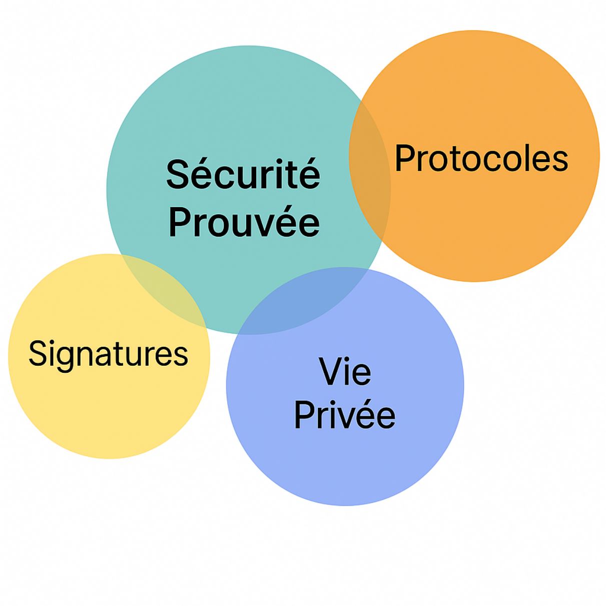
Who Pays Whom? Anonymous EMV-Compliant Contactless Payments

Charles Olivier-Anclin

LIMOS, université Clermont Auvergne

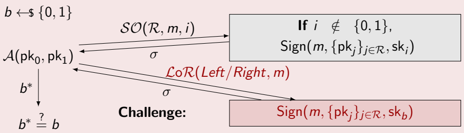
Seminaire équipe MC3 - laboratoire i3S


Sécurité Prouvée
Protocoles
Signatures
Vie Privée

Fields of Contribution

Signature Schemes with Anonymous Properties

Anonymity of Linkable Ring Signatures



$b \leftarrow_{\$} \{0,1\}$

$\mathcal{SO}(\mathcal{R}, m, i)$

If $i \notin \{0,1\}$, $\mathsf{Sign}(m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, \mathsf{sk}_i)$

σ

$\mathcal{A}(\mathsf{pk}_0, \mathsf{pk}_1)$

$\mathcal{LoR}(Left/Right, m)$

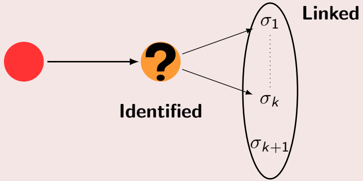
b^*

σ

Challenge: $\mathsf{Sign}(m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, \mathsf{sk}_b)$

$b^* \stackrel{?}{=} b$

k-Times Anonymity for Delegated Signatures



Linked

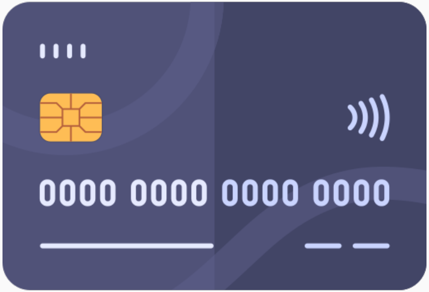
σ_1

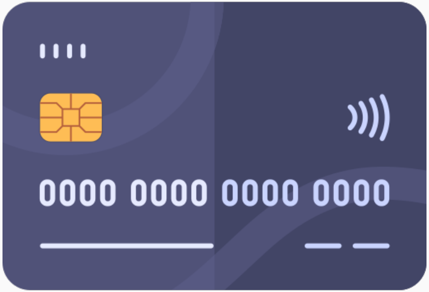
σ_k

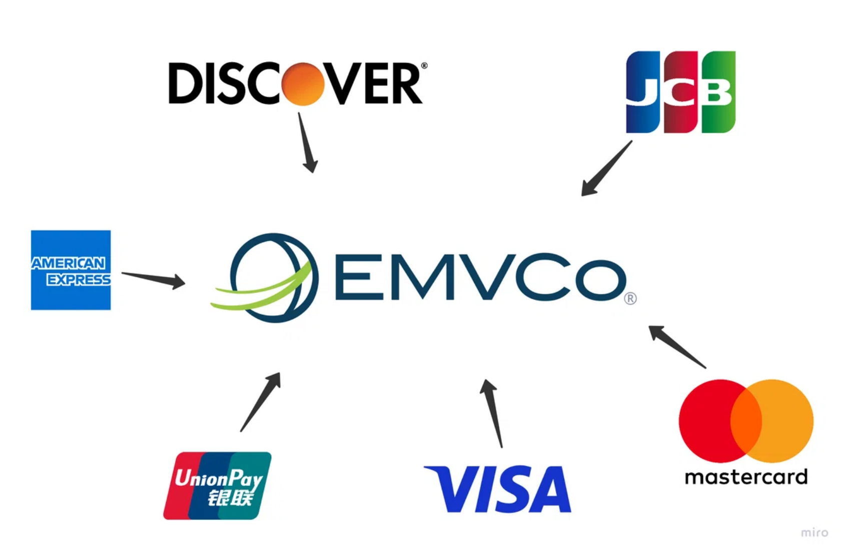
σ_{k+1}

Identified

Privacy Protection in EMV Payments protocol


0000 0000 0000 0000

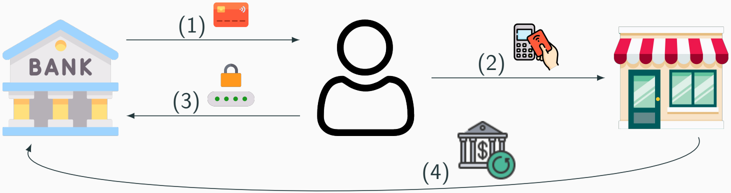

0000 0000 0000 0000



DISCOVER
JCB
AMERICAN EXPRESS
EMVCo
UnionPay 银联
VISA
mastercard
miro

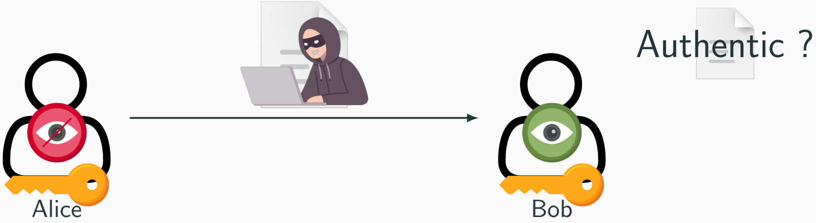
Card payments

Card payment processing:



A Little Cryptographic Background

Signature

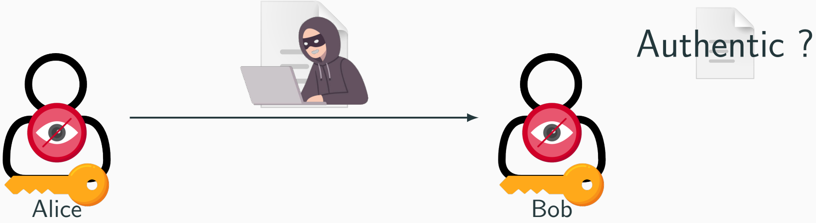


Alice

Bob

Authentic ?

MAC



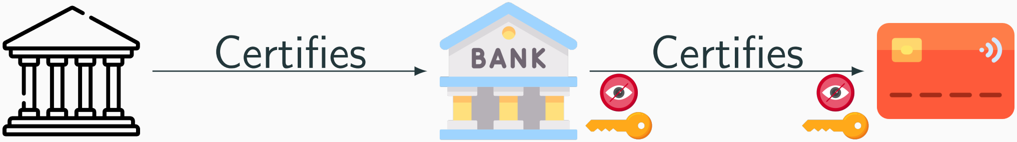
Alice

Bob

Authentic ?

Cryptography in EMV Payment Protocol

Card issuance

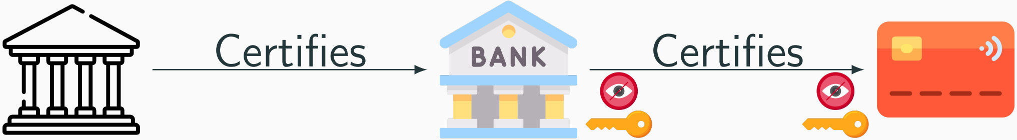


Certifies

Certifies

Cryptography in EMV Payment Protocol

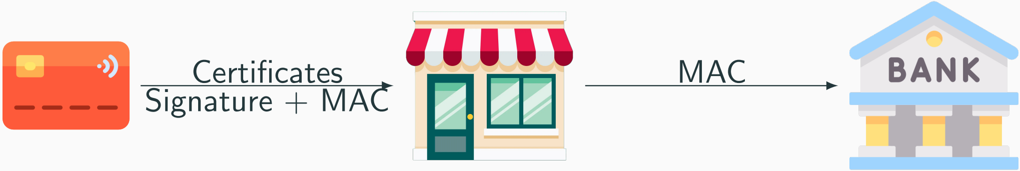
Card issuance



Certifies

Certifies

Payment



Certificates

Signature + MAC

MAC

Cryptography in EMV Payment Protocol

Card issuance

C

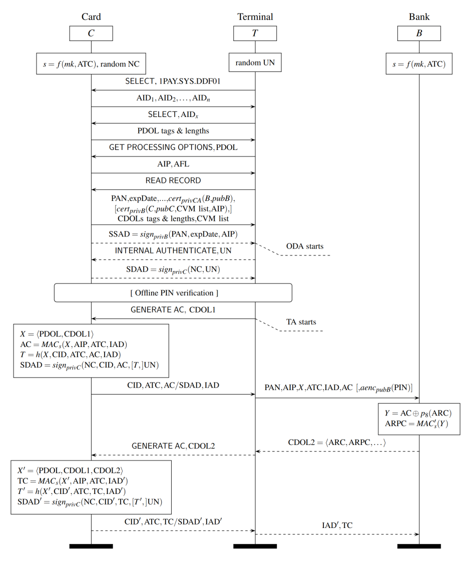
rtifies

Payment

Cer

Signatu

AC



Card C | Terminal T | Bank B

$s = f(mk, \text{ATC})$, random NC

random UN

$s = f(mk, \text{ATC})$

SELECT, 1PAY.SYS.DDF01

$\text{AID}_1, \text{AID}_2, \ldots, \text{AID}_n$

SELECT, AID_x

PDOL tags & lengths

GET PROCESSING OPTIONS, PDOL

AIP, AFL

READ RECORD

PAN,expDate,...,$cert_{privCA}(B,pubB)$,
$[cert_{privB}(C,pubC,\text{CVM list,AIP}),]$
CDOLs tags & lengths,CVM list

$\text{SSAD} = sign_{privB}(\text{PAN, expDate, AIP})$

ODA starts

INTERNAL AUTHENTICATE, UN

$\text{SDAD} = sign_{privC}(\text{NC}, \text{UN})$

[Offline PIN verification]

GENERATE AC, CDOL1

TA starts

$X = \langle \text{PDOL}, \text{CDOL1} \rangle$
$\text{AC} = MAC_s(X, \text{AIP}, \text{ATC}, \text{IAD})$
$T = h(X, \text{CID}, \text{ATC}, \text{AC}, \text{IAD})$
$\text{SDAD} = sign_{privC}(\text{NC}, \text{CID}, \text{AC}, [T,]\text{UN})$

CID, ATC, AC/SDAD, IAD

PAN,AIP,X,ATC,IAD,AC $[,aenc_{pubB}(\text{PIN})]$

$Y = \text{AC} \oplus p_8(\text{ARC})$
$\text{ARPC} = MAC'_s(Y)$

$\text{CDOL2} = \langle \text{ARC}, \text{ARPC}, \ldots \rangle$

GENERATE AC, CDOL2

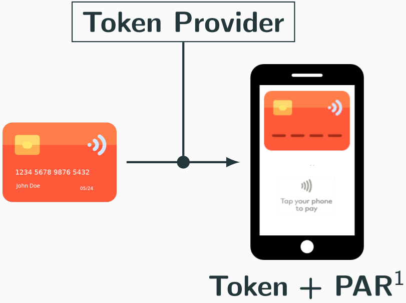
$X' = \langle \text{PDOL}, \text{CDOL1}, \text{CDOL2} \rangle$
$\text{TC} = MAC_s(X', \text{AIP}, \text{ATC}, \text{IAD}')$
$T' = h(X', \text{CID}', \text{ATC}, \text{TC}, \text{IAD}')$
$\text{SDAD}' = sign_{privC}(\text{NC}, \text{CID}', \text{TC}, [T',]\text{UN})$

CID$'$, ATC, TC/SDAD$'$, IAD$'$

IAD$'$, TC

Tokenisation

Generation of an alternative card number .



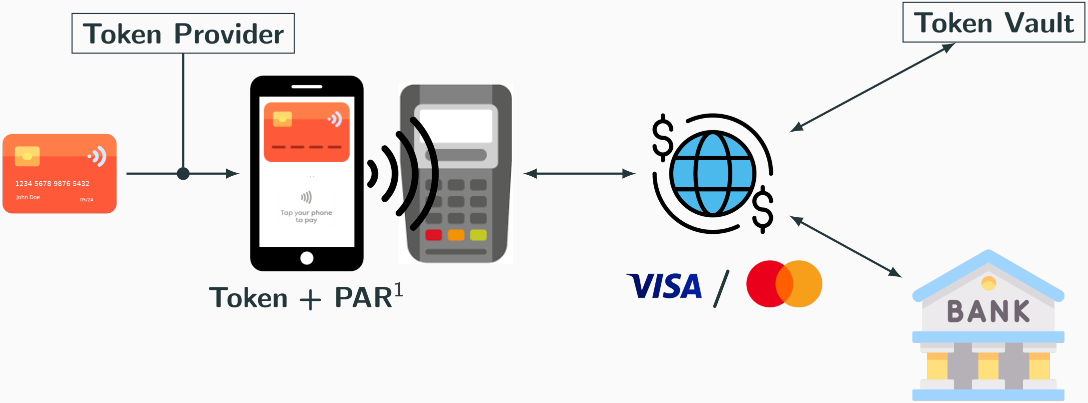
Token Provider

Token + PAR[1]

[1] (unique pour chaque carte) **P**ayment **A**ccount **R**eference

Tokenisation

Generation of an alternative card number & resolution of the modified transaction.



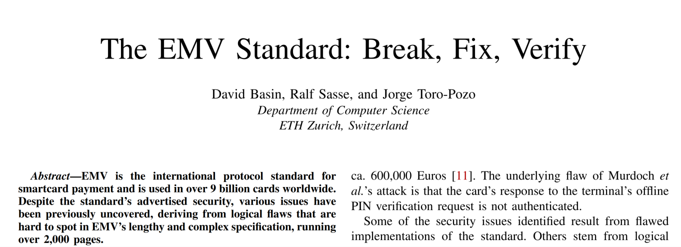
Token Provider

Token Vault

Token + PAR[1]

[1] (unique pour chaque carte) **P**ayment **A**ccount **R**eference

EMV (Security) is the Subject of Numerous Studies



The EMV Standard: Break, Fix, Verify

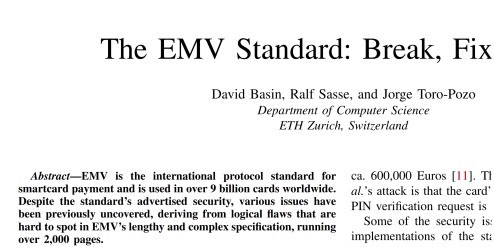
David Basin, Ralf Sasse, and Jorge Toro-Pozo
Department of Computer Science
ETH Zurich, Switzerland

***Abstract*—EMV is the international protocol standard for smartcard payment and is used in over 9 billion cards worldwide. Despite the standard's advertised security, various issues have been previously uncovered, deriving from logical flaws that are hard to spot in EMV's lengthy and complex specification, running over 2,000 pages.**

ca. 600,000 Euros [11]. The underlying flaw of Murdoch *et al.*'s attack is that the card's response to the terminal's offline PIN verification request is not authenticated.

Some of the security issues identified result from flawed implementations of the standard. Others stem from logical

EMV (Security) is the Subject of Numerous Studies

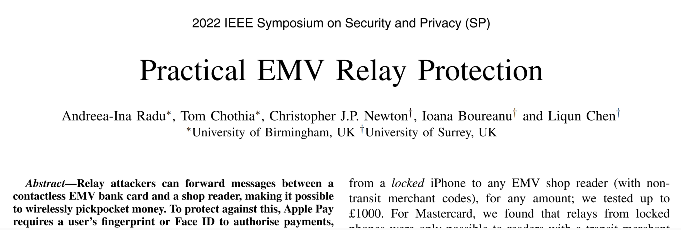


The EMV Standard: Break, Fix

David Basin, Ralf Sasse, and Jorge Toro-Pozo
Department of Computer Science
ETH Zurich, Switzerland

***Abstract*—EMV is the international protocol standard for smartcard payment and is used in over 9 billion cards worldwide. Despite the standard's advertised security, various issues have been previously uncovered, deriving from logical flaws that are hard to spot in EMV's lengthy and complex specification, running over 2,000 pages.**

ca. 600,000 Euros [11]. Th
al.'s attack is that the card'
PIN verification request is
Some of the security is
implementations of the sta



2022 IEEE Symposium on Security and Privacy (SP)

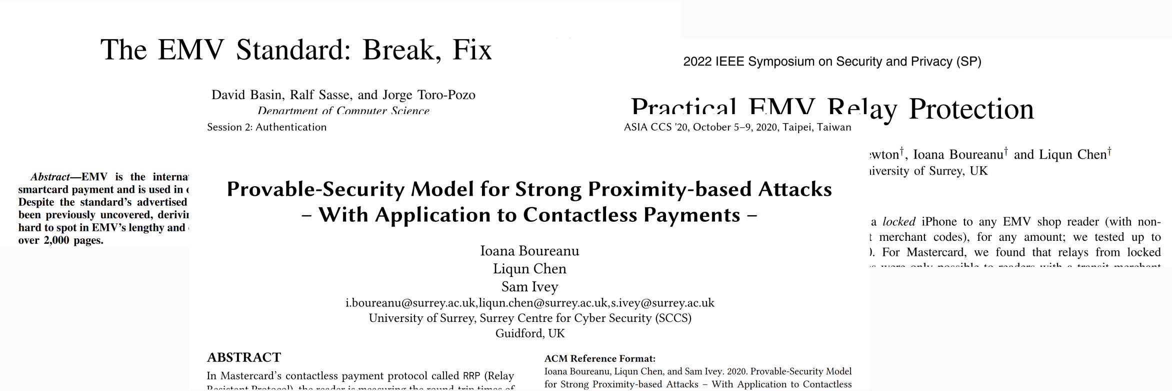
Practical EMV Relay Protection

Andreea-Ina Radu*, Tom Chothia*, Christopher J.P. Newton†, Ioana Boureanu† and Liqun Chen†
*University of Birmingham, UK †University of Surrey, UK

***Abstract*—Relay attackers can forward messages between a contactless EMV bank card and a shop reader, making it possible to wirelessly pickpocket money. To protect against this, Apple Pay requires a user's fingerprint or Face ID to authorise payments,**

from a *locked* iPhone to any EMV shop reader (with non-transit merchant codes), for any amount; we tested up to £1000. For Mastercard, we found that relays from locked

EMV (Security) is the Subject of Numerous Studies



The EMV Standard: Break, Fix

David Basin, Ralf Sasse, and Jorge Toro-Pozo
Department of Computer Science

Abstract—EMV is the interna
smartcard payment and is used in
Despite the standard's advertised
been previously uncovered, derivi
hard to spot in EMV's lengthy and
over 2,000 pages.

Session 2: Authentication

ASIA CCS '20, October 5–9, 2020, Taipei, Taiwan

Provable-Security Model for Strong Proximity-based Attacks – With Application to Contactless Payments –

Ioana Boureanu
Liqun Chen
Sam Ivey
i.boureanu@surrey.ac.uk,liqun.chen@surrey.ac.uk,s.ivey@surrey.ac.uk
University of Surrey, Surrey Centre for Cyber Security (SCCS)
Guidford, UK

ABSTRACT

In Mastercard's contactless payment protocol called RRP (Relay Resistant Protocol), the reader is measuring the round trip times of

ACM Reference Format:

Ioana Boureanu, Liqun Chen, and Sam Ivey. 2020. Provable-Security Model for Strong Proximity-based Attacks – With Application to Contactless

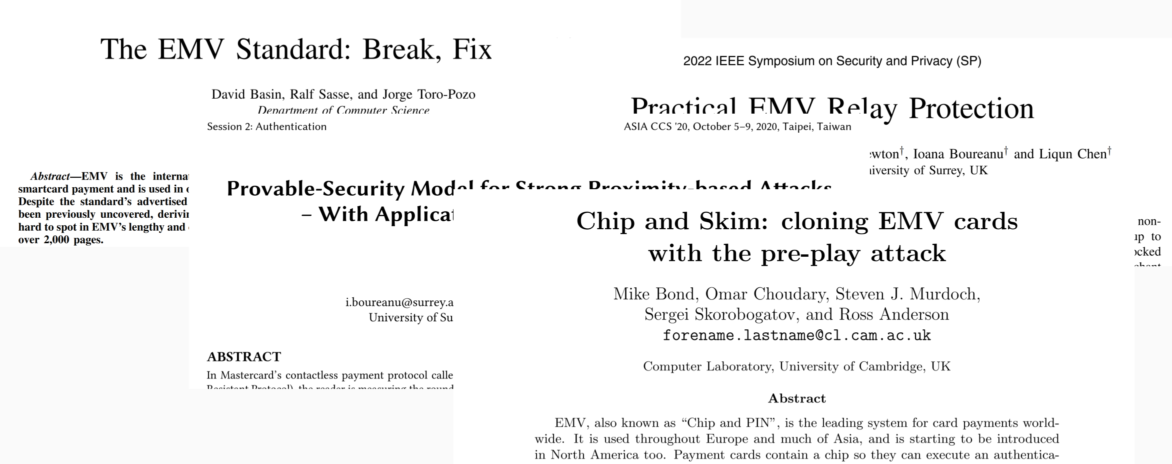
2022 IEEE Symposium on Security and Privacy (SP)

Practical EMV Relay Protection

wton[†], Ioana Boureanu[†] and Liqun Chen[†]
iversity of Surrey, UK

a *locked* iPhone to any EMV shop reader (with non-
t merchant codes), for any amount; we tested up to
). For Mastercard, we found that relays from locked
were only possible to readers with a transit merchant

EMV (Security) is the Subject of Numerous Studies



The EMV Standard: Break, Fix

David Basin, Ralf Sasse, and Jorge Toro-Pozo
Department of Computer Science

Abstract—EMV is the interna
smartcard payment and is used in
Despite the standard's advertised
been previously uncovered, derivi
hard to spot in EMV's lengthy and
over 2,000 pages.

2022 IEEE Symposium on Security and Privacy (SP)

Practical EMV Relay Protection

wton[†], Ioana Boureanu[†] and Liqun Chen[†]
iversity of Surrey, UK

non-
ıp to
ocked

Session 2: Authentication

ASIA CCS '20, October 5–9, 2020, Taipei, Taiwan

Provable-Security Model for Strong Proximity-based Attacks
– With Applica

i.boureanu@surrey.a
University of Su

ABSTRACT

In Mastercard's contactless payment protocol calle

Chip and Skim: cloning EMV cards with the pre-play attack

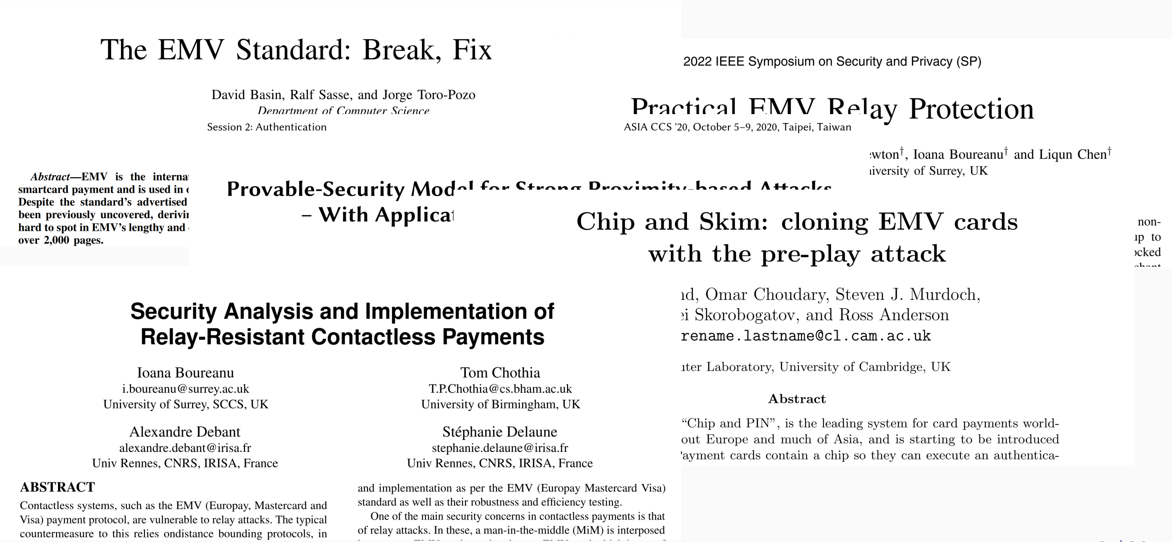
Mike Bond, Omar Choudary, Steven J. Murdoch,
Sergei Skorobogatov, and Ross Anderson
forename.lastname@cl.cam.ac.uk

Computer Laboratory, University of Cambridge, UK

Abstract

EMV, also known as "Chip and PIN", is the leading system for card payments worldwide. It is used throughout Europe and much of Asia, and is starting to be introduced in North America too. Payment cards contain a chip so they can execute an authentica-

EMV (Security) is the Subject of Numerous Studies



The EMV Standard: Break, Fix

David Basin, Ralf Sasse, and Jorge Toro-Pozo
Department of Computer Science

Abstract—EMV is the interna
smartcard payment and is used in
Despite the standard's advertised
been previously uncovered, derivi
hard to spot in EMV's lengthy and
over 2,000 pages.

2022 IEEE Symposium on Security and Privacy (SP)

Practical EMV Relay Protection

wton[†], Ioana Boureanu[†] and Liqun Chen[†]
iversity of Surrey, UK

non-
ip to
ocked

Session 2: Authentication

ASIA CCS '20, October 5–9, 2020, Taipei, Taiwan

Provable-Security Model for Strong Proximity-based Attacks
– With Applica

Chip and Skim: cloning EMV cards
with the pre-play attack

d, Omar Choudary, Steven J. Murdoch,
i Skorobogatov, and Ross Anderson
rename.lastname@cl.cam.ac.uk

ter Laboratory, University of Cambridge, UK

Abstract

"Chip and PIN", is the leading system for card payments world-
out Europe and much of Asia, and is starting to be introduced
ayment cards contain a chip so they can execute an authentica-

Security Analysis and Implementation of Relay-Resistant Contactless Payments

Ioana Boureanu
i.boureanu@surrey.ac.uk
University of Surrey, SCCS, UK

Tom Chothia
T.P.Chothia@cs.bham.ac.uk
University of Birmingham, UK

Alexandre Debant
alexandre.debant@irisa.fr
Univ Rennes, CNRS, IRISA, France

Stéphanie Delaune
stephanie.delaune@irisa.fr
Univ Rennes, CNRS, IRISA, France

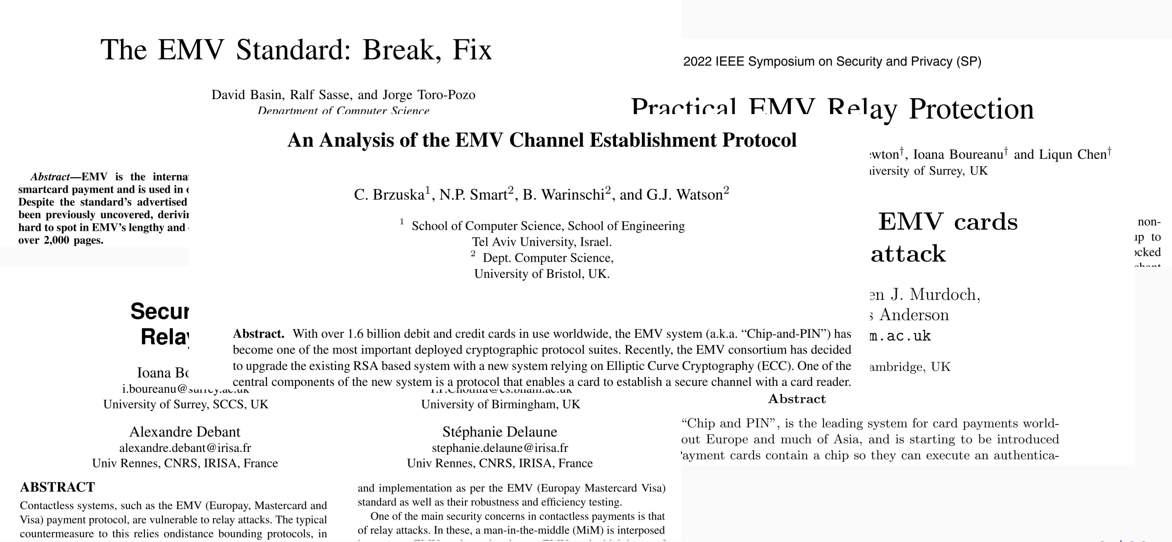
ABSTRACT

Contactless systems, such as the EMV (Europay, Mastercard and Visa) payment protocol, are vulnerable to relay attacks. The typical countermeasure to this relies ondistance bounding protocols, in

and implementation as per the EMV (Europay Mastercard Visa) standard as well as their robustness and efficiency testing.

One of the main security concerns in contactless payments is that of relay attacks. In these, a man-in-the-middle (MiM) is interposed

EMV (Security) is the Subject of Numerous Studies



The EMV Standard: Break, Fix

David Basin, Ralf Sasse, and Jorge Toro-Pozo
Department of Computer Science

Abstract—EMV is the interna
smartcard payment and is used in
Despite the standard's advertised
been previously uncovered, derivi
hard to spot in EMV's lengthy and
over 2,000 pages.

2022 IEEE Symposium on Security and Privacy (SP)

Practical EMV Relay Protection

wton[†], Ioana Boureanu[†] and Liqun Chen[†]
niversity of Surrey, UK

An Analysis of the EMV Channel Establishment Protocol

C. Brzuska[1], N.P. Smart[2], B. Warinschi[2], and G.J. Watson[2]

[1] School of Computer Science, School of Engineering
Tel Aviv University, Israel.
[2] Dept. Computer Science,
University of Bristol, UK.

Abstract. With over 1.6 billion debit and credit cards in use worldwide, the EMV system (a.k.a. "Chip-and-PIN") has become one of the most important deployed cryptographic protocol suites. Recently, the EMV consortium has decided to upgrade the existing RSA based system with a new system relying on Elliptic Curve Cryptography (ECC). One of the central components of the new system is a protocol that enables a card to establish a secure channel with a card reader.

EMV cards
attack

en J. Murdoch,
s Anderson
m.ac.uk

ambridge, UK

non-
up to
ocked

Abstract

"Chip and PIN", is the leading system for card payments world-
out Europe and much of Asia, and is starting to be introduced
ayment cards contain a chip so they can execute an authentica-

Secur
Rela

Ioana Bo
i.boureanu@surrey.ac.uk
University of Surrey, SCCS, UK

University of Birmingham, UK

Alexandre Debant
alexandre.debant@irisa.fr
Univ Rennes, CNRS, IRISA, France

Stéphanie Delaune
stephanie.delaune@irisa.fr
Univ Rennes, CNRS, IRISA, France

ABSTRACT

Contactless systems, such as the EMV (Europay, Mastercard and Visa) payment protocol, are vulnerable to relay attacks. The typical countermeasure to this relies ondistance bounding protocols, in

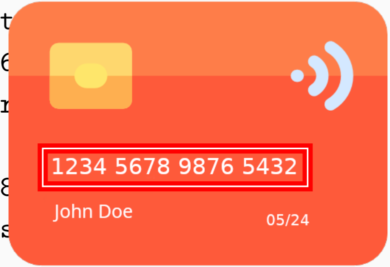
and implementation as per the EMV (Europay Mastercard Visa) standard as well as their robustness and efficiency testing.

One of the main security concerns in contactless payments is that of relay attacks. In these, a man-in-the-middle (MiM) is interposed

Payments Reveal Personal Data

```
  5A | len:8  Application Primary Account Number: 1234567898765432

5F24 | len:3  Application Expiration Date YYMMDD: 240430
5F25 | len:3  Application Effective Dat
5F28 | len:2  Issuer Country Code: 0826
9F02 | len:6  Amount, Authorised (Numer
       000000004600
9F1A | len:2  Terminal Country Code: 08
  95 | len:5  Terminal Verification Res
       0000008001
5F2A | len:2  Transaction Currency Code: 0826
  9A | len:3  Transaction Date: 210318
```



The Resale of Your Data

DATA COLLECTION LISTS
CHEAP!
SOC. SEC. NUMBERS
DRIVER'S LICENSE NUMBERS
HOME OWNERSHIP
INCOME
MARITAL STATUS
INTERNET HABITS
AUTO
FAMILY STATUS
MEDICAL HISTORY
BANK RECORDS
INSURANCE RECORDS
KIRK

FENCING STOLEN GOODS

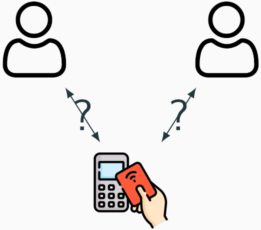
Expected properties

Payer Anonymity

An entity will not get to know a payee's long-term identity *ID* or a long-term pseudonym.

Payments' Unlinkability

An entity will stay unable to link payments made by the same payee.



Merchant Anonymity

An entity cannot not infer the identity of merchant involved in a payment.

Regulations

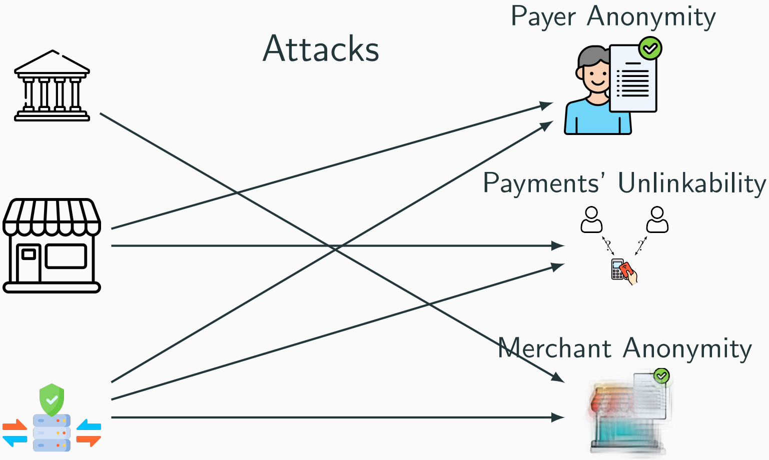
KYC: Know Your Customer

SCA: Strong Customer Authentication

AML: Anti-Money Laundering

Threat model

In general, all participants can be corrupted[2]. However,

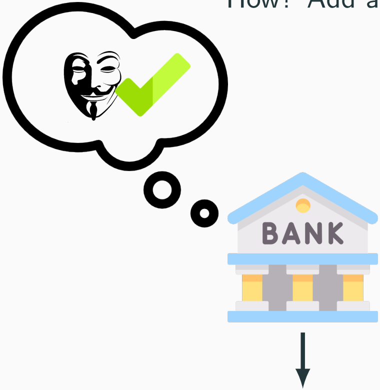


[2] We still need to prevent against trivial attacks.

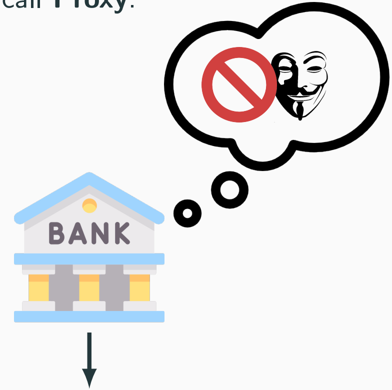
Can we bring (some) anonymity?

Short answer: yes ✓

How? Add an intermediary that we call **Proxy**.



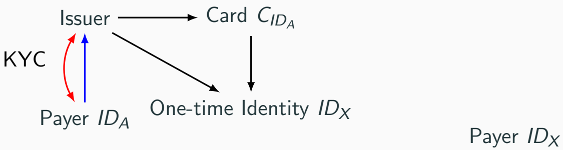
PrivBank



PrivProxy

PrivBank: privacy friendly bank

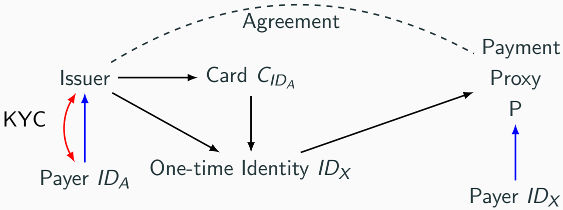
EMV-compliant payments with anonymity provisioned collaboratively by **privacy-friendly issuer and third-party proxy**.



⟶ Flow ⟶ Identity knowledge ⟶ Law requirements (SCA/KYC) ⟶ Clearing operations

PrivBank: privacy friendly bank

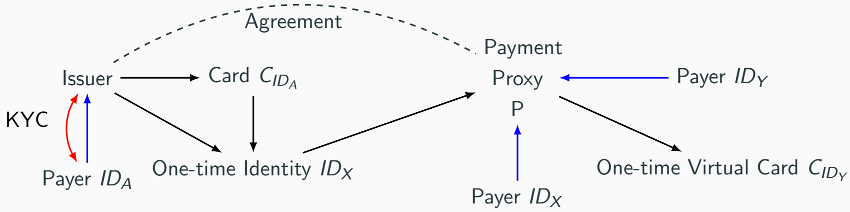
EMV-compliant payments with anonymity provisioned collaboratively by **privacy-friendly issuer and third-party proxy**.



⟶ Flow ⟶ Identity knowledge ⟶ Law requirements (SCA/KYC) ⟶ Clearing operations

PrivBank: **privacy friendly bank**

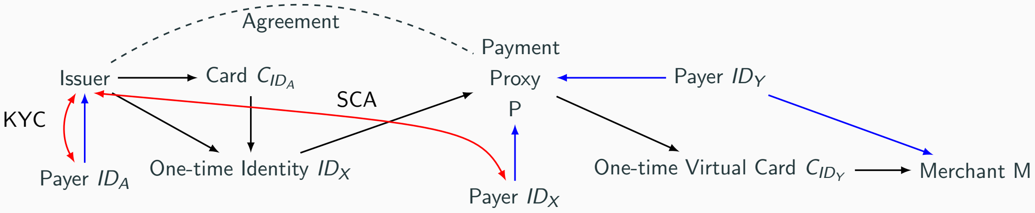
EMV-compliant payments with anonymity provisioned collaboratively by **privacy-friendly issuer and third-party proxy**.



⟶ Flow ⟶ Identity knowledge ⟶ Law requirements (SCA/KYC) ⟶ Clearing operations

PrivBank: privacy friendly bank

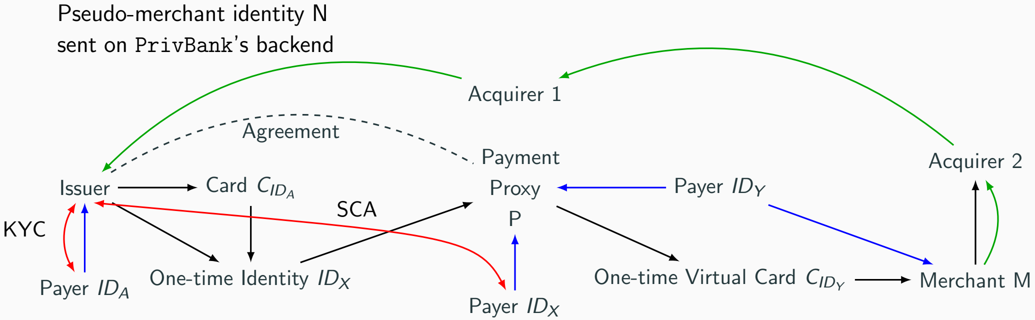
EMV-compliant payments with anonymity provisioned collaboratively by **privacy-friendly issuer and third-party proxy**.



⟶ Flow ⟶ Identity knowledge ⟶ Law requirements (SCA/KYC) ⟶ Clearing operations

PrivBank: privacy friendly bank

EMV-compliant payments with anonymity provisioned collaboratively by **privacy-friendly issuer and third-party proxy**.

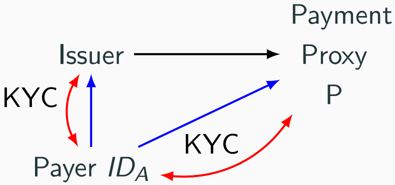


Pseudo-merchant identity N sent on PrivBank's backend

⟶ Flow ⟶ Identity knowledge ⟶ Law requirements (SCA/KYC) ⟶ Clearing operations

PrivProxy: privacy enabeling proxy

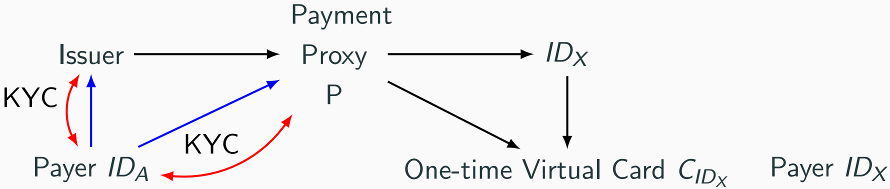
EMV-compliant payments with anonymity provisioned by **third-party proxy**.



$\longrightarrow$ Flow $\longrightarrow$ Identity knowledge $\longrightarrow$ Law requirements (SCA/KYC) $\longrightarrow$ Clearing operations

PrivProxy: privacy enabeling proxy

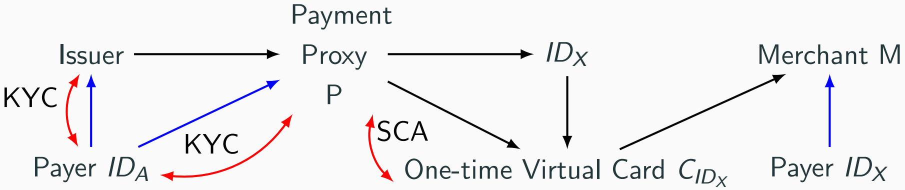
EMV-compliant payments with anonymity provisioned by **third-party proxy**.



⟶ Flow ⟶ Identity knowledge ⟶ Law requirements (SCA/KYC) ⟶ Clearing operations

PrivProxy: privacy enabeling proxy

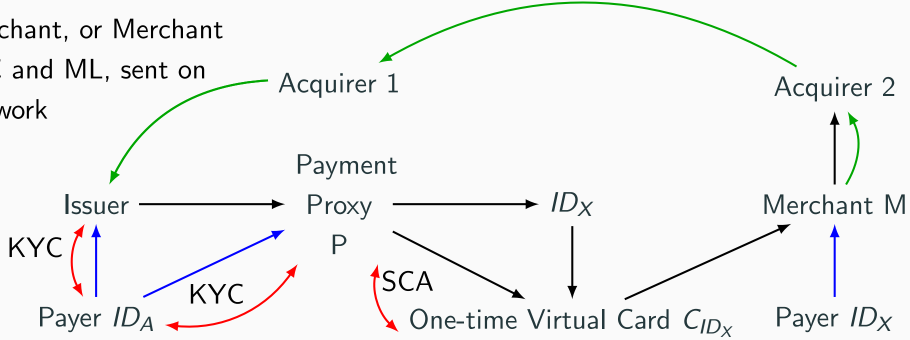
EMV-compliant payments with anonymity provisioned by **third-party proxy**.



⟶ Flow ⟶ Identity knowledge ⟶ Law requirements (SCA/KYC) ⟶ Clearing operations

PrivProxy: privacy enabeling proxy

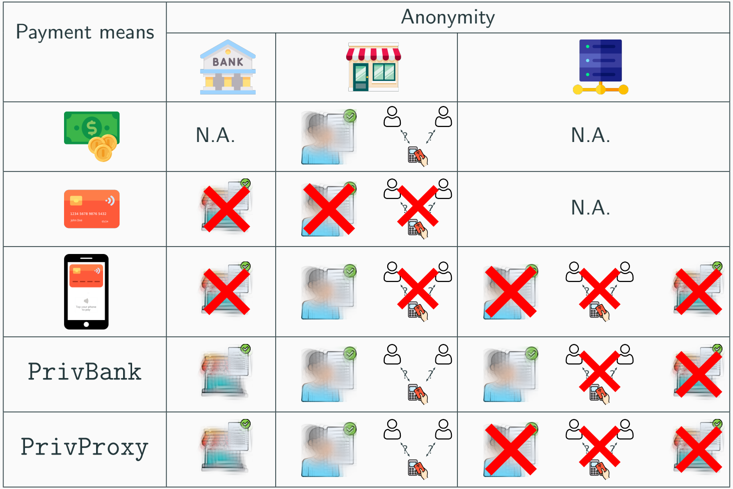
EMV-compliant payments with anonymity provisioned by **third-party proxy**.



P as Merchant, or Merchant *M*'s MCC and ML, sent on EMV network

⟶ Flow ⟶ Identity knowledge ⟶ Law requirements (SCA/KYC) ⟶ Clearing operations

Privacy Improvement Within EMV Payments



Payment means	Anonymity		
	BANK		
💵	N.A.	✓ ✓	N.A.
💳	✗	✗ ✗	N.A.
📱	✗	✓ ✗	✗ ✗ ✗
PrivBank	✓	✓ ✓	✓ ✗ ✗
PrivProxy	✓	✓ ✓	✗ ✗ ✗

Our security analysis

Unforgeability:

The payment authorisation/protocol remains unchanged.

Payer Anonymity

A payment pay has been made by a payer ID: $(\mathsf{ID}, \mathsf{pay}) \in \mathcal{R}_{\mathcal{P}\mathsf{Idt.}}$ if

$$\exists \lambda \in [\mathit{SetupID}(\mathsf{ID})], \exists C \in [\mathit{SetupPayment}(\mathsf{ID})],$$
$$\mathsf{pay} \in [\mathit{Payment}((\mathsf{ID}, C), M)]$$

Is $\mathcal{R}_{\mathcal{P}\mathsf{Idt.}}$ preimage resistant given a payment pay?

Payment's Unlinkability and **Merchant Anonymity** are **similarly defined**.

All our relation based properties also imply some game based defined properties.

Q.E.D. □

Paiement mobile anonyme

- ✓ **Norme compilant**
- ✓ **Law compilant**

Q.E.D. □

Paiement mobile anonyme

✓ **Norme compilant** ✓ **Law compilant**

“No one shall be subjected to arbitrary interference with his privacy [...] or correspondence [...]. Everyone has the right to the protection of the law against such [...] attacks.” **The Universal Declaration for Human Rights**