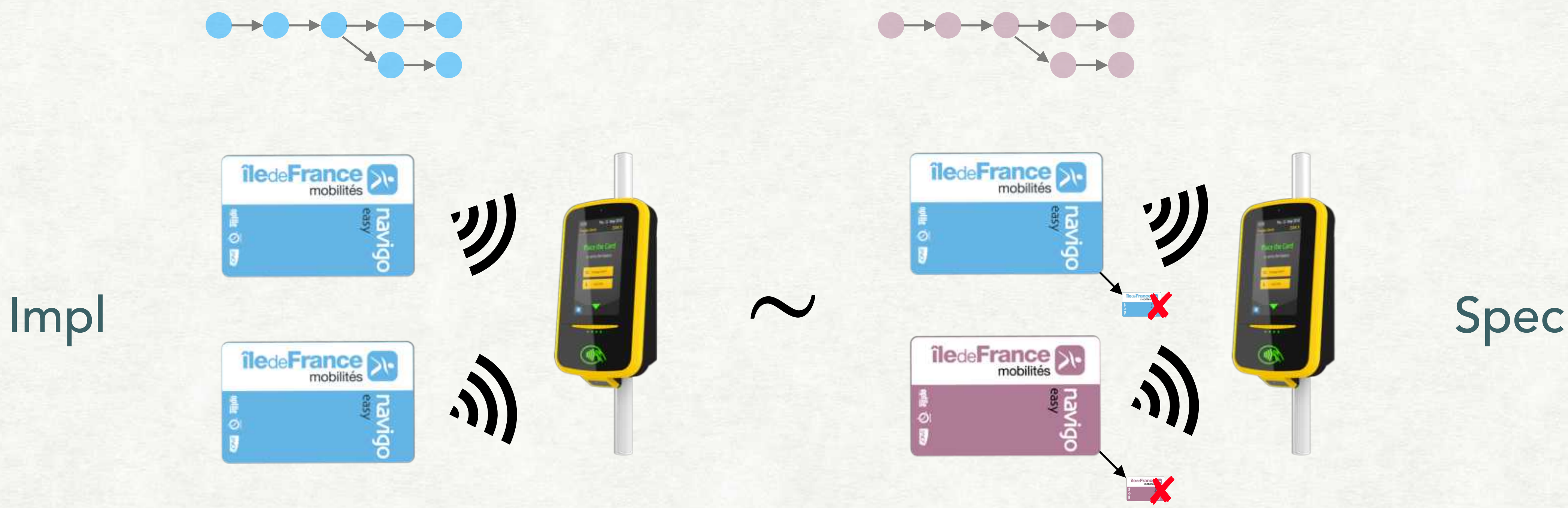
An attacker interacting with the system can not force the system to reach a "bad" state where a property (*authentication*, *secrecy*) is violated.

- 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 can 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

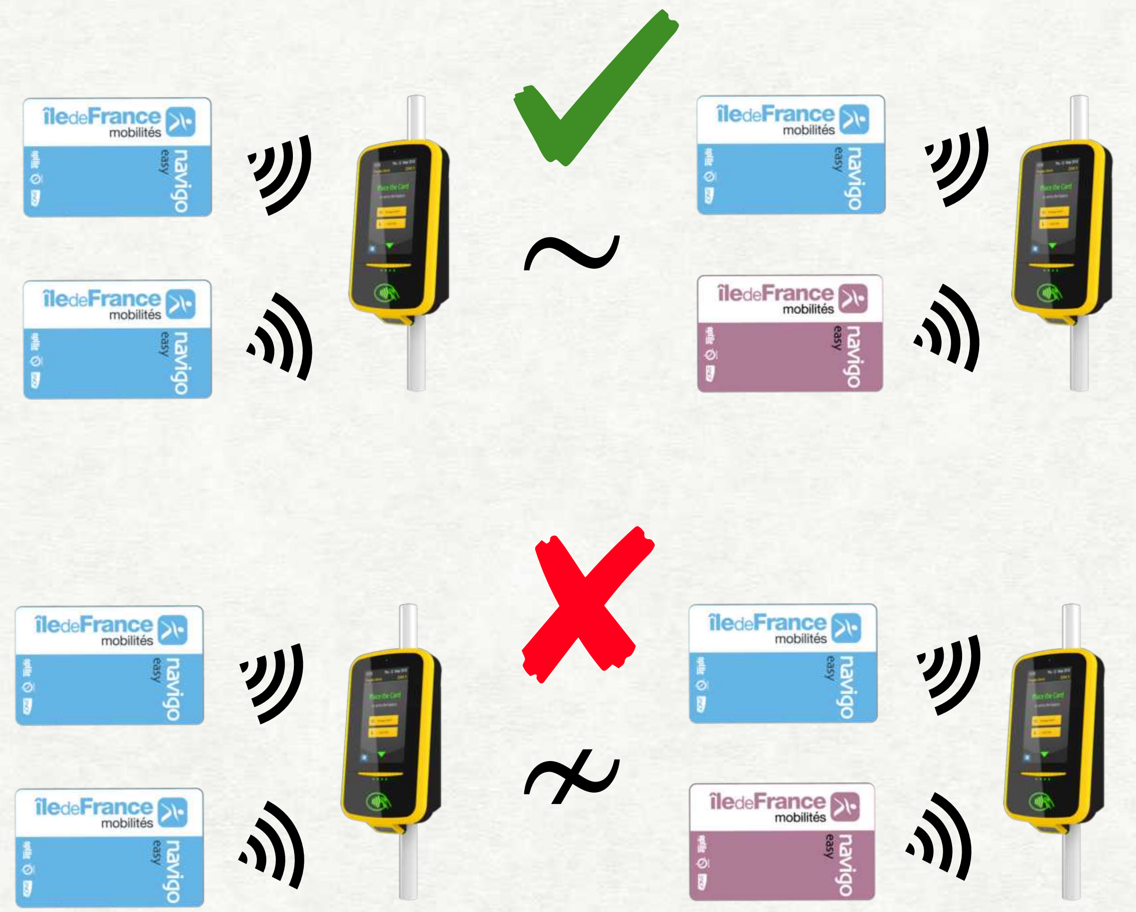
# RESEARCH QUESTIONS

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

***Q2: Can we identify a <u>canonical equivalence</u> notion satisfying the identified demands?***

***Q3: Can we <u>reason effectively</u> about protocols using the identified equivalence?***

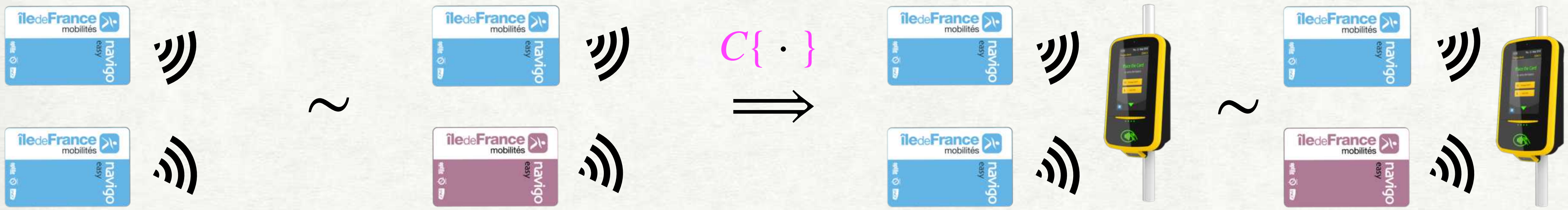
# REQUIREMENT 1: CLEAR VERIFICATION OUTCOME




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

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

# REQUIREMENT 2: CONGRUENCE

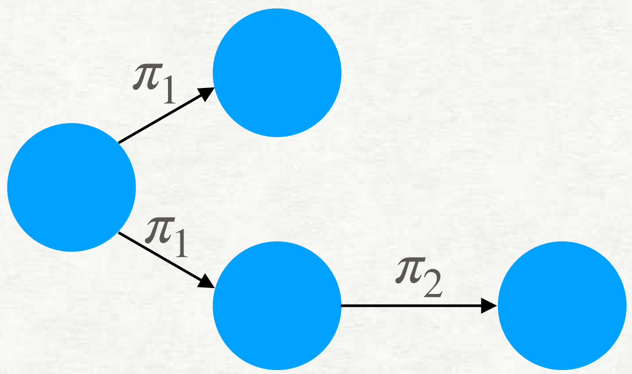



Small_Impl $\qquad$ Small_Spec $\qquad$ $C\{$Small_Impl$\}$ = Impl $\qquad$ $C\{$Small_Spec$\}$ = Spec

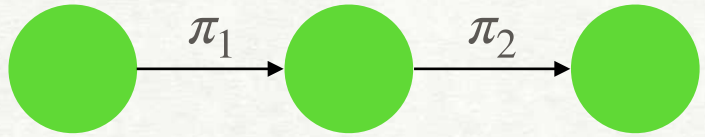
**R2**: $\sim$ should be a congruence relation.

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

# REQUIREMENT 3: BISIMILARITY




$\not\approx$




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

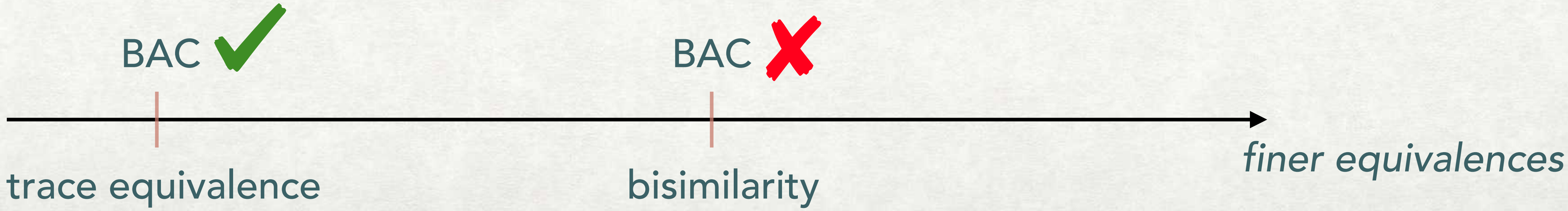
**EVIDENCE:**

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

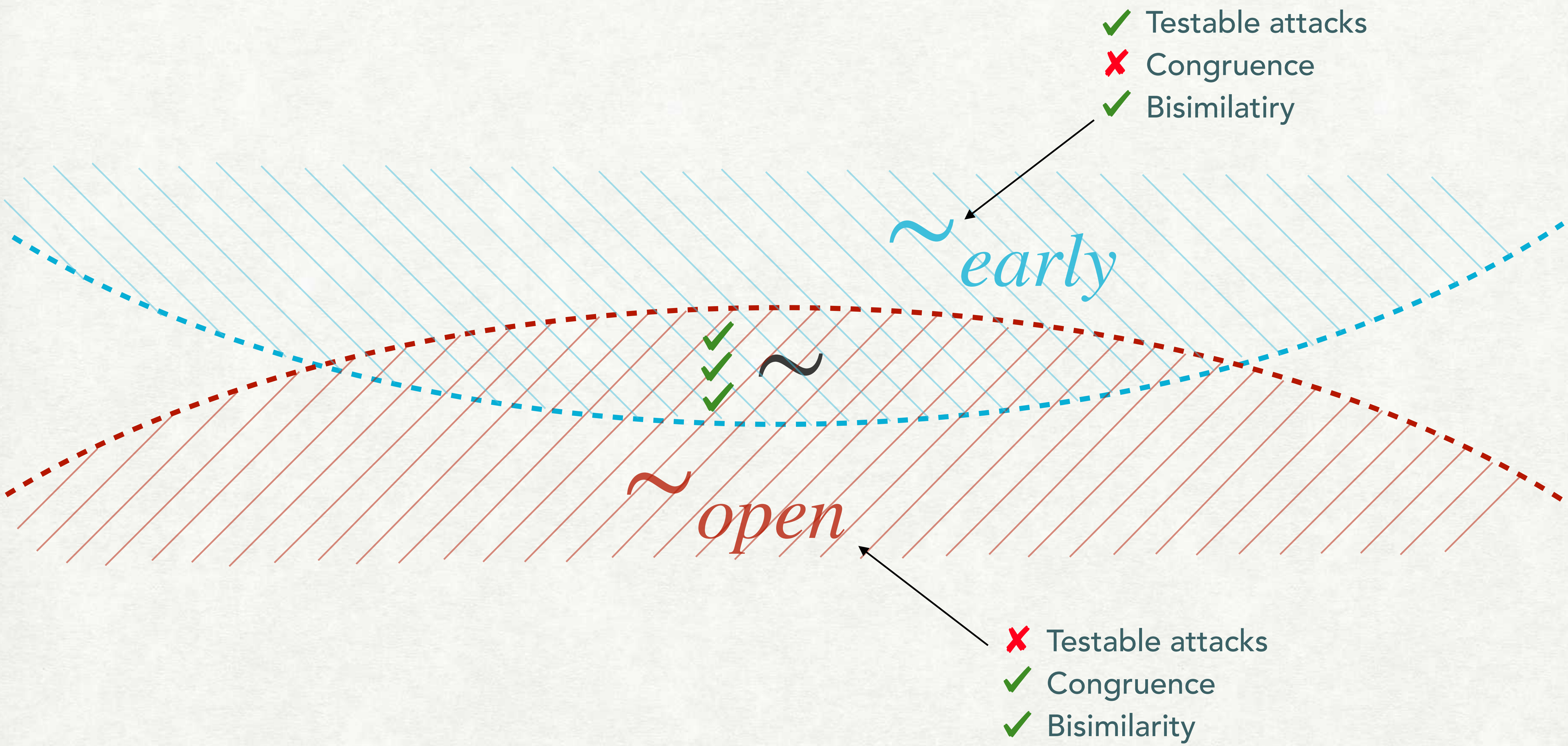
L. Hirschi, D. Baelde, and S. Delaune. A method for verifying privacy-type properties: the unbounded case (S&P).

- 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).



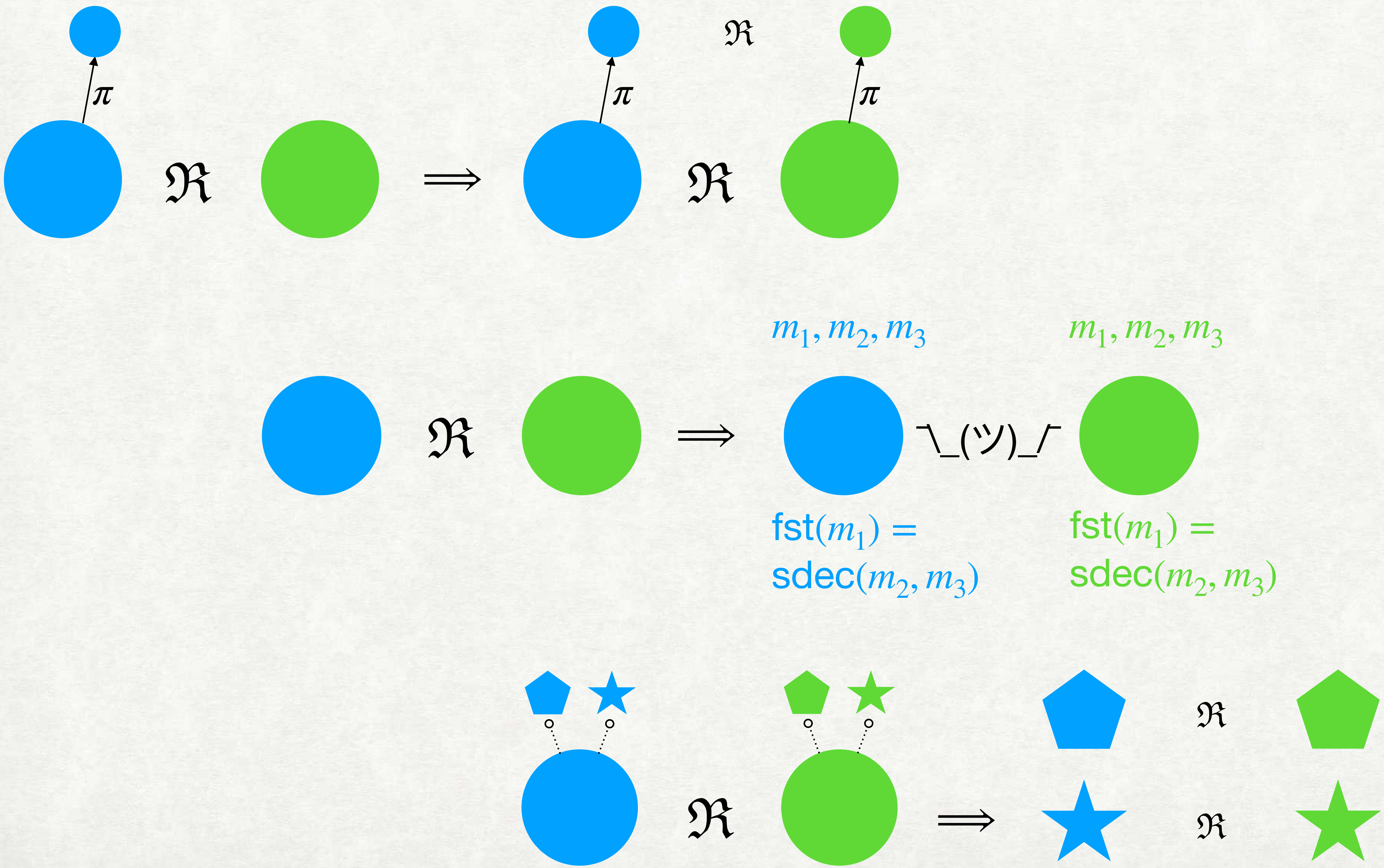
# QUASI-OPEN BISIMILARITY




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

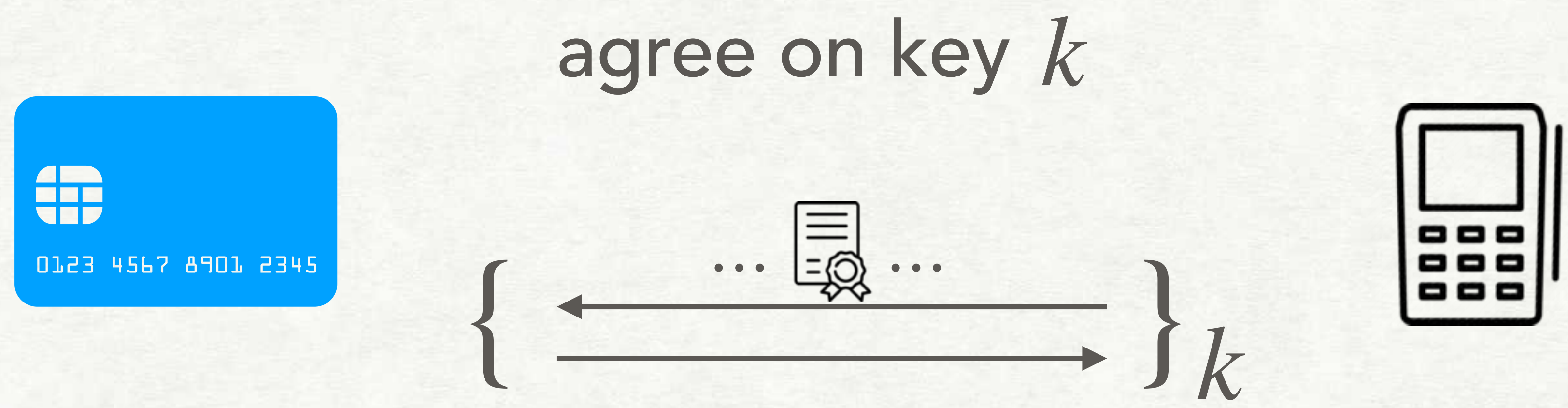
# QUASI-OPEN BISIMILARITY

$P_{\text{Spec}} \sim P_{\text{Impl}} \iff$ 



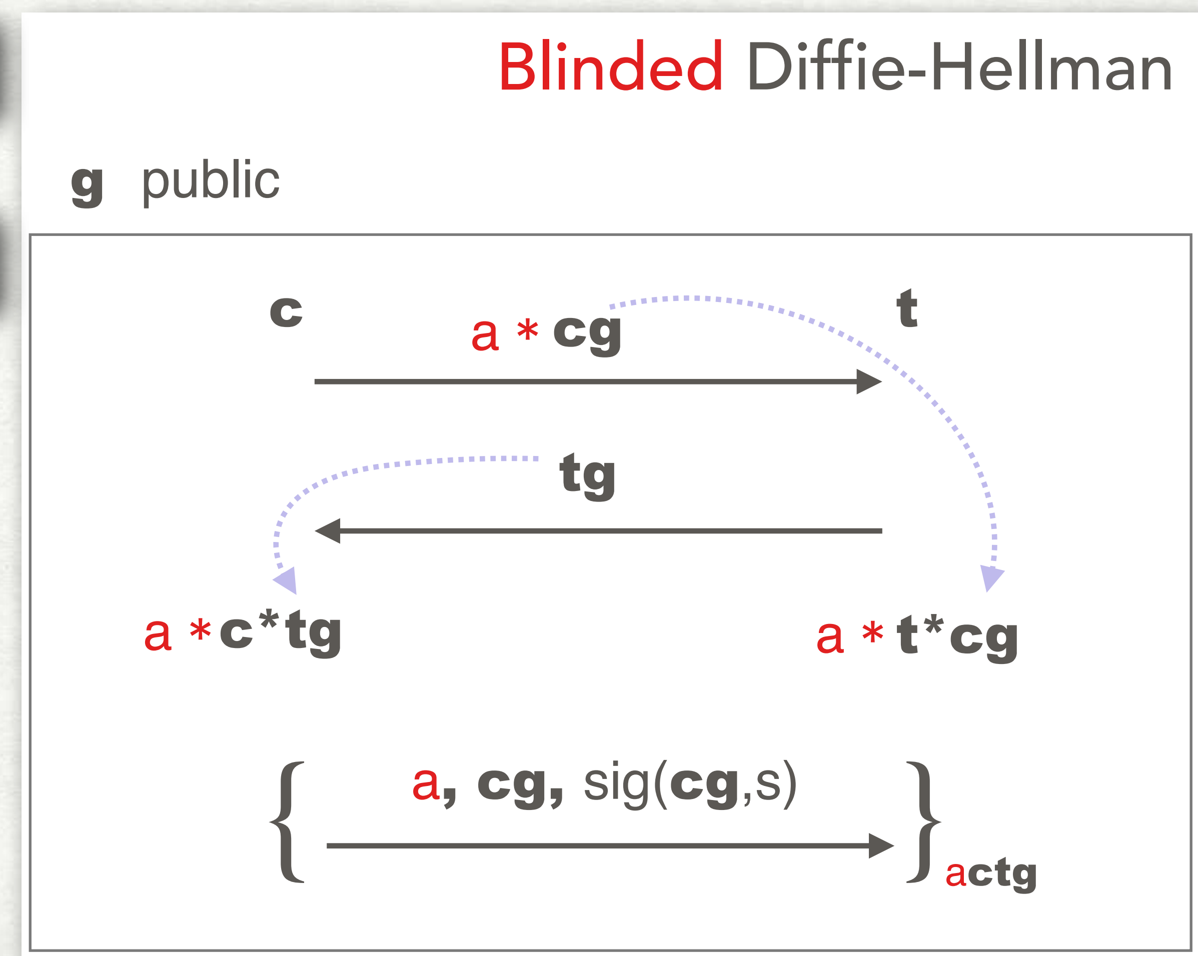
# SMART CARD PAYMENTS (EMV)

# OFFICIAL PROPOSAL: PRIVACY-PROTECTING ENCRYPTION

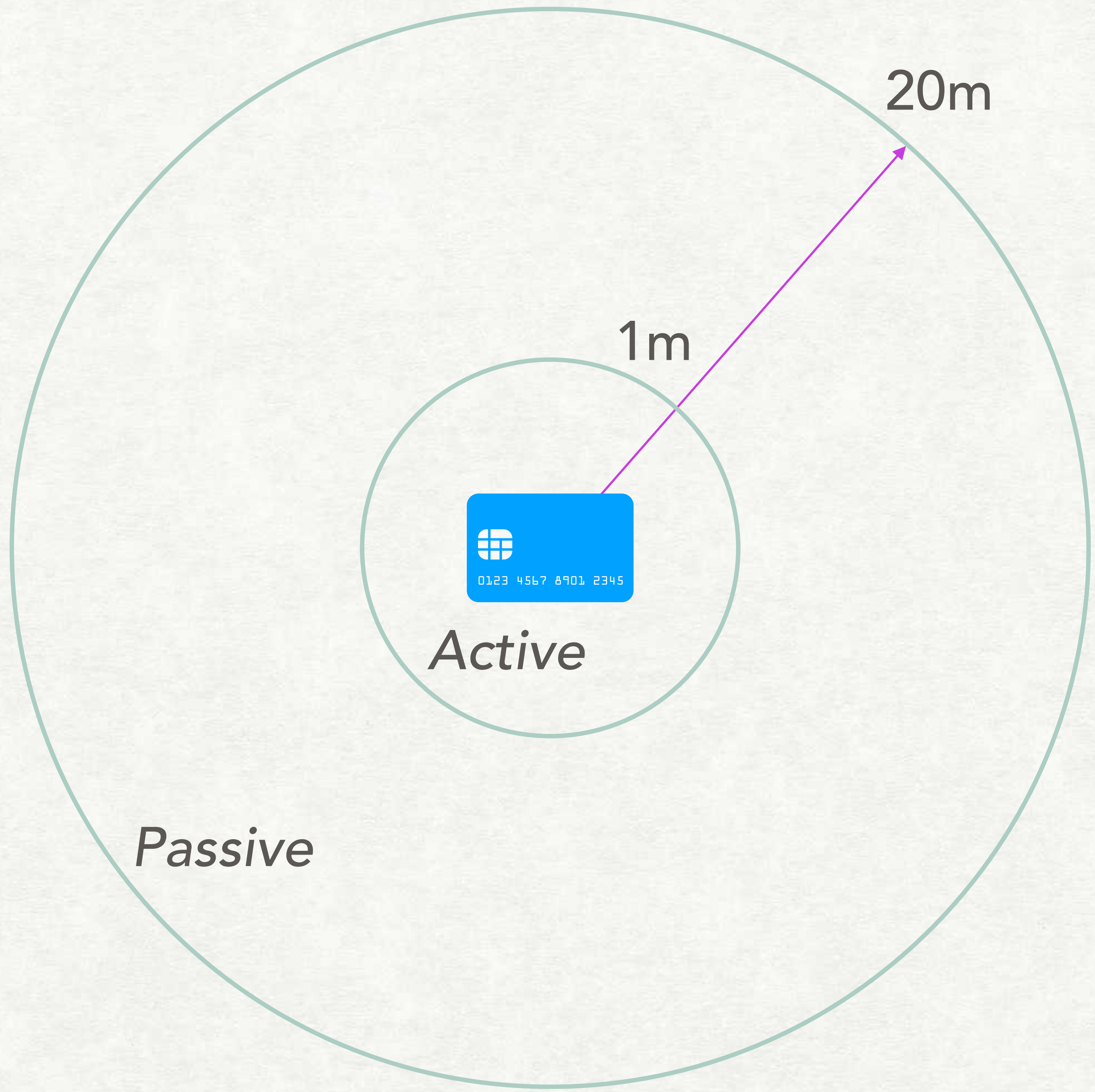



2012: "Blinded Diffie-Hellman RFC", EMVCo LLC

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



# EAVESDROPPER → ACTIVE ATTACKER




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

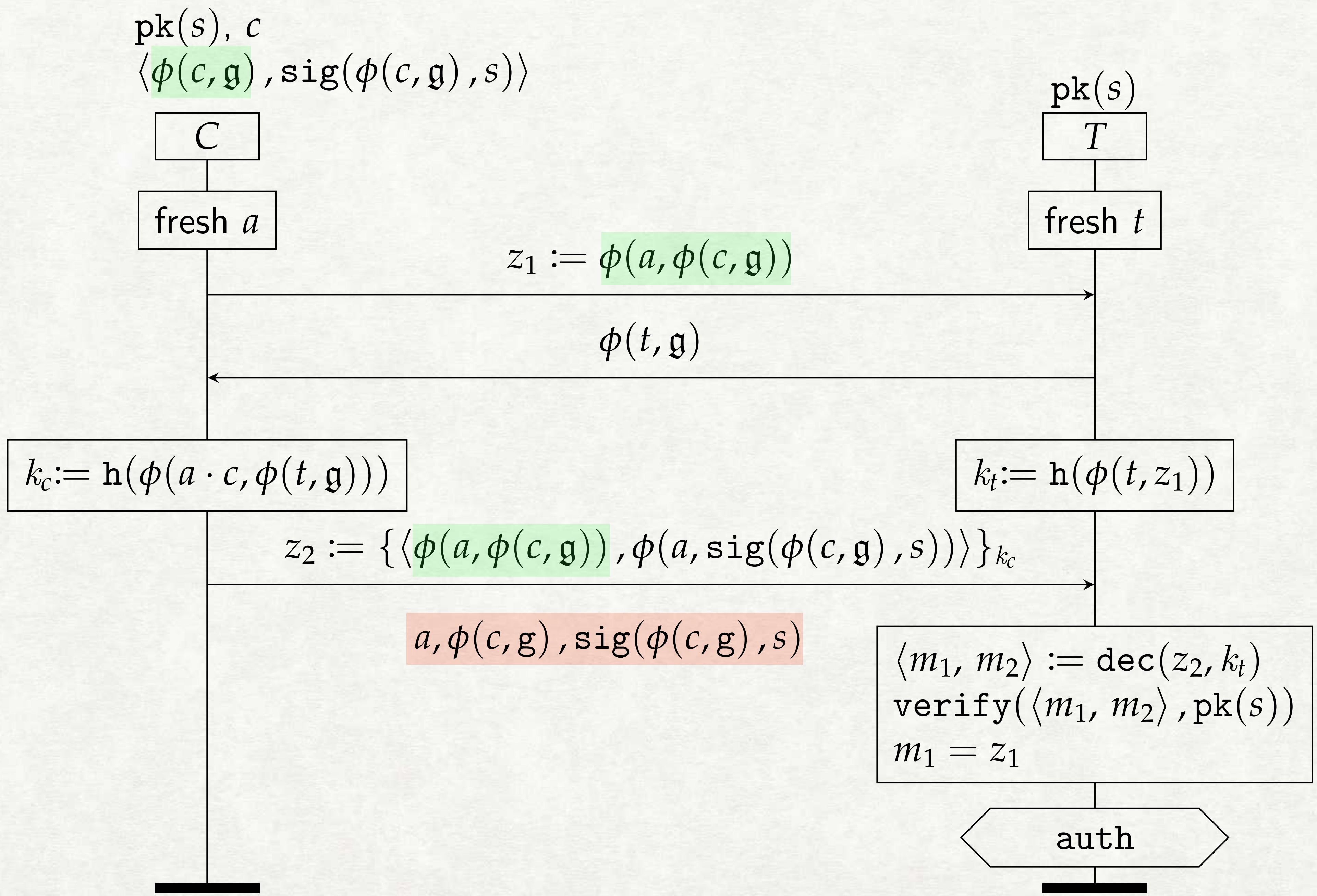
# PASSIVE VS ACTIVE

| | | passive unlinkability | active unlinkability |
|---|---|---|---|
| 1976 | Diffie-Hellman | ✗ | ✗ |
| 2012 | Blinded Diffie-Hellman | ✓ | ✗ |
| | ? | ✓ | ✓ |

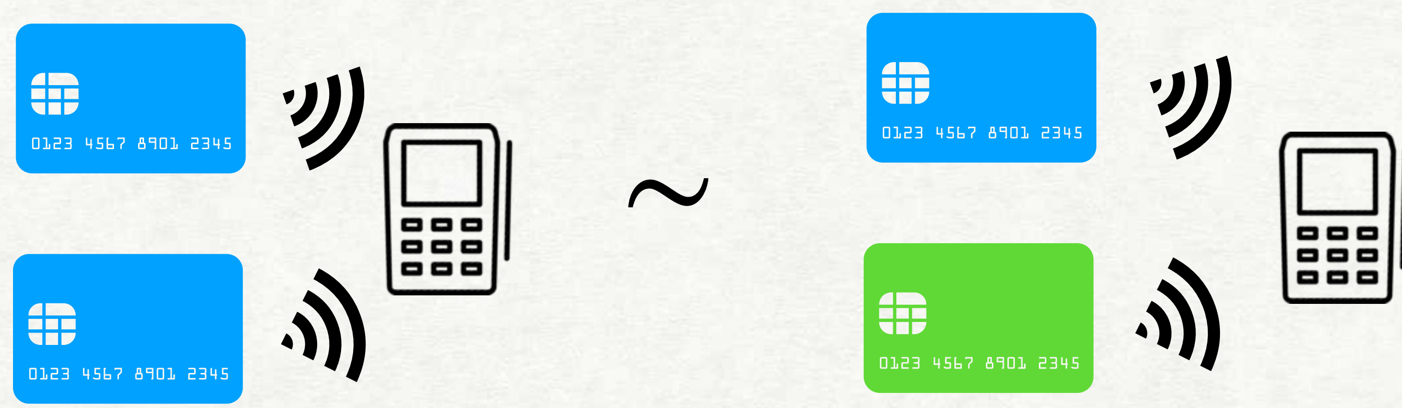
NO IMPROVEMENT

# UNLINKABLE BLINDED DIFFIE-HELLMAN (UBDH)

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



# UNLINKABILITY DEFINITION



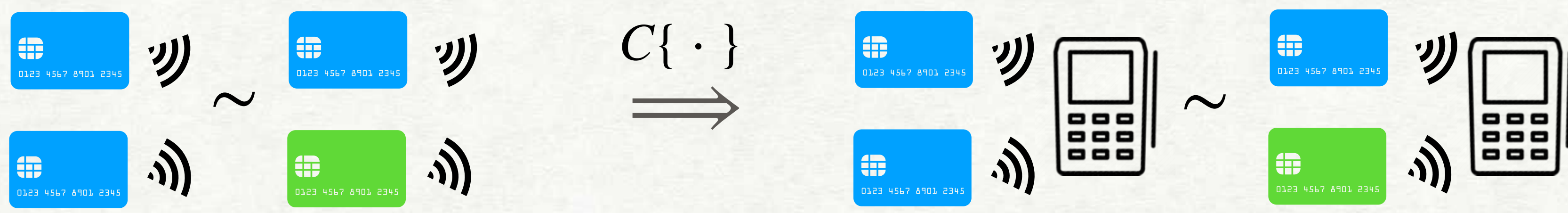

$$\mathrm{Impl} \triangleq \begin{aligned}&\nu s.\Big(\\ &!\nu c.\\ &\quad !\nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \quad \mid\\ &\overline{out}\langle \mathtt{pk}(s)\rangle.\\ &ch_t.\overline{term}\langle ch_t\rangle.T(\mathtt{pk}(s),ch_t)\Big)\end{aligned} \quad \sim \quad \begin{aligned}&\nu s.\Big(\\ &!\nu c.\\ &\quad \nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \quad \mid\\ &\overline{out}\langle \mathtt{pk}(s)\rangle.\\ &ch_t.\overline{term}\langle ch_t\rangle.T(\mathtt{pk}(s),ch_t)\Big)\end{aligned} \triangleq \mathrm{Spec}$$

A card can participate in many sessions.

A card can participates in at most one session.

# CONGRUENCE ENABLES COMPOSITIONAL REASONING

Theorem 1:




Proof.

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

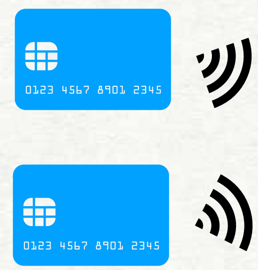
$\blacksquare$

$$\text{Small\_Impl} \triangleq \begin{array}{l} \nu s. \\ \quad \overline{out}\langle \mathtt{pk}(s)\rangle. \\ \quad !\nu c. \\ \quad {\color{red}!}\nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \end{array} \sim \begin{array}{l} \nu s. \\ \quad \overline{out}\langle \mathtt{pk}(s)\rangle. \\ \quad !\nu c. \\ \quad \nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \end{array} \triangleq \text{Small\_Spec}$$

$$\text{Impl} \triangleq \begin{array}{l} \nu s.\Big( \\ \quad !\nu c. \\ \quad\quad {\color{red}!}\nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \ \mid \\ \quad \overline{out}\langle \mathtt{pk}(s)\rangle. \\ \quad \cancel{ch_t.\overline{term}\langle ch_t\rangle.T(\mathtt{pk}(s), ch_t)}\Big) \end{array} \sim \begin{array}{l} \nu s.\Big( \\ \quad !\nu c. \\ \quad\quad \nu ch_c.\overline{card}\langle ch_c\rangle.C(s,c,ch_c) \ \mid \\ \quad \overline{out}\langle \mathtt{pk}(s)\rangle. \\ \quad \cancel{ch_t.\overline{term}\langle ch_t\rangle.T(\mathtt{pk}(s), ch_t)}\Big) \end{array} \triangleq \text{Spec}$$

# BDH PROTOCOL IS NOT UNLINKABLE

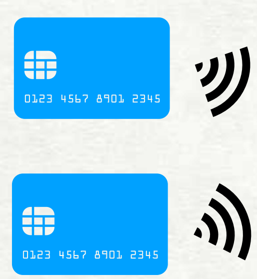
Theorem 2:




$\not\approx$


Proof.

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



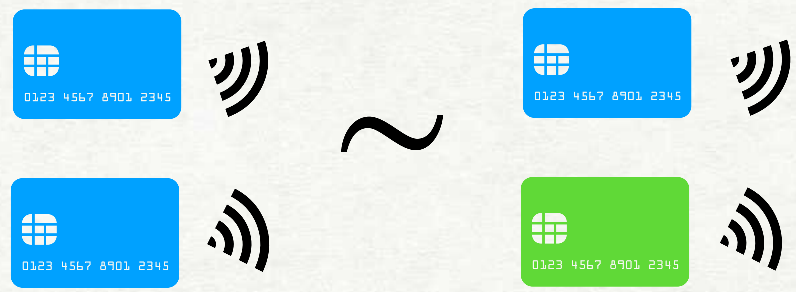

$\models \phi$


$\not\models \phi$

$\blacksquare$

# UBDH PROTOCOL IS UNLINKABLE

Theorem 3:




Proof.

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

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

$$\mathfrak{R}$$

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

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

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

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

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

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

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

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

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

$$\text{fv}(Y_l) \cap (\{v_i | i \in \alpha\} \cup \{w_i | i \in \alpha \cup \beta \cup \gamma \cup \{l\}\}) = \emptyset \qquad \blacksquare$$

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

# KEY AGREEMENT IS FIXED!

| | passive unlinkability | active unlinkability |
|---|---|---|
| DH | ✗ | ✗ |
| BDH | ✓ | ✗ |
| UBDH | ✓ | ✓ |

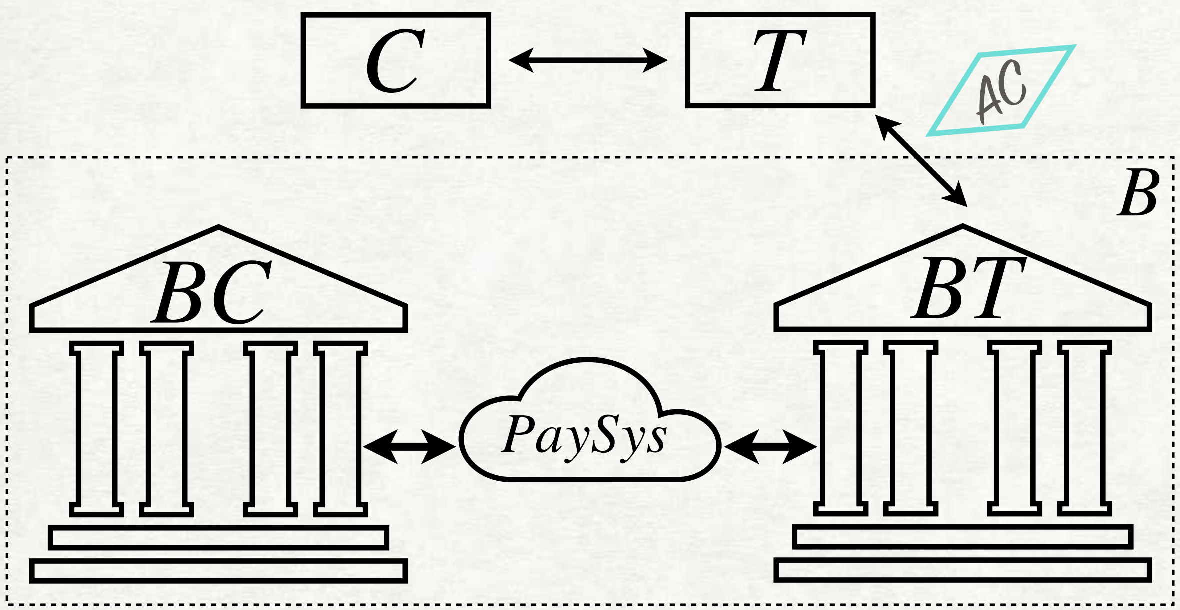
# WHAT ABOUT A FULL PAYMENT PROTOCOL?

2019: EMVCo abandons efforts to enhance privacy.

| | passive unlinkability | active unlinkability |
|---|---|---|
| EMV | ✗ | ✗ |
| BDH + EMV | ✓ | ✗ |
| UBDH + EMV | ✓ | ✗ |
| UBDH + ? = UTX | ✓ | ✓ NO IMPROVEMENT |

# REQUIREMENTS

### *Functional*




- Fast
- The support of PIN
- TX:
  - Offline/Online
  - Contact/Contactless
  - High/Low-Value

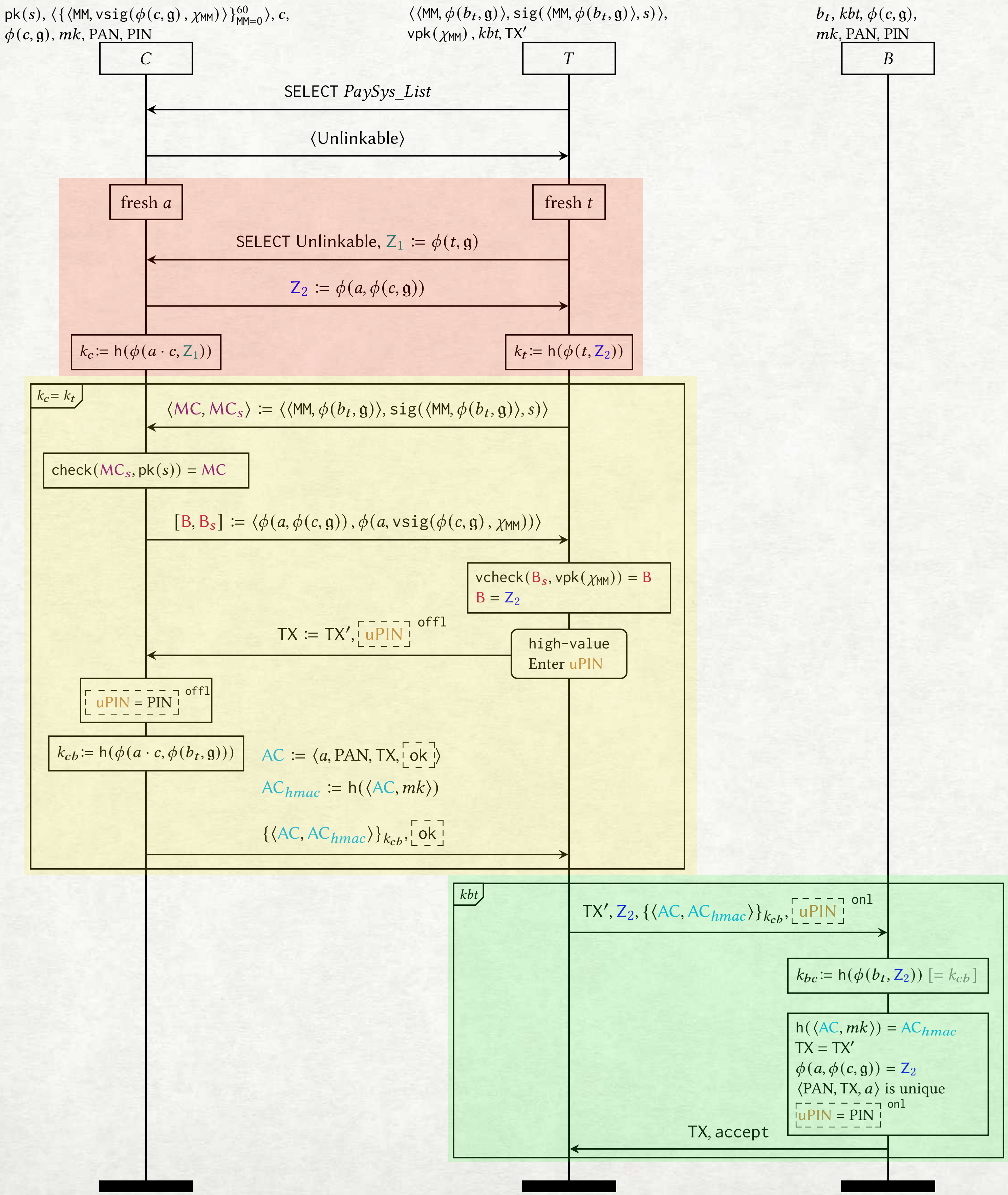
### *Security*

- T authenticates C
  - T checks the legitimacy of C
  - T checks that C is not expired
- Agreement
  - If B accepts the transaction, then B, T, and C agree on the transaction

### *Privacy*

- Unlinkability
  - NO card number PAN
  - NO certificate (public key, signature)
  - NO expiry date

# UTX PROTOCOL



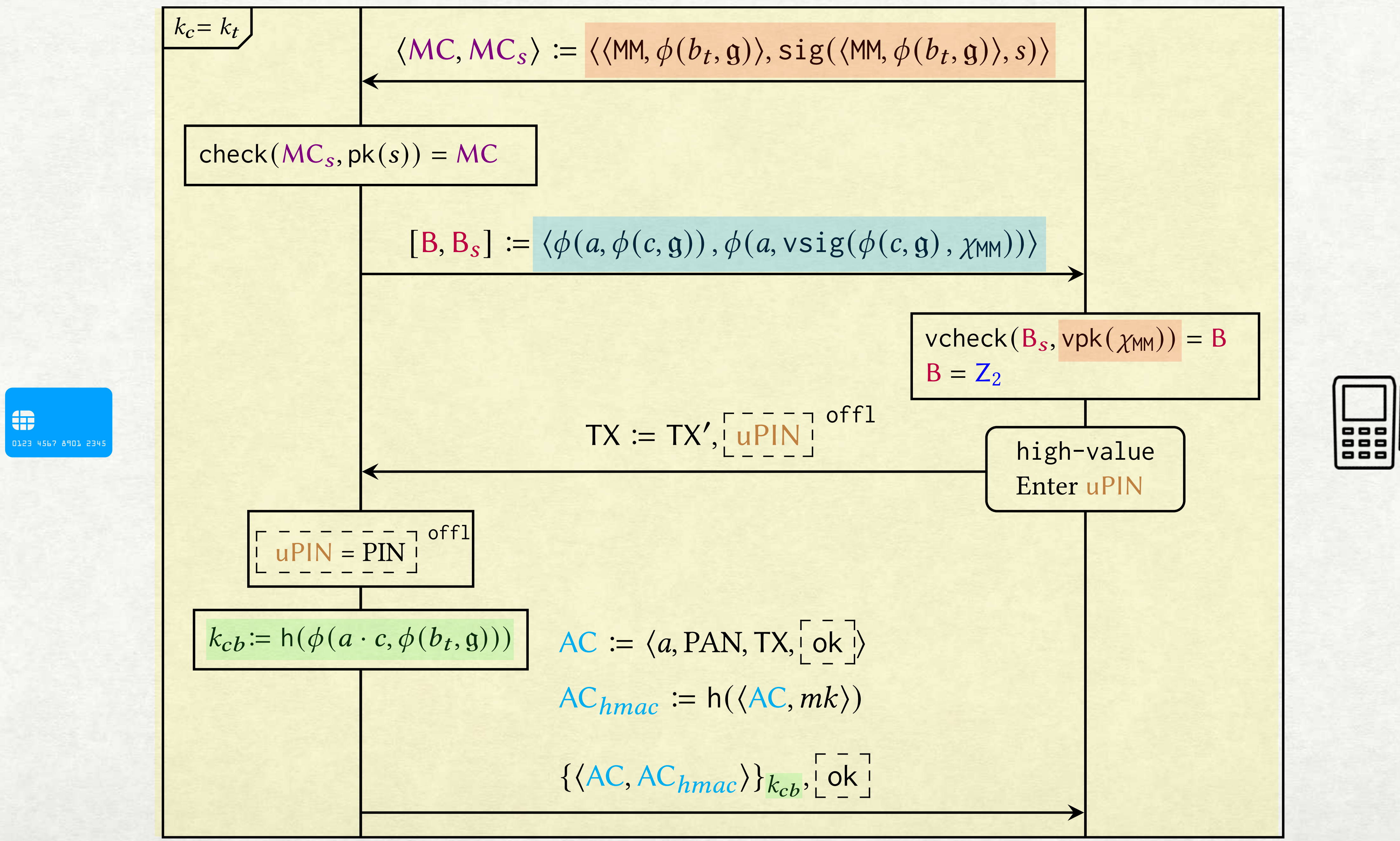

key agreement

card's authentication and cryptogram generation

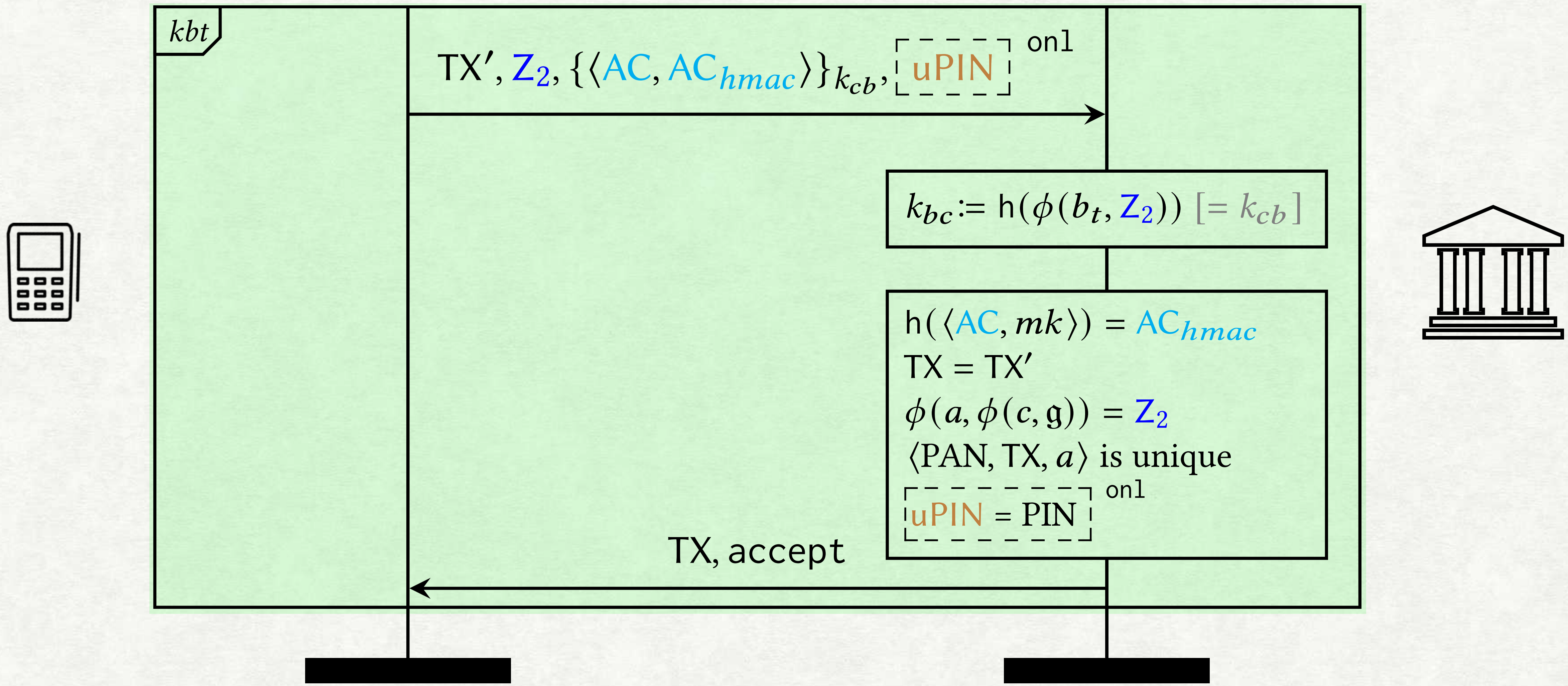
bank's processing

# AUTHENTICATION AND CRYPTOGRAM GENERATION

- Each month PaySys reveals the *signed bank's public key* + the validation key
- The card only responds to the *current and previous months*.
- The card generates a *session key with the bank* and encrypts the PAN.



# BANK'S PROCESSING



# UTX PROTOCOL IS UNLINKABLE

**Theorem 5:**

$$
\begin{array}{l}
\nu\, user, s, si, \chi_{\mathsf{MM}}.\overline{out}\langle \mathsf{pk}(s)\rangle.\overline{out}\langle \mathsf{vpk}(\chi_{\mathsf{MM}})\rangle.\Big(\\
\quad !\nu \mathrm{PIN}, mk, c, \mathrm{PAN}.\big(\\
\quad\quad \mathtt{let}\ \mathsf{crtC} := \mathtt{vsig}(\phi(c,\mathfrak{g}), \chi_{\mathsf{MM}})\ \mathtt{in}\\
\quad\quad\quad !\nu ch.\overline{card}\langle ch\rangle.C(ch, c, \mathsf{pk}(s), \mathsf{crtC}, \mathrm{PAN}, mk, \mathrm{PIN})\\
\quad\quad \mid\ !\overline{user}\langle \mathrm{PIN}\rangle \mid\ !\overline{\langle si, \mathrm{PAN}\rangle}\langle\langle \mathrm{PIN}, mk, \phi(c,\mathfrak{g})\rangle\rangle\ \big) \mid\\
\quad \nu b_t.!\nu kbt.\big(\\
\quad\quad \nu ch.\overline{bank}\langle ch\rangle.B(ch, si, kbt, b_t) \mid\\
\quad\quad \mathtt{let}\ \mathsf{crt} := \langle\langle \mathsf{MM}, \phi(b_t,\mathfrak{g})\rangle, \mathtt{sig}(\langle \mathsf{MM}, \phi(b_t,\mathfrak{g})\rangle, s)\rangle \mathtt{in}\\
\quad\quad \nu ch.\overline{term}\langle ch\rangle.T(user, ch, \mathsf{vpk}(\chi_{\mathsf{MM}}), \mathsf{crt}, kbt)\big)\ \Big)
\end{array}
\sim
\begin{array}{l}
\nu\, user, s, si, \chi_{\mathsf{MM}}.\overline{out}\langle \mathsf{pk}(s)\rangle.\overline{out}\langle \mathsf{vpk}(\chi_{\mathsf{MM}})\rangle.\Big(\\
\quad !\nu \mathrm{PIN}, mk, c, \mathrm{PAN}.\big(\\
\quad\quad \mathtt{let}\ \mathsf{crtC} := \mathtt{vsig}(\phi(c,\mathfrak{g}), \chi_{\mathsf{MM}})\ \mathtt{in}\\
\quad\quad\quad \nu ch.\overline{card}\langle ch\rangle.C(ch, c, \mathsf{pk}(s), \mathsf{crtC}, \mathrm{PAN}, mk, \mathrm{PIN})\\
\quad\quad \mid\ !\overline{user}\langle \mathrm{PIN}\rangle \mid\ !\overline{\langle si, \mathrm{PAN}\rangle}\langle\langle \mathrm{PIN}, mk, \phi(c,\mathfrak{g})\rangle\rangle\ \big) \mid\\
\quad \nu b_t.!\nu kbt.\big(\\
\quad\quad \nu ch.\overline{bank}\langle ch\rangle.B(ch, si, kbt, b_t) \mid\\
\quad\quad \mathtt{let}\ \mathsf{crt} := \langle\langle \mathsf{MM}, \phi(b_t,\mathfrak{g})\rangle, \mathtt{sig}(\langle \mathsf{MM}, \phi(b_t,\mathfrak{g})\rangle, s)\rangle \mathtt{in}\\
\quad\quad \nu ch.\overline{term}\langle ch\rangle.T(user, ch, \mathsf{vpk}(\chi_{\mathsf{MM}}), \mathsf{crt}, kbt)\big)\ \Big)
\end{array}
$$

**Proof.**

$$
\begin{array}{l}
(K, F, A, \Gamma, B)_{\mathrm{spec}}(X, Y, Z) \triangleq\\
\nu\, \vec{\epsilon}, \mathrm{PIN}_{1\ldots D+K}, mk_{1\ldots D+K}, c_{1\ldots D+K}, \mathrm{PAN}_{1\ldots D+K},\\
\dot{ch}_{1\ldots D}, a_{1\ldots E}, b_t, ch_{1\ldots F+G+M}, \ddot{ch}_{1\ldots F+G},\\
\dddot{ch}_{1\ldots F+M}, t_{1\ldots L}, \mathrm{TX}_{1\ldots L}.(\ \sigma \mid\\
\quad C_1 \mid \ldots \mid 0 \mid !\overline{user}\langle \mathrm{PIN}_1\rangle\mid\\
\quad\quad \ldots \mid 0 \mid !\overline{\langle si, \mathrm{PAN}_1\rangle}\langle\langle \mathrm{PIN}_1, mk_1, \phi(c_1,\mathfrak{g})\rangle\rangle) \mid\\
\quad \ldots\\
\quad C_i \mid \ldots \mid 0 \mid !\overline{user}\langle \mathrm{PIN}_i\rangle\mid\\
\quad\quad \ldots \mid 0 \mid !\overline{\langle si, \mathrm{PAN}_i\rangle}\langle\langle \mathrm{PIN}_i, mk_i, \phi(c_i,\mathfrak{g})\rangle\rangle) \mid\\
\quad \ldots\\
\quad C_{D+K} \mid \ldots \mid 0 \mid !\overline{user}\langle \mathrm{PIN}_{D+K}\rangle\mid\\
\quad\quad \ldots \mid 0 \mid !\overline{\langle si, \mathrm{PAN}_{D+K}\rangle}\langle\langle \mathrm{PIN}_{D+K}, mk_{D+K}, \phi(c_{D+K},\mathfrak{g})\rangle\rangle) \mid\\
\quad !PC_{\mathrm{spec}} \mid\\
\quad B_1 \mid T_1 \mid\\
\quad \ldots \mid\\
\quad B_j \mid T_j \mid\\
\quad \ldots \mid\\
\quad B_{F+G+M} \mid T_{F+G+M} \mid !PBT)
\end{array}
$$

$$
UTX_{\mathrm{spec}} \quad \mathfrak{R} \quad UTX_{\mathrm{impl}}
$$

$$
\begin{array}{rcl}
\begin{array}{r} UTX^1_{\mathrm{spec}} \triangleq\\ \nu\vec{\epsilon}.(\left\{^{\mathsf{pk}(s)}/_{pk_s}\right\} \mid\\ \overline{out}\langle \mathsf{vpk}(\chi_{\mathsf{MM}})\rangle.\\ (!PC_{\mathrm{spec}} \mid \nu b_t.!PBT)) \end{array} & \mathfrak{R} & \begin{array}{l} UTX^1_{\mathrm{impl}} \triangleq\\ \nu\vec{\epsilon}.(\left\{^{\mathsf{pk}(s)}/_{pk_s}\right\} \mid\\ \overline{out}\langle \mathsf{vpk}(\chi_{\mathsf{MM}})\rangle.\\ (!PC_{\mathrm{impl}} \mid \nu b_t.!PBT)) \end{array}\\
\begin{array}{r} UTX^2_{\mathrm{spec}} \triangleq\\ \nu\vec{\epsilon}.(\sigma_0 \mid !PC_{\mathrm{spec}} \mid \nu b_t.!PBT) \end{array} & \mathfrak{R} & \begin{array}{l} UTX^2_{\mathrm{impl}} \triangleq\\ \nu\vec{\epsilon}.(\sigma_0 \mid !PC_{\mathrm{impl}} \mid \nu b_t.!PBT) \end{array}\\
(K, F, A, \Gamma, B)_{\mathrm{spec}}(X, Y, Z) & \mathfrak{R} & (\vec{K}, F, A, \Gamma, B, \Lambda)_{\mathrm{impl}}(X, Y, Z)
\end{array}
$$

$$
T_i = \begin{cases}
\mathcal{TONH}_1(user, \vec{\psi}_i) & \text{if } i \in \gamma^{\mathrm{on}}_1\\
\mathcal{TONH}_2(user, \vec{\psi}_i, t_i, \mathrm{TX}_i) & \text{if } i \in \gamma^{\mathrm{on}}_2\\
\mathcal{TONH}_3(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma) & \text{if } i \in \gamma^{\mathrm{on}}_3\\
\mathcal{TONH}_4(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma) & \text{if } i \in \gamma^{\mathrm{on}}_4\\
\mathcal{TONH}_5(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma) & \text{if } i \in \gamma^{\mathrm{on}}_5\\
\mathcal{TONH}_6(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}) & \text{if } i \in \gamma^{\mathrm{on}}_6\\
\mathcal{TONH}_7(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}) & \text{if } i \in \gamma^{\mathrm{on}}_7\\
\mathcal{TONH}_8(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}, Z^3_i\sigma) & \text{if } i \in \gamma^{\mathrm{on}}_8\\
\mathcal{TONH}_9(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}, Z^3_i\sigma) & \text{if } i \in \gamma^{\mathrm{on}}_9\\
\mathcal{TONH}_{10}(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}, Z^3_i\sigma, \mathrm{R}) & \text{if } i \in \gamma^{\mathrm{on}}_{10}\\
\mathcal{TONH}_{11} & \text{if } i \in \gamma^{\mathrm{on}}_{11}\\
\mathcal{TOFH}_1(user, \vec{\psi}_i) & \text{if } i \in \gamma^{\mathrm{of}}_1\\
\mathcal{TOFH}_2(user, \vec{\psi}_i, t_i, \mathrm{TX}_i) & \text{if } i \in \gamma^{\mathrm{of}}_2\\
\mathcal{TONH}_3(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma) & \text{if } i \in \gamma^{\mathrm{of}}_3\\
\mathcal{TONH}_4(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma) & \text{if } i \in \gamma^{\mathrm{of}}_4\\
\mathcal{TONH}_5(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma) & \text{if } i \in \gamma^{\mathrm{of}}_5\\
\mathcal{TONH}_6(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}) & \text{if } i \in \gamma^{\mathrm{of}}_6\\
\mathcal{TONH}_7(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}) & \text{if } i \in \gamma^{\mathrm{of}}_7\\
\mathcal{TONH}_8(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}, Z^3_i\sigma) & \text{if } i \in \gamma^{\mathrm{of}}_8\\
\mathcal{TONH}_9(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}, Z^3_i\sigma) & \text{if } i \in \gamma^{\mathrm{of}}_9\\
\mathcal{TONH}_{10}(user, \vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, \mathrm{uPIN}, Z^3_i\sigma) & \text{if } i \in \gamma^{\mathrm{of}}_{10}\\
\mathcal{TONH}_{11} & \text{if } i \in \gamma^{\mathrm{of}}_{11}\\
\mathcal{TLO}_1(\vec{\psi}_i) & \text{if } i \in \gamma^{\mathrm{lo}}_1\\
\mathcal{TLO}_2(\vec{\psi}_i, t_i, \mathrm{TX}_i) & \text{if } i \in \gamma^{\mathrm{lo}}_2\\
\mathcal{TLO}_3(\vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma) & \text{if } i \in \gamma^{\mathrm{lo}}_3\\
\mathcal{TLO}_4(\vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma) & \text{if } i \in \gamma^{\mathrm{lo}}_4\\
\mathcal{TLO}_5(\vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma) & \text{if } i \in \gamma^{\mathrm{lo}}_5\\
\mathcal{TLO}_6(\vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma) & \text{if } i \in \gamma^{\mathrm{lo}}_6\\
\mathcal{TLO}_7(\vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, Z^3_i\sigma) & \text{if } i \in \gamma^{\mathrm{lo}}_7\\
\mathcal{TLO}_8(\vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, Z^3_i\sigma) & \text{if } i \in \gamma^{\mathrm{lo}}_8\\
\mathcal{TLO}_9(\vec{\psi}_i, t_i, \mathrm{TX}_i, Z^1_i\sigma, Z^2_i\sigma, Z^3_i\sigma, \mathrm{R}) & \text{if } i \in \gamma^{\mathrm{lo}}_9\\
\mathcal{TLO}_{10} & \text{if } i \in \gamma^{\mathrm{lo}}_{10}
\end{cases}
$$

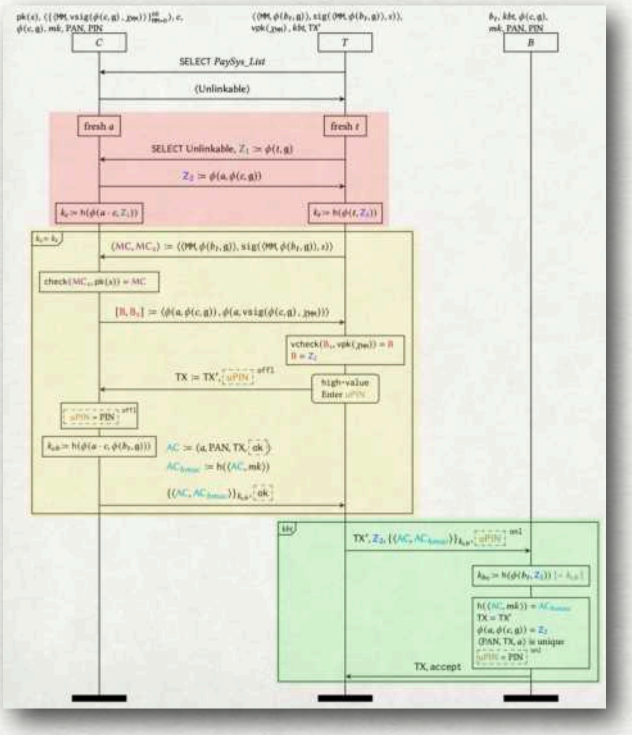
$$
\begin{array}{l}
(\vec{K}, F, A, \Gamma, B, \Lambda)_{\mathrm{impl}}(X, Y, Z) \triangleq\\
\nu\vec{\epsilon}, \mathrm{PIN}_{1\ldots H}, mk_{1\ldots H}, c_{1\ldots H}, \mathrm{PAN}_{1\ldots H}, \dot{ch}_{1\ldots D},\\
a_{1\ldots E}, b_t, ch_{1\ldots F+G+M}, \ddot{ch}_{1\ldots F+G}, \dddot{ch}_{1\ldots F+M}\\
t_{1\ldots L}, \mathrm{TX}_{1\ldots L}.(\ \theta \mid\\
\quad C^1_1 \mid U^1_1 \mid DB^1_1 \mid\\
\quad \ldots\\
\quad C^1_{i_1} \mid U^1_{i_1} \mid DB^1_{i_1} \mid\\
\quad \ldots\\
\quad C^1_{D_1+K_1} \mid U^1_{D_1+K_1} \mid DB^1_{D_1+K_1} \mid\\
\quad !(\nu ch.\overline{card}\langle ch\rangle.\\
\quad C(ch, c_j, \mathsf{pk}(s), \mathtt{vsig}(\phi(c,\mathfrak{g}), \chi_{\mathsf{MM}}), \mathrm{PAN}_j, mk_j, \mathrm{PIN}_j) \mid\\
\quad \overline{user}\langle \mathrm{PIN}_1\rangle\mid DB(si, \mathrm{PAN}_1, mk_1, \mathrm{PIN}_1)) \mid\\
\quad \ldots\\
\quad C^h_{D_{h-1}+K_{h-1}+1} \mid U^h_{D_{h-1}+K_{h-1}+1} \mid DB^h_{D_{h-1}+K_{h-1}+1} \mid\\
\quad \ldots\\
\quad C^h_{i_h} \mid U^h_{i_h} \mid DB^h_{i_h} \mid\\
\quad \ldots\\
\quad C^h_{D_{h-1}+K_{h-1}+D_h+K_h} \mid U^h_{D_{h-1}+K_{h-1}+D_h+K_h} \mid\\
\quad\quad DB^h_{D_{h-1}+K_{h-1}+D_h+K_h} \mid\\
\quad !(\nu ch.\overline{card}\langle ch\rangle.\\
\quad C(ch, c_h, \mathsf{pk}(s), \mathtt{vsig}(\phi(c,\mathfrak{g}), \chi_{\mathsf{MM}}), \mathrm{PAN}_h, mk_h, \mathrm{PIN}_h) \mid\\
\quad \overline{user}\langle \mathrm{PIN}_h\rangle\mid DB(si, \mathrm{PAN}_h, mk_h, \mathrm{PIN}_h)) \mid\\
\quad \ldots\\
\quad C^H_{D_{H-1}+K_{H-1}+1} \mid U^H_{D_{H-1}+K_{H-1}+1} \mid DB^H_{D_{H-1}+K_{H-1}+1} \mid\\
\quad \ldots\\
\quad C^H_{i_H} \mid U^H_{i_H} \mid DB^H_{i_H} \mid\\
\quad \ldots\\
\quad C^H_{D_{H-1}+K_{H-1}+D_H+K_H} \mid U^H_{D_{H-1}+K_{H-1}+D_H+K_H} \mid\\
\quad\quad DB^H_{D_{H-1}+K_{H-1}+D_H+K_H} \mid\\
\quad !(\nu ch.\overline{card}\langle ch\rangle.\\
\quad C(ch, c_H, \mathsf{pk}(s), \mathtt{vsig}(\phi(c,\mathfrak{g}), \chi_{\mathsf{MM}}), \mathrm{PAN}_H, mk_H, \mathrm{PIN}_H) \mid\\
\quad \overline{user}\langle \mathrm{PIN}_H\rangle\mid DB(si, \mathrm{PAN}_H, mk_H, \mathrm{PIN}_H)) \mid\\
\quad !PC_{\mathrm{impl}} \mid\\
\quad B_1 \mid T_1 \mid\\
\quad \ldots \mid\\
\quad B_j \mid T_j \mid\\
\quad \ldots \mid\\
\quad B_{F+G+M} \mid T_{F+G+M} \mid !PBT)
\end{array}
$$

$\blacksquare$

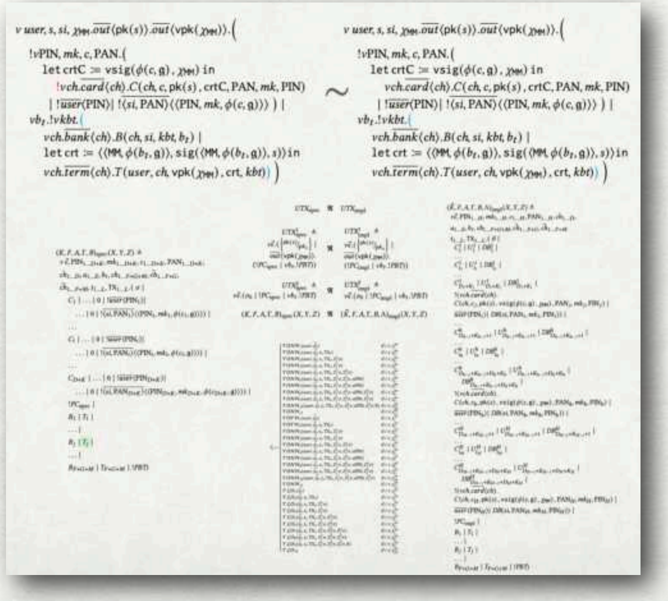
- Define a relation (hard)
- Verify it is a quasi-open bisimulation (less hard)

# CONTRIBUTIONS

- UTX: a practical and provably unlinkable secure **payment protocol**.



- A **methodology** of proving privacy properties.



# 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?***

*UBDH and UTX have been analysed, compositionality allows to reduce the amount of work, direction for future work is an automated proof certificate verifier.*


# Thank you!

# PUBLICATIONS

- Compositional Analysis of Protocol Equivalence in the Applied pi-Calculus Using Quasi-open Bisimilarity – Horne, Ross James; Mauw, Sjouke; Yurkov, Semen; Cerone, Antonio; Ölveczky, Peter Csaba in Theoretical Aspects of Computing – ICTAC (2021)
- Unlinkability of an Improved Key Agreement Protocol for EMV 2nd Gen Payments – Horne, Ross James; Mauw, Sjouke; Yurkov, Semen in 35th IEEE Computer Security Foundations Symposium (CSF) (2022)
- When privacy fails, a formula describes an attack: A complete and compositional verification method for the applied pi-calculus – Horne, Ross James; Mauw, Sjouke; Yurkov, Semen in Theoretical Computer Science, Elsevier (2023)
- full protocol paper (under submission)