Security Analysis of Relay Contactless Payments

Ioana Boureanu[1], Tom Chothia[2], **Alexandre Debant[3]**, Stéphanie Delaune[3]

[1] University of Surrey
[2] University of Birmingham
[3] Univ Rennes, CNRS, IRISA

CCS 2020
November 11th 2020

Payments protocols

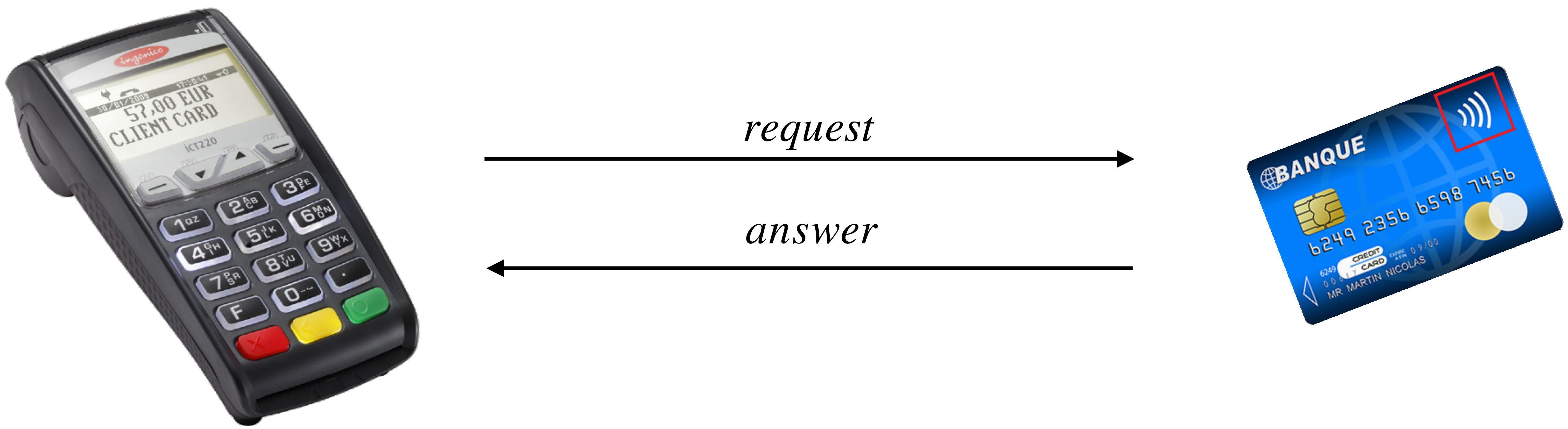
Historically:
Contact-based payments

- ✓ Well understood security
- ✗ time consumption
- ✗ contamination risks

Since the 2000s
Contact-less payments

- ✓ Easier to use
- ✗ Larger surface of attack

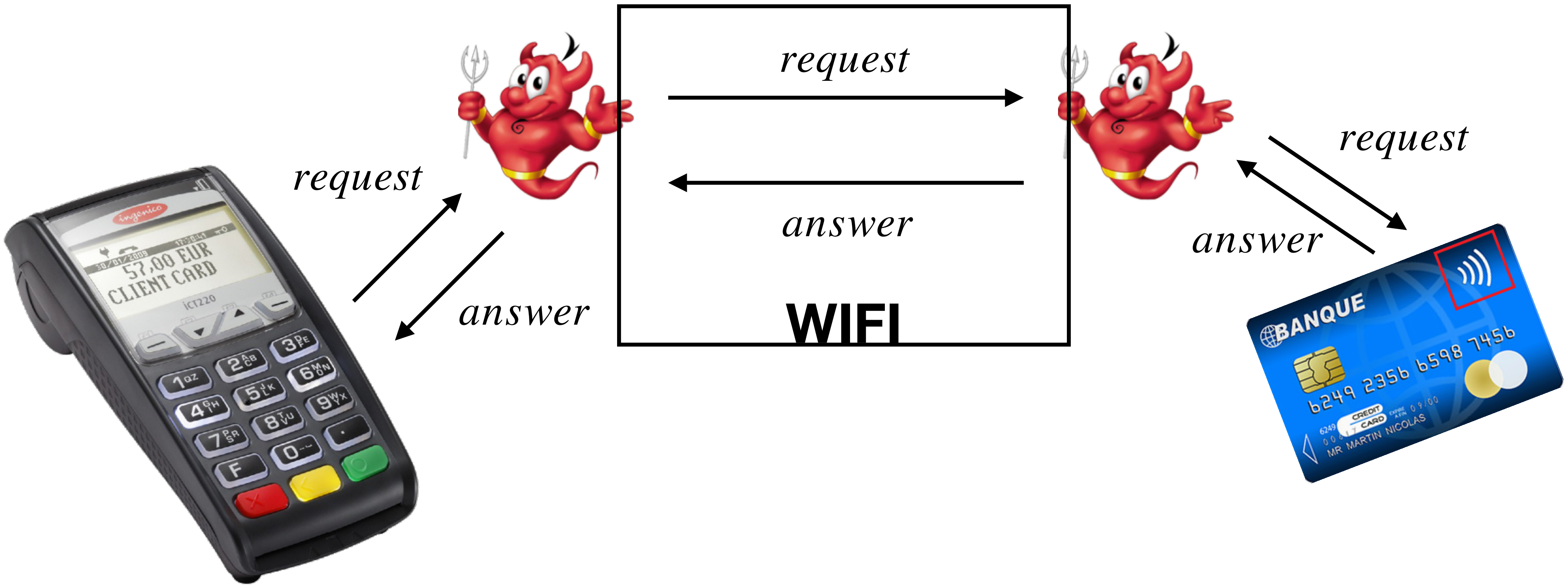
Contactless payments



Security features

- certificates and cryptographic material provided by the banks
- physical proximity ensured by NFC use
- amount limit

Contactless payments

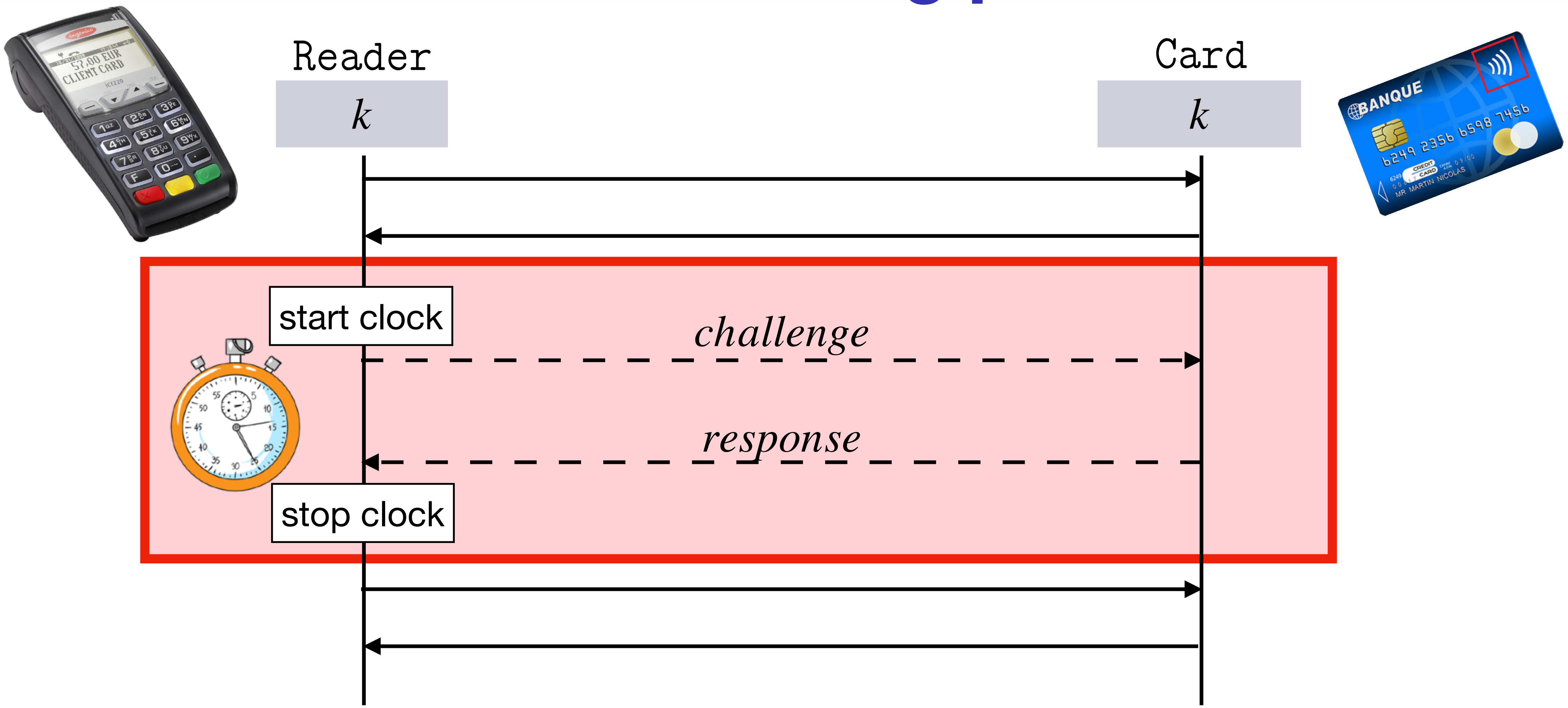


Security features

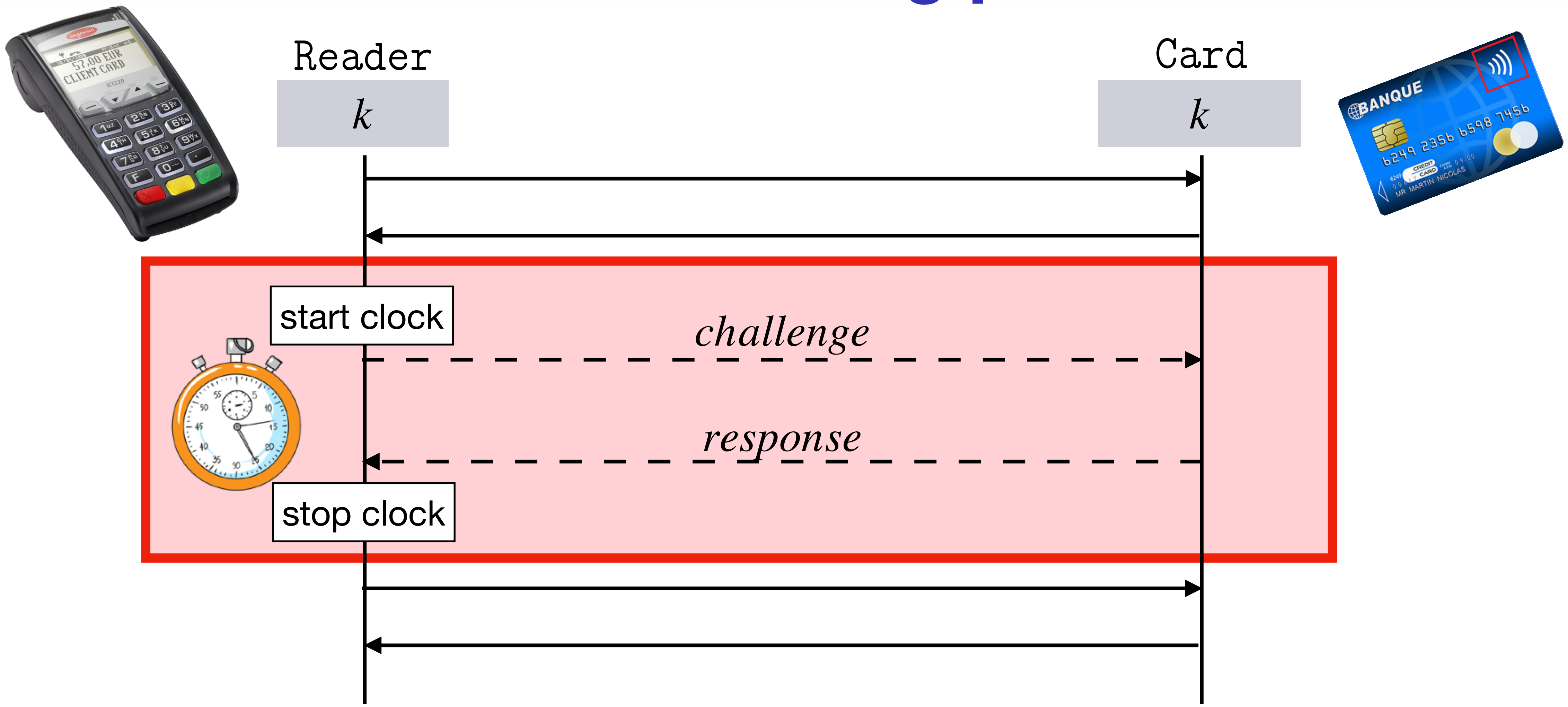
- certificates and cryptographic material provided by the banks ✓
- ~~physical proximity ensured by NFC use~~ **Can easily be overcome (e.g. [FC15])**
- ~~amount limit~~ **Continuously increased...**

Distance-bounding protocols have been proposed!

Distance-bounding protocols



Distance-bounding protocols



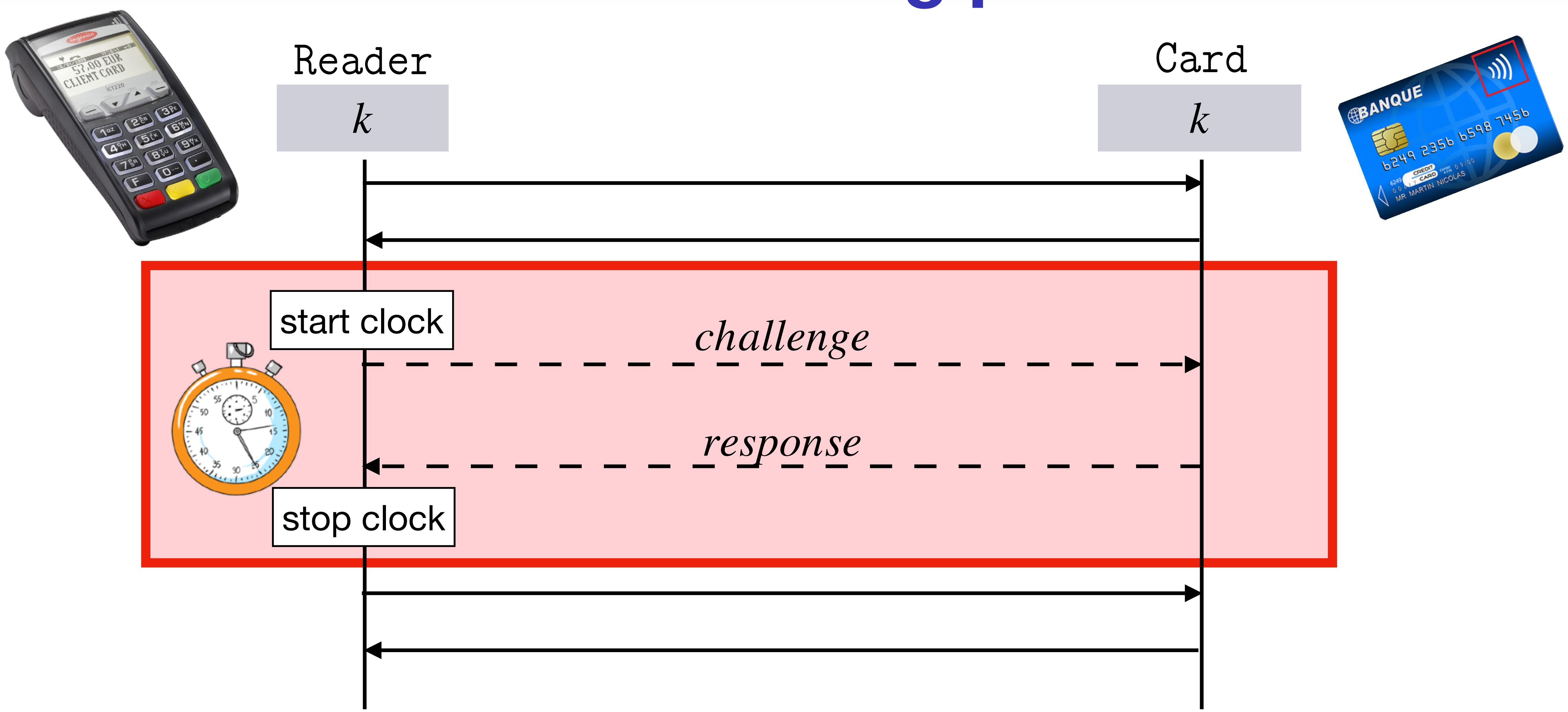
Formal verification:

- computational models: Avoine *et. al.* 2011, Dürholz *et. al.* 2011…
- Symbolic models: Chothia *et.al.* 2018, Mauw *et. al*. 2018, Debant *et. al.* 2018

A common assumption

The reader is honest!
He generates the timestamps and performs the time check

Distance-bounding protocols



Formal verification:

- computational models: Avoine *et. al.* 2011, Dürholz *et. al* 2011…
- Symbolic models: Chothia *et.al.* 2018, Mauw *et* … Debant *et. al.* 2018

A commo…

He gener… …performs the time check

This assumption is too strong!

Contributions

1. A symbolic model with malicious readers, TPM and mobility

2. An equivalent causality-based property

3. A comprehensive analysis of two novel EMV protocols

Contributions

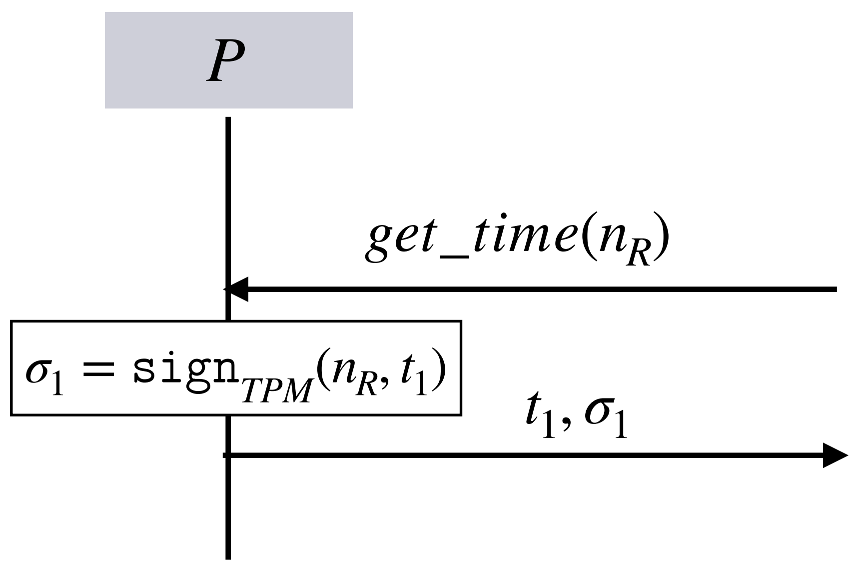
1. A symbolic model with malicious readers, TPM and mobility
2. An equivalent causality-based property
3. A comprehensive analysis of two novel EMV protocols

Protocol description

An extension of the Applied-Pi calculus:

- messages are terms:
  - atoms: private/public names + non-negative real numbers
  - function symbols: enc, dec, sign, checksign, sk, pk, ...
- roles are processes: $\mathtt{out}(u)$, $\mathtt{in}(x)$, $\mathtt{new}\ n$, $\mathtt{let}\ x = u\ \mathtt{in}\ P\ \mathtt{else}\ Q$
  + get_time(x)

$$
\begin{aligned}
P(z_0) :=&\\
&\mathtt{in}(x).\\
&\mathtt{get\_time}(y).\\
&\mathtt{let}\ \sigma_1 = \mathtt{sign}(\langle x, y\rangle, \mathtt{sk}(z_0))\ \mathtt{in}\\
&\mathtt{out}(\langle y, \sigma_1\rangle).\\
&0
\end{aligned}
$$



Semantics

An operational semantics that manipulates configurations

Novelty compared to the usual/untimed semantics:

- configurations include the global time
- the *TIM* rule let the time elapse/increase
- a physical constraints for inputs: enough time must have elapsed to let the inputted message reach its destination

Locations and agent positions:

- locations: $l_1, l_2, \ldots \in \mathbb{R}^3$ with the usual distance $\mathtt{Dist}(l_1, l_2) = \|l_1 - l_2\|$
- agent positions: defined by $\mathtt{Loc} : \mathscr{A} \times \mathbb{R}_+ \to \mathbb{R}^3$
- **Attention:** agents should not move faster than messages, i.e.:

$$\mathtt{Dist}(\mathtt{Loc}(a, t_1), \mathtt{Loc}(a, t_2)) \leq c \times (t_2 - t_1)$$

with c the communication speed

Security property: DB-security

DB-security

A protocol $\mathscr{P}$ is DB-secure if for all mobility plan $\mathtt{Loc}$, all valid initial configuration $\mathscr{K}_0$, and all execution

$$\mathtt{exec} = \mathscr{K}_0 \xrightarrow{(a_1,\ t_1,\ \mathtt{act}_1).\dots.(a_n,\ t_n,\ \mathtt{act}_n).(b_0,\ t,\ \mathtt{claim}(b_1,b_2,t_1^0,t_2^0))}_{\mathtt{Loc}} \mathscr{K}$$

we have that:

- either b_1 or b_2 are malicious
- or there exists $k \leq n$ such that $\mathtt{act}_k = \mathtt{check}(t_1^0, t_2^0, t_3^0)$ and

$$c \times (t_2^0 - t_1^0) \geq \mathtt{Dist}(\mathtt{Loc}(b_1, t_1^0), \mathtt{Loc}(b_2, t)) + \mathtt{Dist}(\mathtt{Loc}(b_2, t), \mathtt{Loc}(b_1, t_2^0))$$

for some $t_1^0 \leq t \leq t_2^0$.

Informally: if b_1 and b_2 are honest, **they have been close** between the two timestamps.

Existing verification tools: Proverif, Tamarin…

They cannot verify properties relying on time

Contributions

1. A symbolic model with malicious readers, TPM and mobility

2. **An equivalent causality-based property**

3. A comprehensive analysis of two novel EMV protocols

Causality-based security

(extending [Mauw *et al.*, 2018])

Causality-based security

A protocol $\mathscr{P}$ is causality-based secure if for all valid initial configuration $\mathscr{K}_0$ and all execution

$$\texttt{exec} = \mathscr{K}_0 \xrightarrow{(a_1,\, \texttt{act}_1).\ldots.(a_n,\, \texttt{act}_n).(b_0,\, \texttt{claim}(b_1, b_2, c_1, c_2))} \mathscr{K}$$

we have that:

- either $b_1 \in \mathscr{M}$ or $b_2 \in \mathscr{M}$
- or there exists $i, j, k, k' \leq n$ with $i \leq k' \leq j$ and such that:
  - $\texttt{act}_k = \texttt{check}(c_1, c_2, u)$;
  - $(a_i, \texttt{act}_i) = (b_1, \texttt{timestamp}(c_1))$ and $(a_j, \texttt{act}_j) = (b_1, \texttt{timestamp}(c_2))$ and $a_{k'} = b_2$

Theorem

Given a protocol $\mathscr{P}$, we have that:

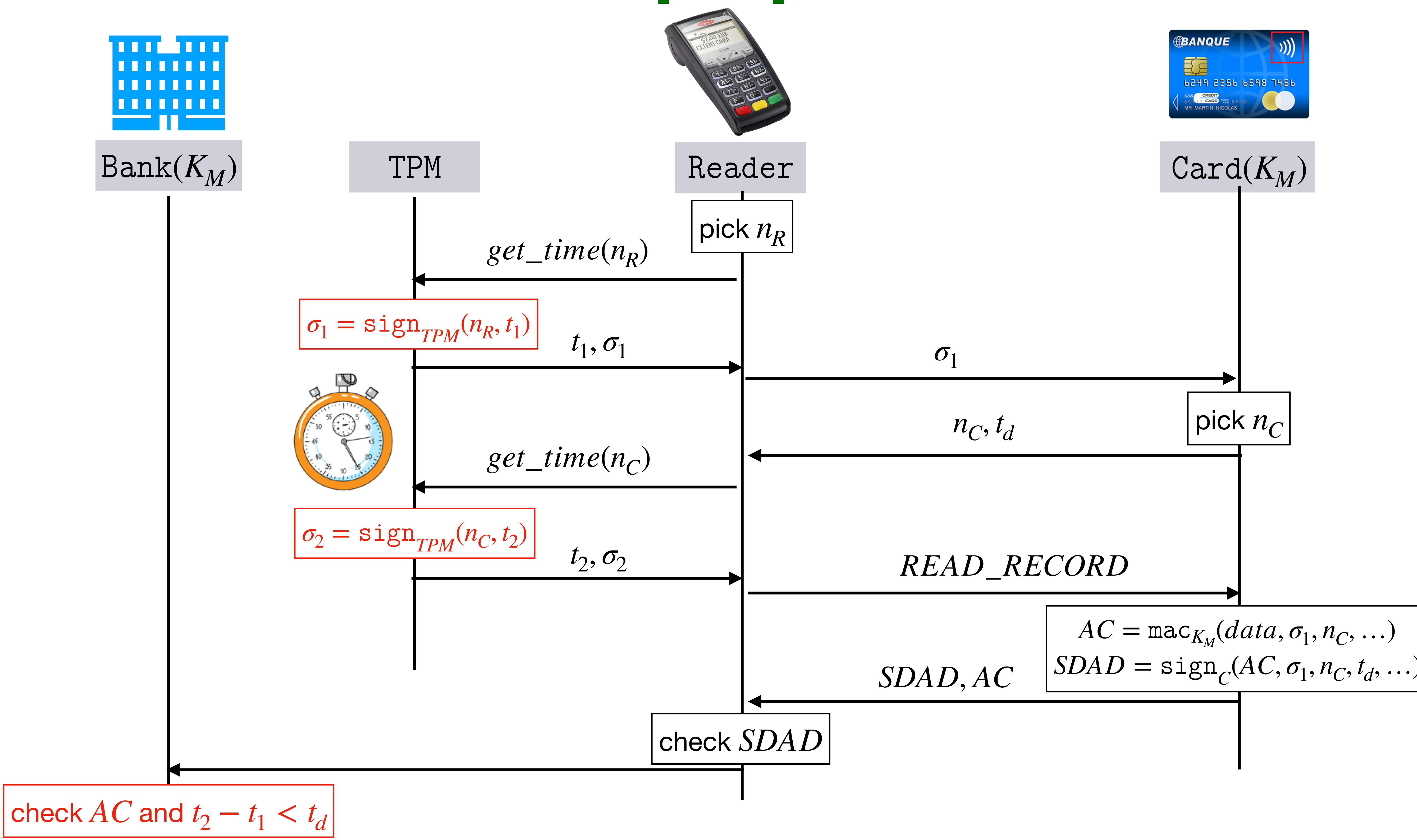
$\mathscr{P}$ is DB-secure $\Leftrightarrow$ $\mathscr{P}$ is causality-based secure

Contributions

1. A symbolic model with malicious readers, TPM and mobility
2. An equivalent causality-based property
3. **A comprehensive analysis of two novel EMV protocols**

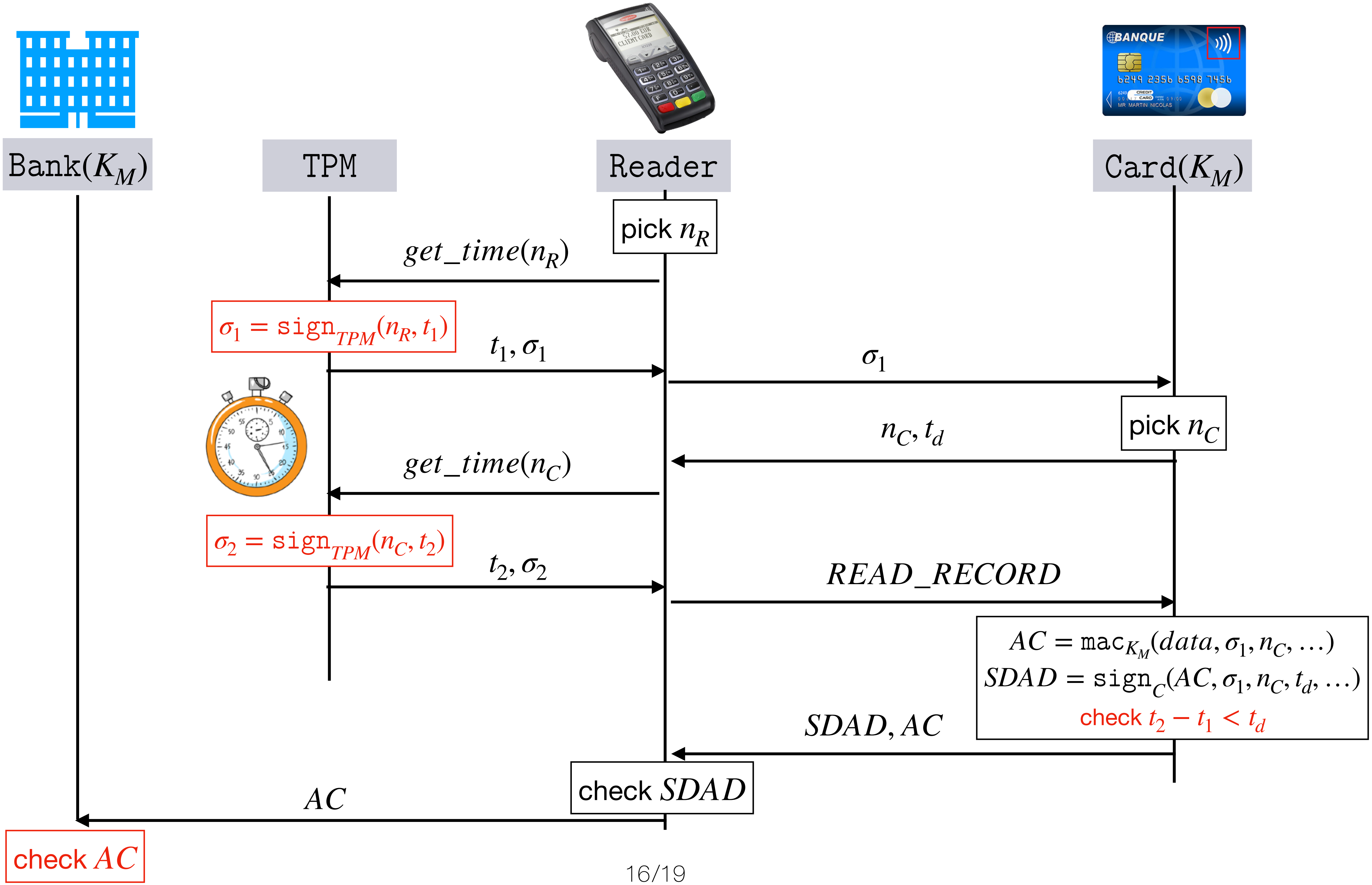
PayBCR protocol

[FC19]



PayCCR protocol

[FC19]



Case studies

Scenario under study

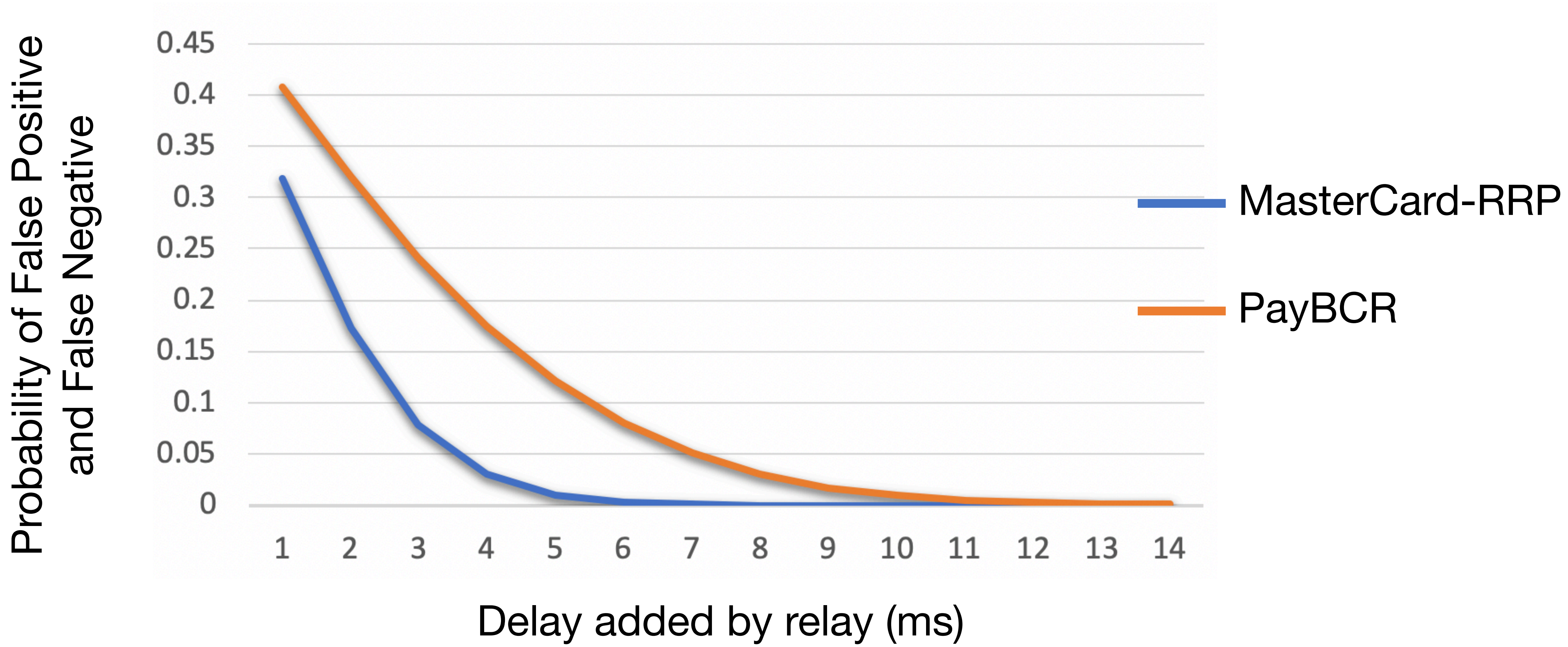
- unbounded number of banks that can certify an unbounded number of honest/dishonest cards and TPMs
- we do not model readers since they are assumed dishonest
- an identity cannot be certified as both card and TPM

The always authenticates a TPM and a card

The attacker cannot modify the time-bound

Protocol	Role authentication	Time-bound authentication	Causality-based security
PayCCR	✗	✓	✓
PayBCR	✓	✓	✓

Implementation of PayBCR



Results

- MasterCard-RRP detects relays of 5ms.
- PayBCR detects relays of 10ms.

Both are practical to stop relays using smartphones (~30ms)

Contributions

1. A symbolic model with malicious readers, TPM and mobility
2. An equivalent causality-based property
3. A comprehensive analysis of two novel EMV protocols

$\Rightarrow$ we can hope that these protocols will be used by EMVCo