UNIVERSITÉ DU LUXEMBOURG

Provably unlinkable smart card-based payments

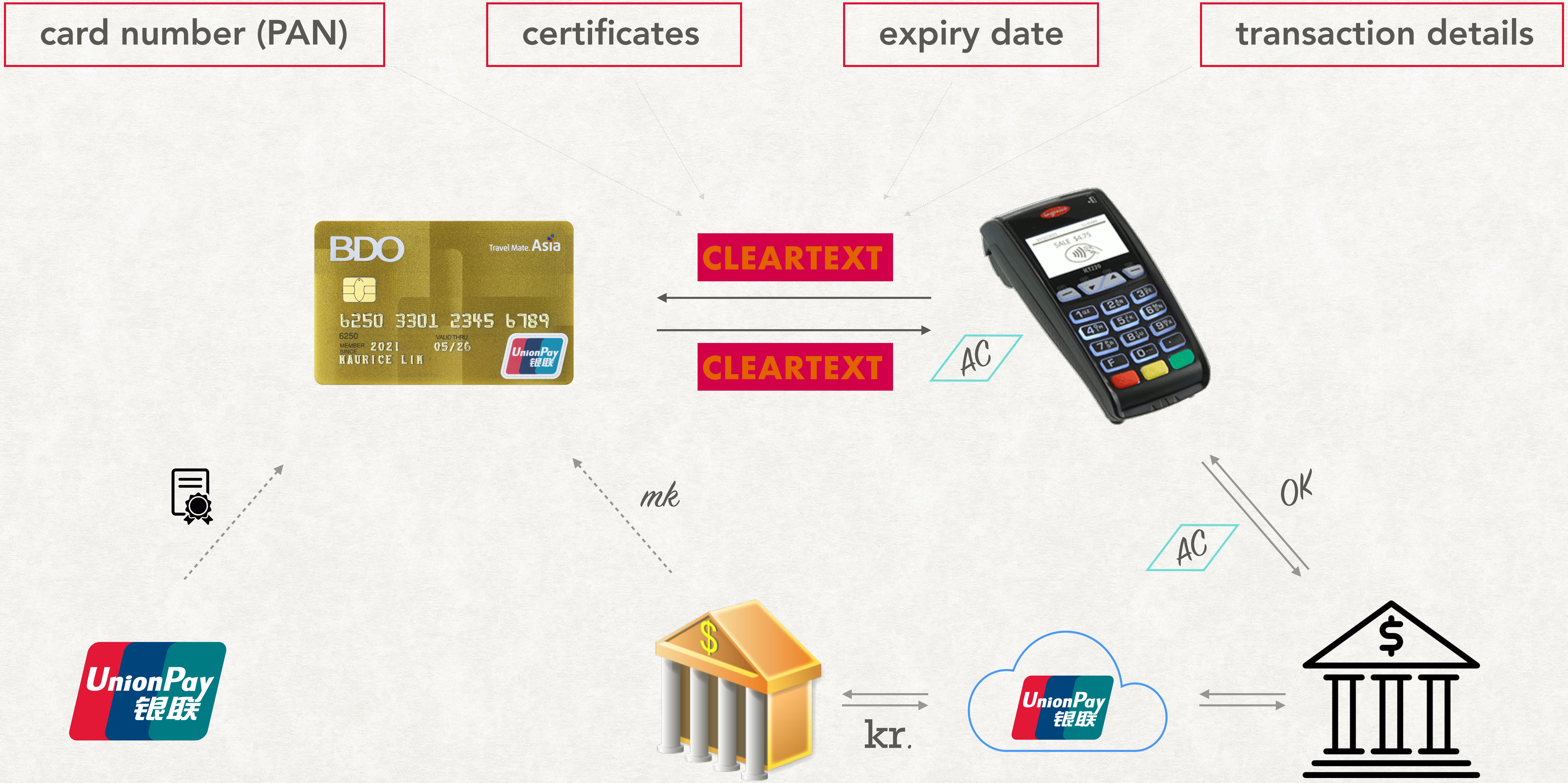
Sergiu Bursuc, Ross Horne, Sjouke Mauw, Semyon Yurkov

28 November, 2023

Luxembourg National Research Fund

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

SMART CARD PAYMENTS (EMV)



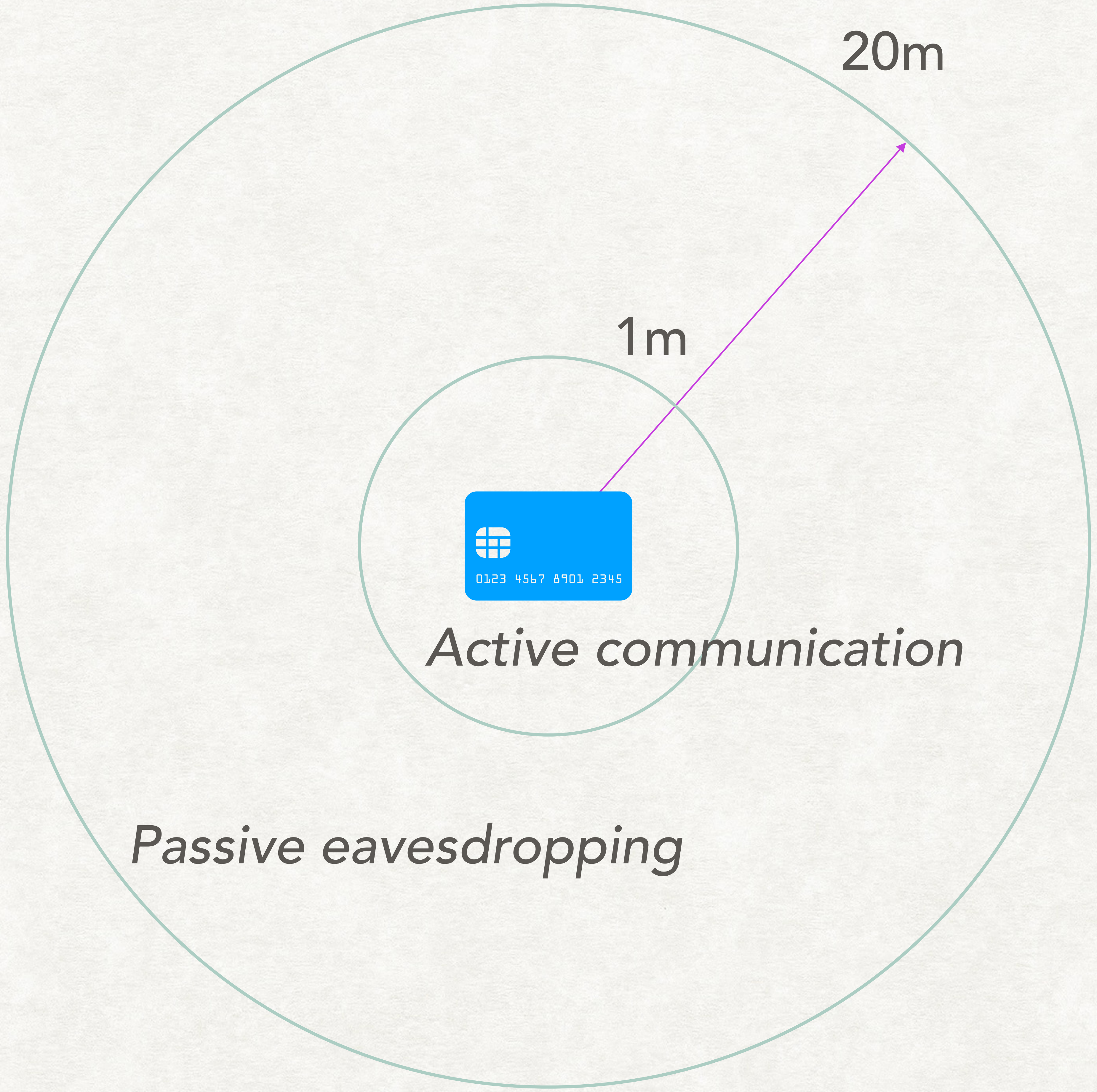
card number (PAN)

certificates

expiry date

transaction details

ACTIVE ATTACKERS CAN ACTIVATE THE CARD



20m

1m

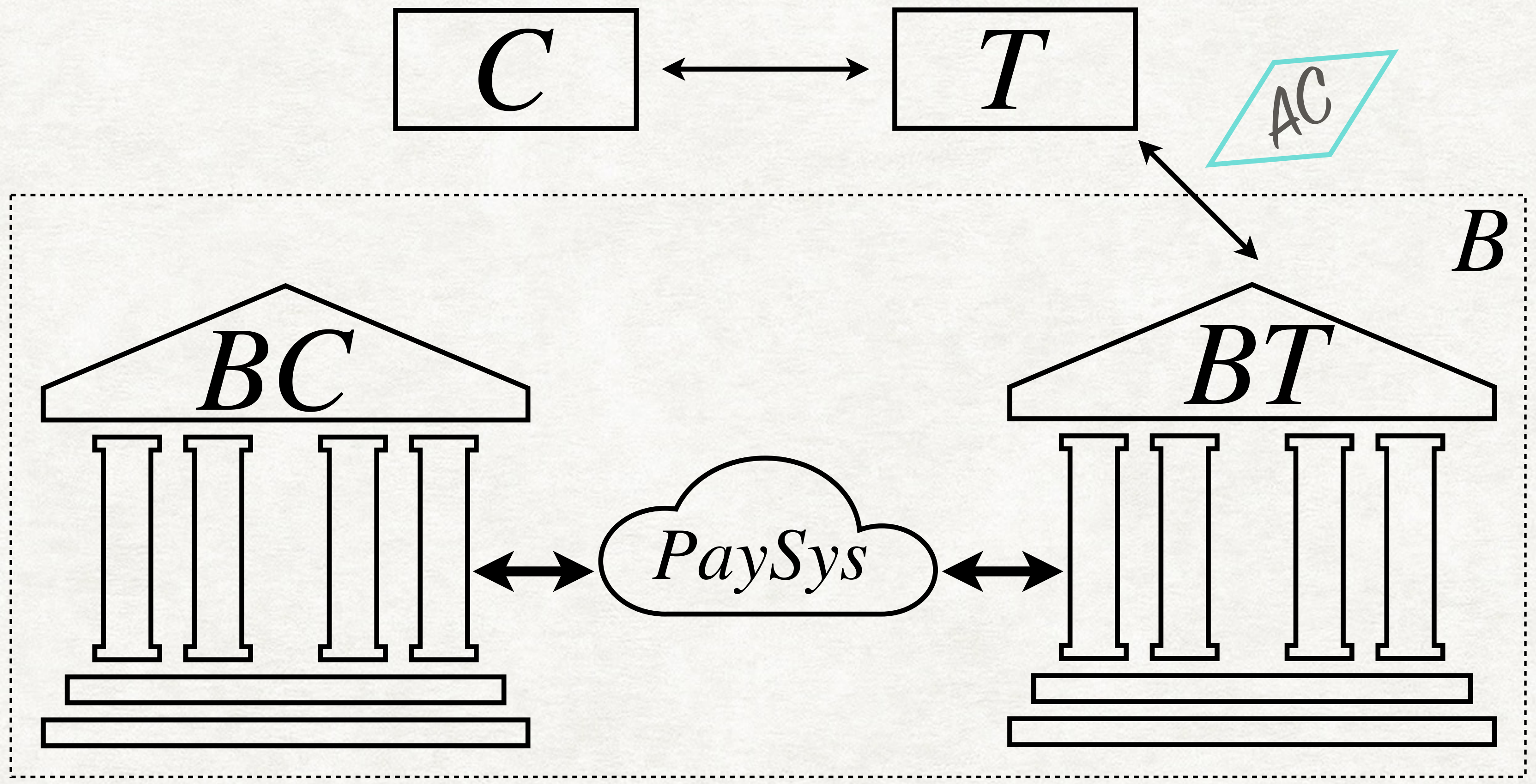
Active communication

Passive eavesdropping

- *To the card* an active attacker is indistinguishable from the honest terminal
- The cardholder, however, never enters their PIN into a random terminal that pop up on the street

REQUIREMENTS

Functional



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

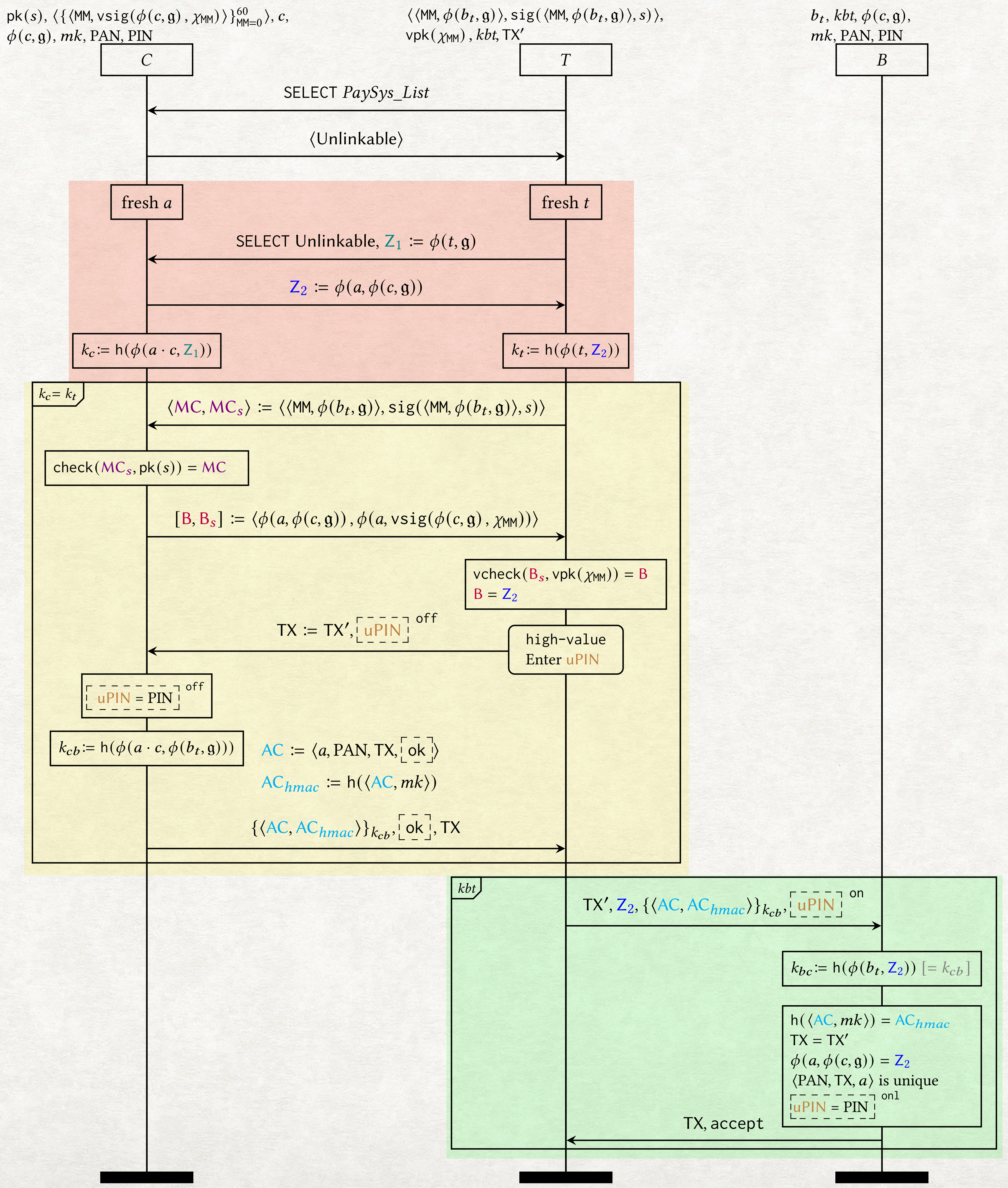
Security

- 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: PHASES



pk(s), $\langle \{\langle$MM, vsig($\phi(c,\mathfrak{g})$, χ_{MM})$\rangle\}_{\text{MM}=0}^{60}\rangle$, c, $\phi(c,\mathfrak{g})$, mk, PAN, PIN
$\langle\langle$MM, $\phi(b_t,\mathfrak{g})\rangle$, sig($\langle$MM, $\phi(b_t,\mathfrak{g})\rangle$, s)$\rangle$, vpk(χ_{MM}), kbt, TX′
b_t, kbt, $\phi(c,\mathfrak{g})$, mk, PAN, PIN
C
T
B
SELECT $PaySys\_List$
⟨Unlinkable⟩
fresh a
fresh t
SELECT Unlinkable, $Z_1 := \phi(t,\mathfrak{g})$
$Z_2 := \phi(a,\phi(c,\mathfrak{g}))$
$k_c := h(\phi(a\cdot c, Z_1))$
$k_t := h(\phi(t, Z_2))$
$k_c = k_t$
$\langle MC, MC_s\rangle := \langle\langle MM, \phi(b_t,\mathfrak{g})\rangle, sig(\langle MM, \phi(b_t,\mathfrak{g})\rangle, s)\rangle$
check(MC_s, pk(s)) = MC
$[B, B_s] := \langle \phi(a,\phi(c,\mathfrak{g})), \phi(a, vsig(\phi(c,\mathfrak{g}), \chi_{MM}))\rangle$
vcheck(B_s, vpk(χ_{MM})) = B
B = Z_2
TX := TX′, uPIN off
high-value
Enter uPIN
uPIN = PIN off
$k_{cb} := h(\phi(a\cdot c, \phi(b_t,\mathfrak{g})))$
AC := ⟨a, PAN, TX, ok⟩
$AC_{hmac} := h(\langle AC, mk\rangle)$
$\{\langle AC, AC_{hmac}\rangle\}_{k_{cb}}$, ok, TX
kbt
TX′, Z_2, $\{\langle AC, AC_{hmac}\rangle\}_{k_{cb}}$, uPIN on
$k_{bc} := h(\phi(b_t, Z_2))$ $[= k_{cb}]$
$h(\langle AC, mk\rangle) = AC_{hmac}$
TX = TX′
$\phi(a,\phi(c,\mathfrak{g})) = Z_2$
⟨PAN, TX, a⟩ is unique
uPIN = PIN onl
TX, accept

key agreement

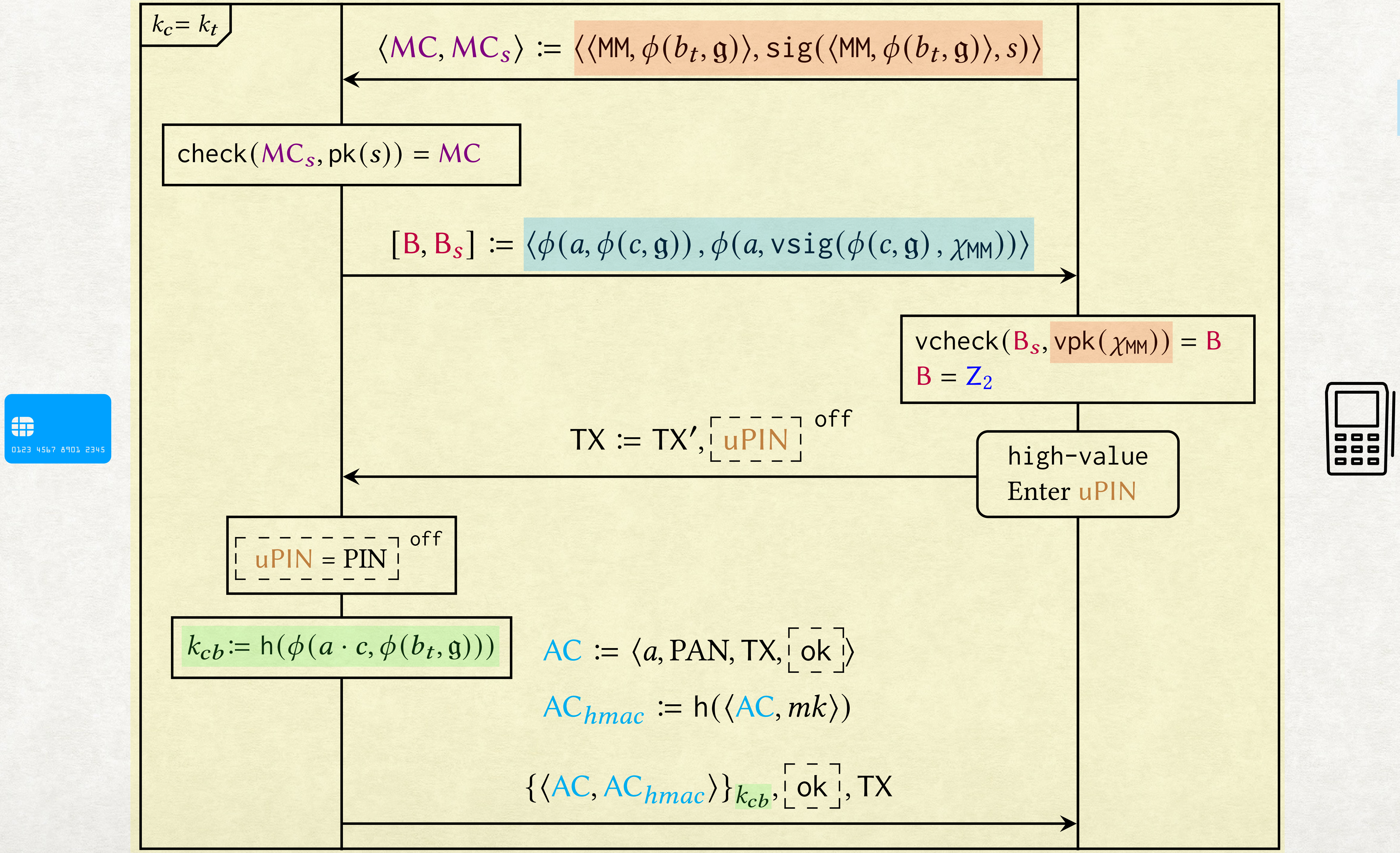
card's authentication

cryptogram generation

bank's processing

THE ESSENCE OF *UTX*

- Each month PaySys reveals the *signed bank's public key* + the validation key
- The card responds to the *current (or previous) month* by presenting the *month certificate*
- The card generates a *session key with the bank* and encrypts the card number PAN



$k_c = k_t$

$\langle \mathsf{MC}, \mathsf{MC}_s \rangle := \langle \langle \mathsf{MM}, \phi(b_t, \mathfrak{g}) \rangle, \mathsf{sig}(\langle \mathsf{MM}, \phi(b_t, \mathfrak{g}) \rangle, s) \rangle$

$\mathsf{check}(\mathsf{MC}_s, \mathsf{pk}(s)) = \mathsf{MC}$

$[\mathsf{B}, \mathsf{B}_s] := \langle \phi(a, \phi(c, \mathfrak{g})), \phi(a, \mathsf{vsig}(\phi(c, \mathfrak{g}), \chi_{\mathsf{MM}})) \rangle$

$\mathsf{vcheck}(\mathsf{B}_s, \mathsf{vpk}(\chi_{\mathsf{MM}})) = \mathsf{B}$
$\mathsf{B} = \mathsf{Z}_2$

$\mathsf{TX} := \mathsf{TX}', \boxed{\mathsf{uPIN}}^{\mathsf{off}}$

high-value
Enter uPIN

$\boxed{\mathsf{uPIN} = \mathsf{PIN}}^{\mathsf{off}}$

$k_{cb} := \mathsf{h}(\phi(a \cdot c, \phi(b_t, \mathfrak{g})))$

$\mathsf{AC} := \langle a, \mathsf{PAN}, \mathsf{TX}, \boxed{\mathsf{ok}} \rangle$

$\mathsf{AC}_{hmac} := \mathsf{h}(\langle \mathsf{AC}, mk \rangle)$

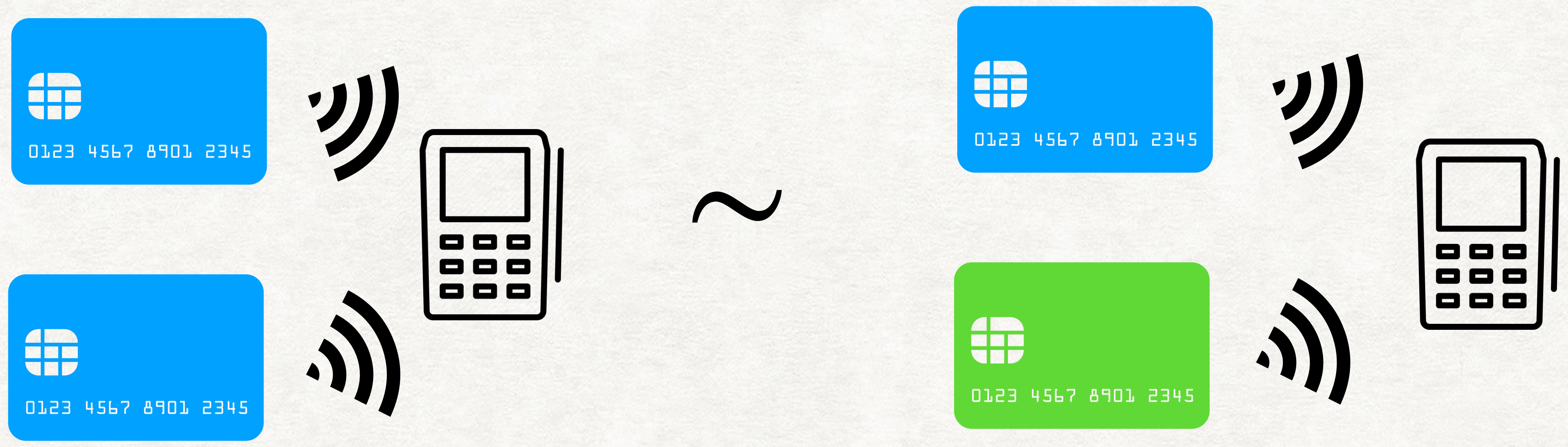
$\{\langle \mathsf{AC}, \mathsf{AC}_{hmac} \rangle\}_{k_{cb}}, \boxed{\mathsf{ok}}, \mathsf{TX}$

VERHEUL SIGNATURES

$$\mathtt{check}(\langle M, \mathtt{vsig}(M, s) \rangle, \mathtt{vpk}(s)) = \mathtt{OK}$$

$$\mathtt{check}(\langle \phi(a, M), \phi(a, \mathtt{vsig}(M, s)) \rangle, \mathtt{vpk}(s)) = \mathtt{OK}$$

UNLINKABILITY (DEFINITION)



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

A card can participate in many sessions.

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

A card can participate in at most one session.

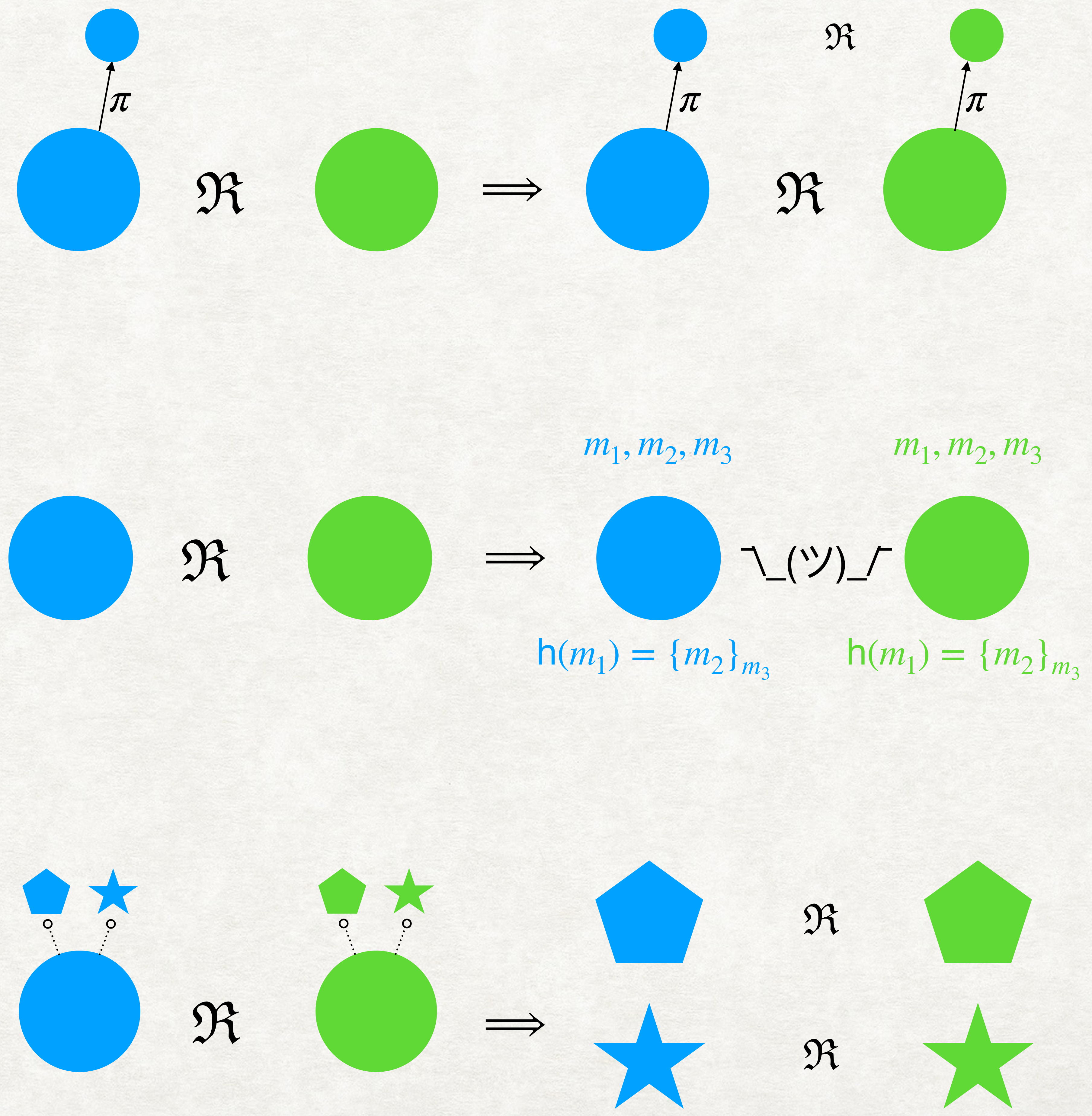
UNLINKABILITY (PROOF CERTIFICATE)

$$
\begin{array}{l}
(\vec{K}, F, A, \Gamma, B, \Lambda)_{\mathrm{impl}}(X, Y, Z) \triangleq \\
\quad \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}, \\
\quad a_{1\ldots E}, b_t, \ddot{ch}_{1\ldots F+G}, \dddot{ch}_{1\ldots F+M} \\
\quad t_{1\ldots L}, \mathsf{TX}_{1\ldots L}.(\ \theta \mid \\
\qquad C^1_1 \mid U^1_1 \mid DB^1_1 \mid \\
\qquad \ldots \\
\qquad C^1_{i_1} \mid U^1_{i_1} \mid DB^1_{i_1} \mid \\
\qquad \ldots \\
\qquad C^1_{D_1+K_1} \mid U^1_{D_1+K_1} \mid DB^1_{D_1+K_1} \mid \\
\qquad !(\nu ch.\overline{card}\langle ch\rangle. \\
\qquad\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 \\
\qquad\quad \overline{user}\langle \mathrm{PIN}_1\rangle \mid DB(si, \mathrm{PAN}_1, mk_1, \mathrm{PIN}_1)) \mid \\
\qquad \ldots \\
\qquad 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 \\
\qquad \ldots \\
\qquad C^h_{i_h} \mid U^h_{i_h} \mid DB^h_{i_h} \mid \\
\qquad \ldots \\
\qquad 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 \\
\qquad\quad DB^h_{D_{h-1}+K_{h-1}+D_h+K_h} \mid \\
\qquad !(\nu ch.\overline{card}\langle ch\rangle. \\
\qquad\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 \\
\qquad\quad \overline{user}\langle \mathrm{PIN}_h\rangle \mid DB(si, \mathrm{PAN}_h, mk_h, \mathrm{PIN}_h)) \mid \\
\qquad \ldots \\
\qquad 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 \\
\qquad \ldots \\
\qquad C^H_{i_H} \mid U^H_{i_H} \mid DB^H_{i_H} \mid \\
\qquad \ldots \\
\qquad 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 \\
\qquad\quad DB^H_{D_{H-1}+K_{H-1}+D_H+K_H} \mid \\
\qquad !(\nu ch.\overline{card}\langle ch\rangle. \\
\qquad\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 \\
\qquad\quad \overline{user}\langle \mathrm{PIN}_H\rangle \mid DB(si, \mathrm{PAN}_H, mk_H, \mathrm{PIN}_H)) \mid \\
\qquad !PC_{\mathrm{impl}} \mid \\
\qquad B^\theta_1 \mid T^\theta_1 \mid \\
\qquad \ldots \mid \\
\qquad B^\theta_j \mid T^\theta_j \mid \\
\qquad \ldots \mid \\
\qquad B^\theta_{F+G+M} \mid T^\theta_{F+G+M} \mid !PBT)
\end{array}
$$

$$\mathfrak{R}$$

$$
\begin{array}{l}
(K, F, A, \Gamma, B)_{\mathrm{spec}}(X, Y, Z) \triangleq \\
\quad \nu\,\vec{\epsilon}, \mathrm{PIN}_{1\ldots D+K}, mk_{1\ldots D+K}, c_{1\ldots D+K}, \mathrm{PAN}_{1\ldots D+K}, \\
\quad \dot{ch}_{1\ldots D}, a_{1\ldots E}, b_t, \ddot{ch}_{1\ldots F+G}, \\
\quad \dddot{ch}_{1\ldots F+M}, t_{1\ldots L}, \mathsf{TX}_{1\ldots L}.(\ \sigma \mid \\
\qquad C_1 \mid \ldots \mid 0 \mid !\overline{user}\langle \mathrm{PIN}_1\rangle \mid \\
\qquad\quad \ldots \mid 0 \mid !\overline{\langle si, \mathrm{PAN}_1\rangle}\langle\langle \mathrm{PIN}_1, mk_1, \phi(c_1, \mathfrak{g})\rangle\rangle) \mid \\
\qquad \ldots \\
\qquad C_i \mid \ldots \mid 0 \mid !\overline{user}\langle \mathrm{PIN}_i\rangle \mid \\
\qquad\quad \ldots \mid 0 \mid !\overline{\langle si, \mathrm{PAN}_i\rangle}\langle\langle \mathrm{PIN}_i, mk_i, \phi(c_i, \mathfrak{g})\rangle\rangle) \mid \\
\qquad \ldots \\
\qquad C_{D+K} \mid \ldots \mid 0 \mid !\overline{user}\langle \mathrm{PIN}_{D+K}\rangle \mid \\
\qquad\quad \ldots \mid 0 \mid !\overline{\langle si, \mathrm{PAN}_{D+K}\rangle}\langle\langle \mathrm{PIN}_{D+K}, mk_{D+K}, \phi(c_{D+K}, \mathfrak{g})\rangle\rangle) \mid \\
\qquad !PC_{\mathrm{spec}} \mid \\
\qquad B^\sigma_1 \mid T^\sigma_1 \mid \\
\qquad \ldots \mid \\
\qquad B^\sigma_j \mid T^\sigma_j \mid \\
\qquad \ldots \mid \\
\qquad B^\sigma_{F+G+M} \mid T^\sigma_{F+G+M} \mid !PBT)
\end{array}
$$

$\mathfrak{R}$ is a quasi-open bisimulation:



CONCLUSION

- **Privacy-preserving smart card payments are feasible**
    - *UTX* is unlinkable in the presence of active attackers
    - *UTX* respects the essential security guarantees card payments provide
    - *UTX* requires only a software update to the current payment infrastructure
    - *UTX* can coexist with traditional card payments
- **It is feasible to prove bisimilarity-based properties of complex protocols**