# About Machine Readable Travel Documents

## Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication

Jean Monnerat, **Serge Vaudenay**, Martin Vuagnoux

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

http://lasecwww.epfl.ch/

1. ICAO-MRTD
2. Non-Transferable Proofs

1. ICAO-MRTD
2. Non-Transferable Proofs

1. **ICAO-MRTD**
   - ICAO-MRTD Overview
   - Data Structures and PKI
   - MRTD Cryptography
   - Security and Privacy Issues

2. **Non-Transferable Proofs**

# Objectives

to enable inspecting authorities to securely identify visitors with the help of machine-readable digital information

- $\longrightarrow$ biometrics
- $\longrightarrow$ contactless IC chip
- $\longrightarrow$ digital signature + PKI

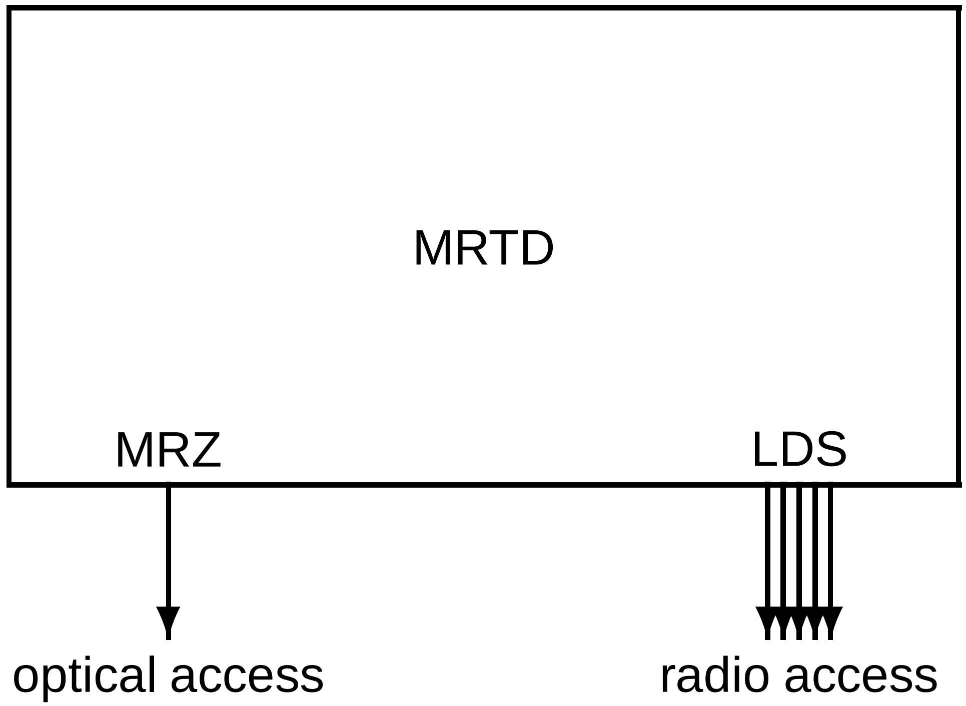
- maintained by UN/ICAO (International Civil Aviation Organization)

# MRTD History

- 1968: ICAO starts working on MRTD
- 1980: first standard (OCR-B Machine Readable Zone (MRZ))
- 1997: ICAO-NTWG (New Tech. WG) starts working on biometrics
- 2001 9/11: US want to speed up the process
- 2004: version 1.1 of standard with ICC
- 2006: extended access control under development in the EU

# How to Distinguish a Compliant MRTD

# MRTD in a Nutshell




- data authentication by digital signature + PKI
  aka **passive authentication**
- access control + key agreement based on MRZ_info
  aka **basic access control (BAC)**
- chip authentication by public-key cryptgraphy
  aka **active authentication (AA)**

# MRZ Example

- document type
- issuing country
- holder name
- doc. number + CRC
- nationality
- date of birth + CRC
- gender
- date of expiry + CRC
- options + CRC

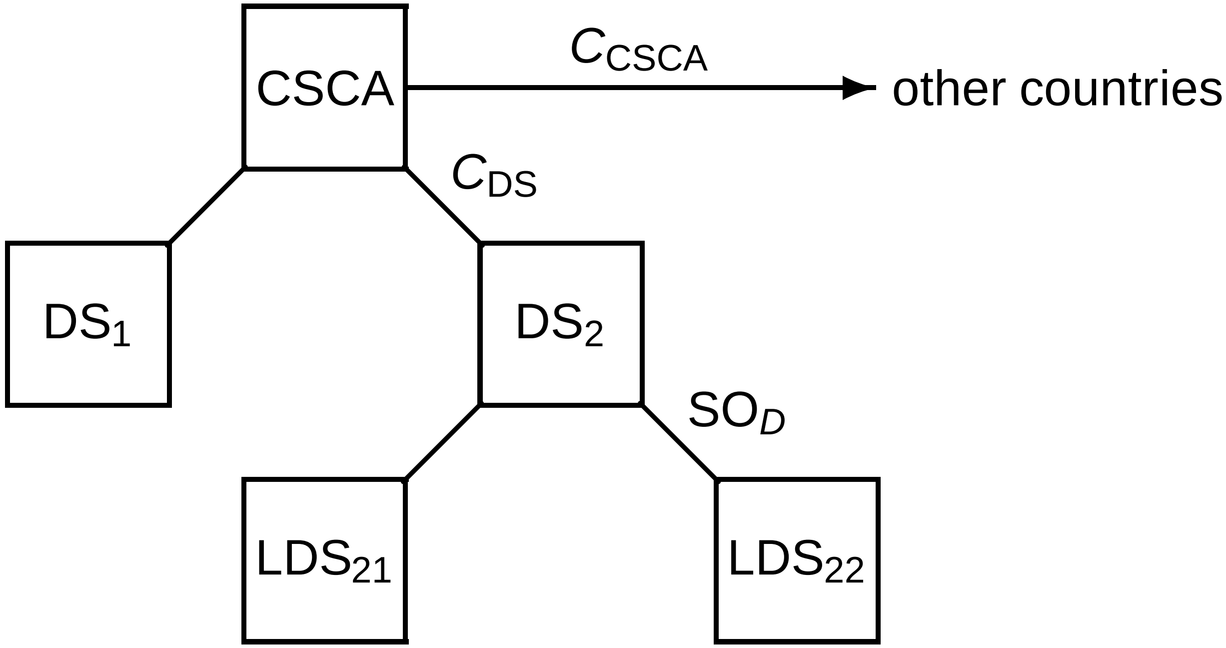
# LDS Structure

- DG1 (mandatory): same as MRZ
- DG2 (mandatory): encoded face
- DG3: encoded finger(s)
- DG4: encoded eye(s)
- DG5: displayed portrait
- DG6: (reserved)
- DG7: displayed signature
- DG8: data feature(s)
- DG9: structure feature(s)
- DG10: substance feature(s)
- DG11: add. personal detail(s)
- DG12: add. document detail(s)
- DG13: optional detail(s)
- DG14: (reserved)
- DG15: $KPu_{AA}$
- *DG16: person(s) to notify*
- DG17: autom. border clearance
- DG18: electronic visa
- DG19: travel record(s)
- $SO_D$ (mandatory)

# $SO_D$ Structure

- list of hash for data groups DG1–DG15
- formatted signature by DS (include: information about DS)
- (optional) $C_{\text{DS}}$

# Hierarchy




- one PKI per country
  one CSCA (Country Signing Certificate Authority)
  $C_{CSCA}$: self-signed CSCA public key $KPu_{CSCA}$
  $C_{CSCA}$ distributed to other countries by diplomatic means
- possibly many DS (Document Signer) per country
  $C_{DS}$: certificate for a DS public key $KPu_{DS}$
- $SO_D$: signature of (part of) LDS in MRTD

1. **ICAO-MRTD**
   - ICAO-MRTD Overview
   - Data Structures and PKI
   - MRTD Cryptography
   - Security and Privacy Issues

2. **Non-Transferable Proofs**

# Basic Access Control

**goal** prevent from unauthorized access by the holder (privacy)

- read MRZ (OCR-B)
- extract MRZ_info
- run an authenticated key exchange based on MRZ_info
- open secure messaging based on the exchanged symmetric key

$\longrightarrow$ proves that reader knows MRZ_info

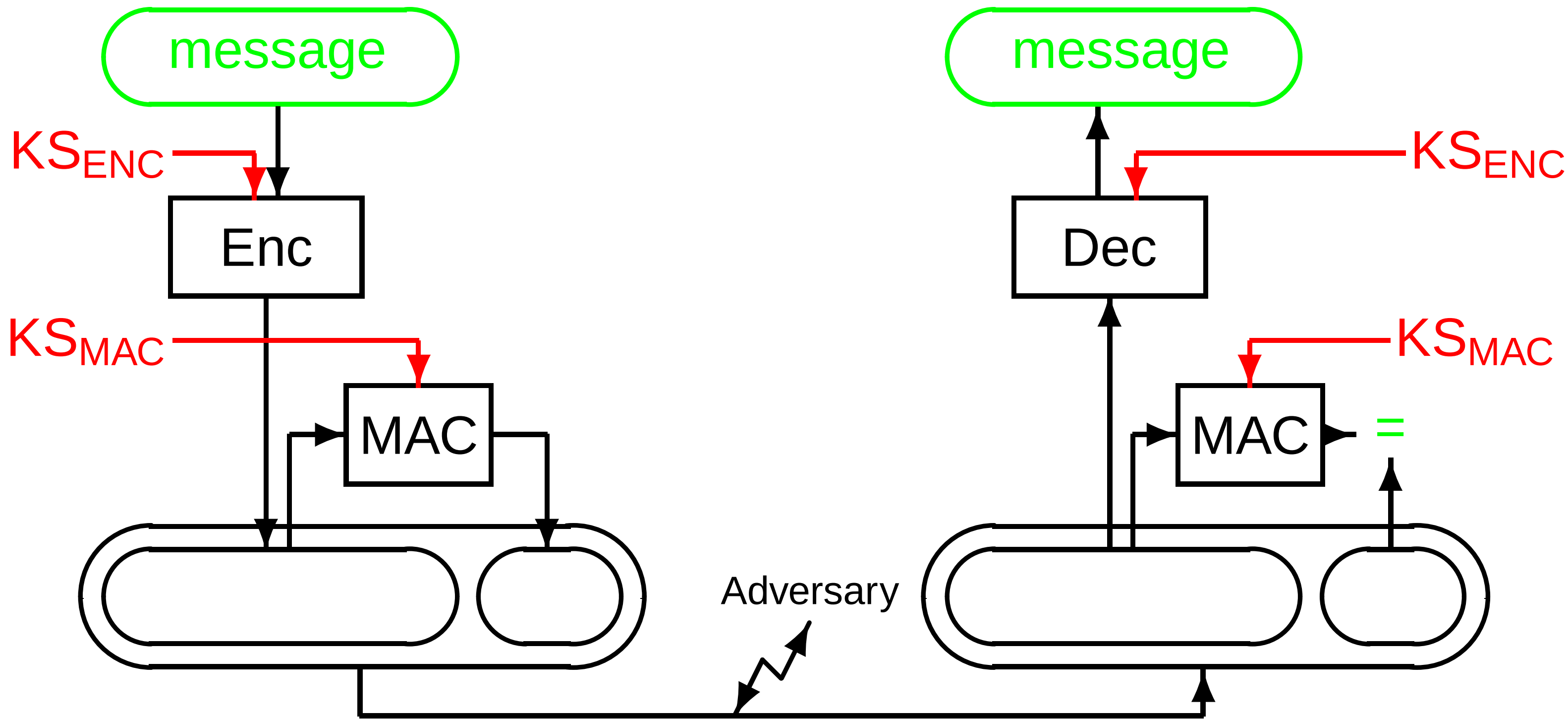
# MRZ_info

```
PMFRADUPONT<<<<JEAN<<<<<<<<<<<<<<<<<<<<<<<<<
74HK8215<6CHE7304017M0705121<<<<<<<<<<<<<<03
```

- document type
- issuing country
- holder name
- doc. number + CRC
- nationality
- date of birth + CRC
- gender
- date of expiry + CRC
- options + CRC

# Secure Messaging

**goal** authentication, integrity, confidentiality of communication




⟶ secure channel based on 3DES

# Passive Authentication

**goal** authenticate LDS

- after getting $SO_D$, check the included certificate $C_{\mathrm{DS}}$ and the signature
- when loading a data group from LDS, check its hash with what is in $SO_D$

→ stamp by DS on LDS

# Active Authentication

**goal** authenticate the chip

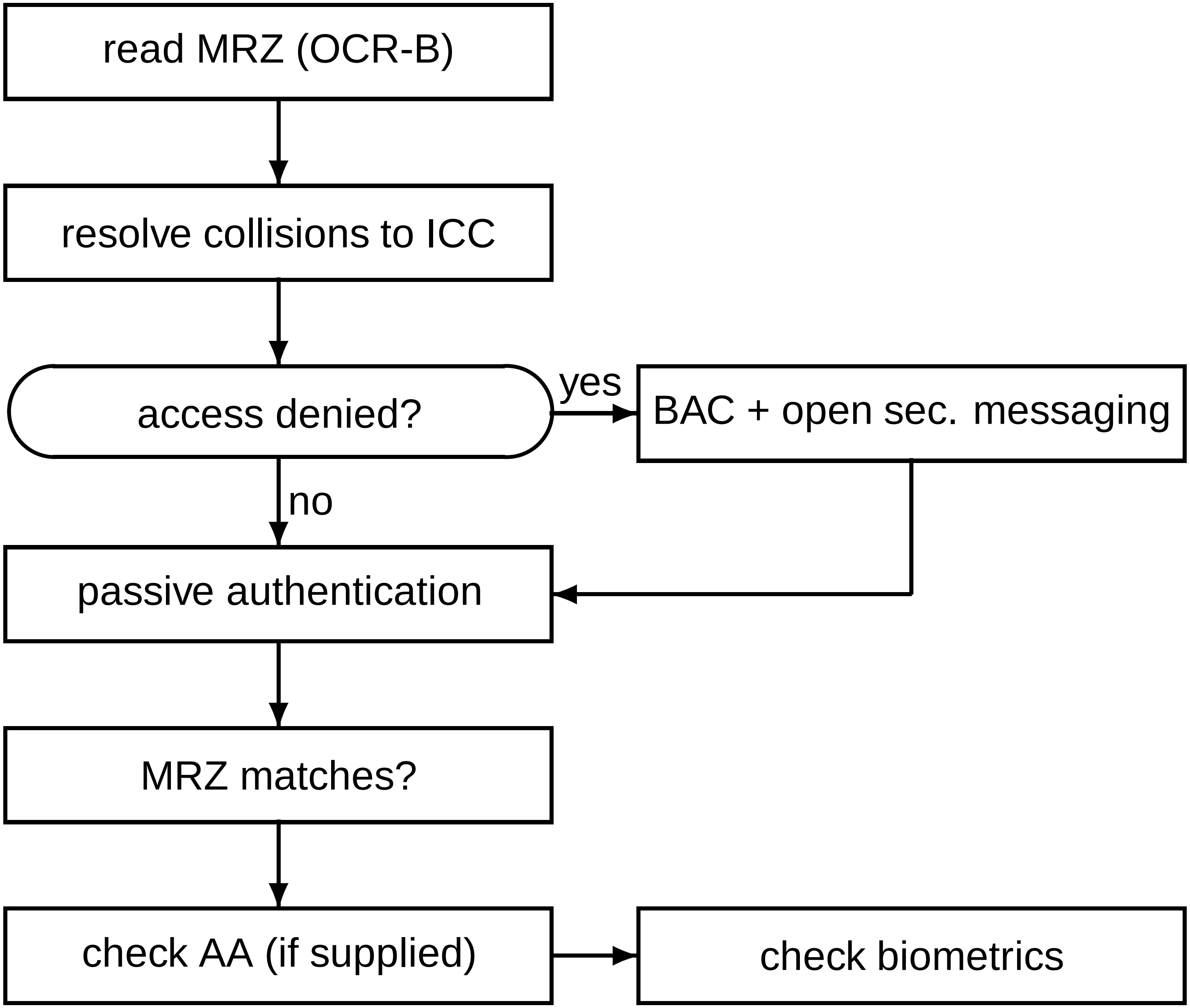
- proves that ICC knows some secret key $KPr_{AA}$ linked to a public key $KPu_{AA}$ by a challenge-response protocol
  ($KPu_{AA}$ in LDS authenticated by passive authentication)

$\longrightarrow$ prove that the chip is not a clone

# Active Authentication Protocol

| IFD | | ICC |
|---|---|---|
| pick RND.IFD | $\xrightarrow{\text{RND.IFD}}$ | $F \leftarrow \text{nonce} \| \text{RND.IFD}$ |
| check | $\xleftarrow{\Sigma}$ | $\Sigma \leftarrow \text{Sign}_{\text{KPr}_{\text{AA}}}(F)$ |

# Sequence of Steps for Identification



# Coming From Wireless Technology

(claimed to be possible at a distance of 10m)

- detecting the proximity of an e-passport
  **threat**: giving valuable information to passport theafs
  **threat**: privacy (in some cases) by tracking people
- data skimming
  **threat**: privacy
- unauthorized access
  **threat**: privacy

# Coming From IC Chip

- too much trust in automated process, lazzy identification
  **threat**: identity theft
- malicious cookies put in MRTD
  **threat**: privacy
- dependence on the technology: DoS attack could kill the IC chip
  **threat**: waste of time at border controls
- abuse of automatic recognition
  **threat**: privacy
- leakage of digital evidence
  **threat**: privacy

# Digital Evidence: Challenge Semantics Attack

challenge semantics in AA:

- evidence that $D$ existed when MRTD was queried

$$\begin{aligned} \text{RND.IFD} &= H(D) \\ \text{evidence} &= (D||\text{LDS}||\Sigma) \end{aligned}$$

- evidence that MRTD was accessed at time $t$

$$\begin{aligned} \text{RND.IFD} &= H(\text{social}(t-1)) \\ \text{evidence} &= \text{timestamp}_t(\text{social}(t-1)||\text{LDS}||\Sigma) \end{aligned}$$

# Digital Evidence: Transferable LDS Authentication

- signed personal data (name, age, gender, face, etc)
- can no longer hide/deny name, age, gender...
- when DG11 is used: more personal data (place of birth etc)
- personal profiles can be sold if they come with a proof

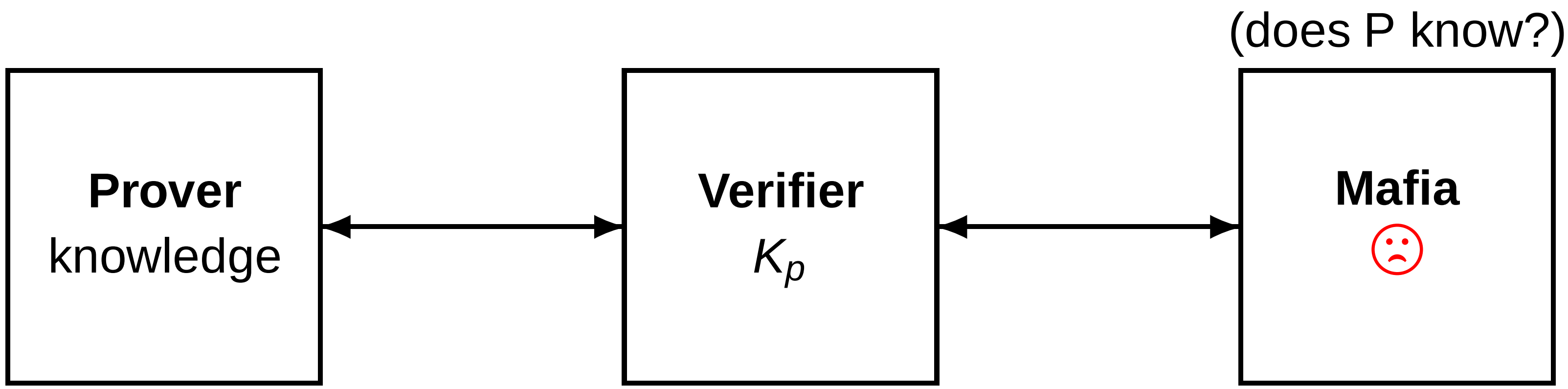
1 ICAO-MRTD

2 Non-Transferable Proofs

1. ICAO-MRTD

2. **Non-Transferable Proofs**
   - Notions of Non-Transferability
   - ZK Protocols for MRTD

# Mafia Fraud + Fully Non-Transferable Proof



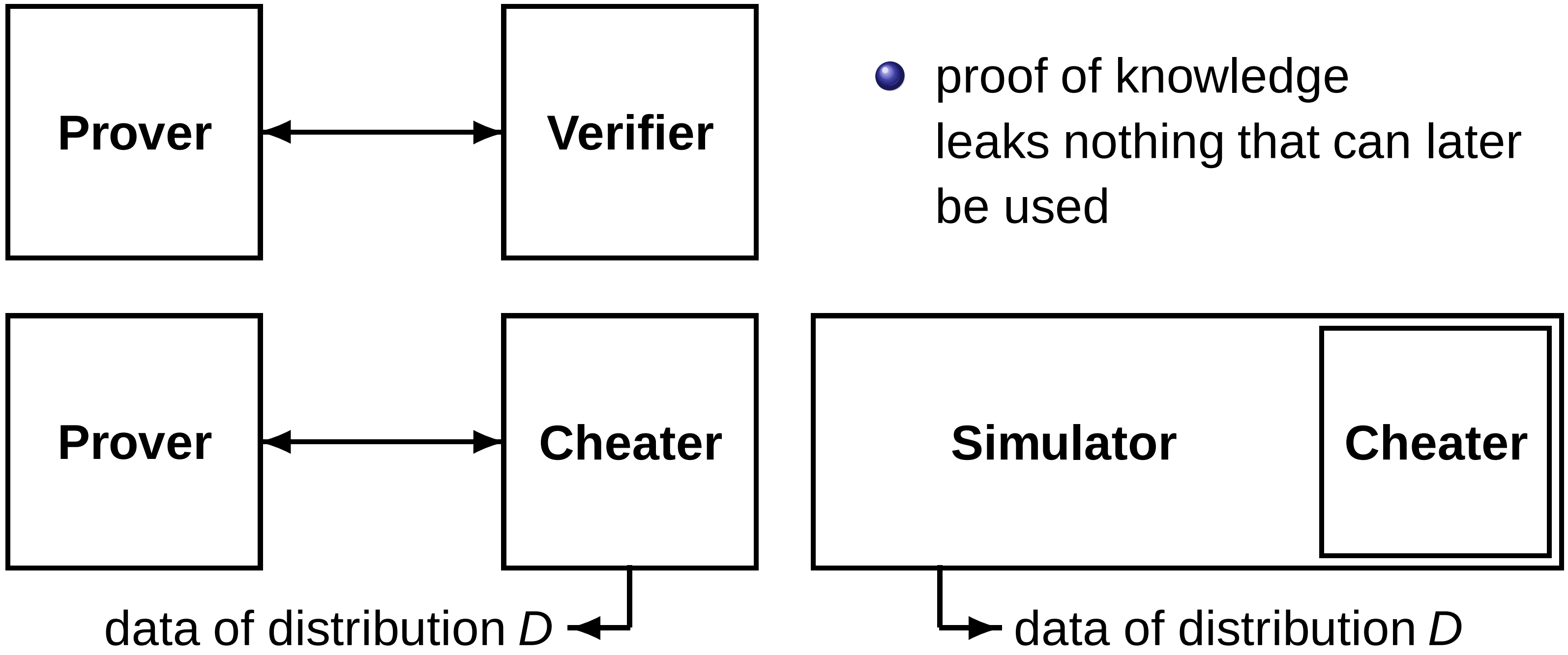

proof of knowledge

$\downarrow$

proof of knowledge or of knowing a secret key attached to $K_p$

$\longrightarrow$ need PKI for verifiers: maybe an overkill

# Zero-Knowledge: Offline Non-Transferability




- proof of knowledge leaks nothing that can later be used

# Sigma Protocols

| Prover | | Verifier |
|---|---|---|
| **secret**: $x$ | | |
| | commitment → | |
| | ← challenge | |
| | response → | check |

# Example: GPS Identification

| **Prover** | | **Verifier** |
|---|---|---|
| **parameters**: $g, A, B, S$ | | |
| **public key**: $I$ ($I = g^s$) | | **input**: $I, g, A, B, S$ |
| **secret key**: $s \in [0, S]$ | | |
| pick $r \in [0, A-1]$ | | pick $c \in [0, B-1]$ |
| $x \leftarrow g^r$ | $\xrightarrow{x}$ | |
| | $\xleftarrow{c}$ | |
| $y \leftarrow r + cs$ | $\xrightarrow{y}$ | check $g^y = xI^c$ |
| | | and $0 \leq y < A + (B-1)(S-1)$ |

# Fiat-Shamir Signature

Basic Fiat-Shamir identification protocol:

| **Prover** | | **Verifier** |
|---|---|---|
| pick $r$, $x = r^2 \bmod n$ | $\xrightarrow{v,x}$ | |
| | $\xleftarrow{e}$ | $e = 0$ or $1$ |
| $y = rs^e \bmod n$ | $\xrightarrow{y}$ | check $y^2 v^e \equiv x$ |

Conversion into a signature:

- use random coins from $H(\text{message}, \text{previously seen transcript})$
- simulate the verifier using these coins
- the signature is the final transcript

# Honest vs Malicious Verifier

- for Sigma-protocols: the signature is unforgeable
- malicious verifier that simulates the previous conversion: it produces a signature
- consequences: Sigma-protocols are not ZK
- maybe honest-verifier ZK
- verifiers playing the challenge semantics are not honest
- challenge semantics in GPS identification: $c = H(\text{semantics}, x)$
- UDVSP [Baek et al. Asiacrypt05]: same

1. ICAO-MRTD

2. **Non-Transferable Proofs**
   - Notions of Non-Transferability
   - ZK Protocols for MRTD

# Converting Sigma Protocols into ZK Protocols

| **Prover** | | **Verifier** |
| --- | --- | --- |
| **secret**: $x$ | | |
| pick $c_P$ | | pick $c_V$ |
| | $\xleftarrow{\gamma}$ | $(\gamma, \delta) \leftarrow \text{commit}(c_V)$ |
| | $\xrightarrow{\text{commitment}, c_P}$ | |
| | $\xleftarrow{\delta, c_V}$ | |
| $\text{check}(c_V, \gamma, \delta)$ | $\xrightarrow{\text{response}}$ | check |
| | (challenge is $c_P \oplus c_V$) | |

# Proof of Signature Knowledge based on GQ

| Prover | | Verifier |
|---|---|---|
| **formated digest**: $X$<br>**signature**: $x$ | **public key**: $N, e$ | **formated digest**: $X$ |
| pick $y \in \mathbf{Z}_N^*$ | | pick $c_V \in \{0,1\}^\ell$ |
| pick $c_P \in \{0,1\}^\ell$ | $\xleftarrow{\gamma}$ | $(\gamma, \delta) \leftarrow \text{commit}(c_V)$ |
| $Y \leftarrow y^e \bmod N$ | $\xrightarrow{Y, c_P}$ | |
| $\text{check}(c_V, \gamma, \delta)$ | $\xleftarrow{\delta, c_V}$ | |
| $z \leftarrow yx^c \bmod N$ | $\xrightarrow{z}$ | check $z^e = YX^c \pmod{N}$ |
| | $(c = c_P \oplus c_V)$ | |

# Easy AA from Previous Passive Authentication

proof of holding a signature of SOD

$$\downarrow$$

proof of holding a secret signature of SOD

# AA based on GPS

| Prover | | Verifier |
|---|---|---|
| **parameters**: $g, A, B, S$ | | |
| **public key**: $I$ ($I = g^s$) | | **input**: $I, g, A, B, S$ |
| **secret key**: $s \in [0, S]$ | | |
| pick $r \in [0, A-1]$ | | pick $c_V \in [0, B-1]$ |
| pick $c_P \in [0, B-1]$ | $\xleftarrow{\gamma}$ | $(\gamma, \delta) \leftarrow \text{commit}(c_V)$ |
| $x \leftarrow g^r$ | $\xrightarrow{x, c_P}$ | |
| $\text{check}(c_V, \gamma, \delta)$ | $\xleftarrow{\delta, c_V}$ | |
| $y \leftarrow r + cs$ | $\xrightarrow{y}$ | check $g^y = xI^c$ |
| | | and $0 \leq y < A + (B-1)(S-1)$ |

$$(c = c_P + c_V \bmod B)$$

# Conclusion

- privacy threat of MRTD coming from wireless channel
- privacy threat of MRTD coming from leakage of evidence
- weakly non-transferable proofs
- proof of signature knowledge based on GQ
- fix of AA

Q & A