Efficient Selective Disclosure on Smart Cards using Idemix

Pim Vullers Gergely Alpár

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

Conference on Policies & Research in Identity Management
8th April 2013

Attributes on Smart Cards

Privacy issues

- Smart cards are "Big Brother's little helper" (Stefan Brands)
- With Oyster / OV-chipcard / Charlie / . . . , you tell who you are when you get on a bus, metro, train, . . .
- Identity-based solutions violate their users' privacy (and increase identity-fraud risk)

Attribute-based credentials

- Attribute-based authorisation: only provide the information which the system needs
- Example of attribute-based credentials (electronic wietpas):
  - card only says "I'm a Dutch *citizen*, and my *age* is over 18"

Outline

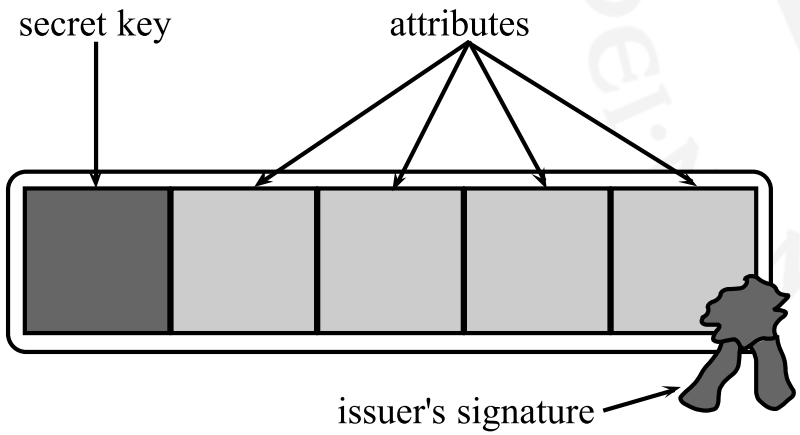
Credential-based System

The ideas

- Attributes: grouped in credentials
- Data minimisation: selective disclosure
- Unlinkability: randomisation & zero-knowledge

A credential

- Attributes
- Secret key
- Issuer's signature



Protocols

1. **Credential issuance**
   - *Blind signature* generated by the issuer over the secret key of the card and the attributes to be issued.
   - Issuer unlinkability

2. **Attribute verification**

   I **Proof generation / presentation**
   - *Selective disclosure* of the credential's attributes
   - Randomisation of the issuer's signature

   II **Proof verification / authentication**
   - Verify the *zero-knowledge proof* using the issuer's public key
   - Multi-show unlinkability

Idemix specifics

Camenisch-Lysyanskaya signature scheme

- Keys: $(n, S, Z, R_{0\ldots l})$, (p', q') where $n = (2p' + 1)(2q' + 1)$
- Signature: (A, e, v) where $A = \left(\frac{Z}{S^v \prod_{i=0}^{l} R_i^{m_i}} \right)^{e^{-1} \mod p'q'} \mod n$

Credentials

- Secret key: m_0
- Attributes: $m_1 \ldots m_l$

Verification

- Randomisation (with r): $A' = A \cdot S^r \mod n$, $v' = v - e \cdot r$
- Zero-knowledge proof of e and undisclosed m_i

Outline

Smart Card Platforms

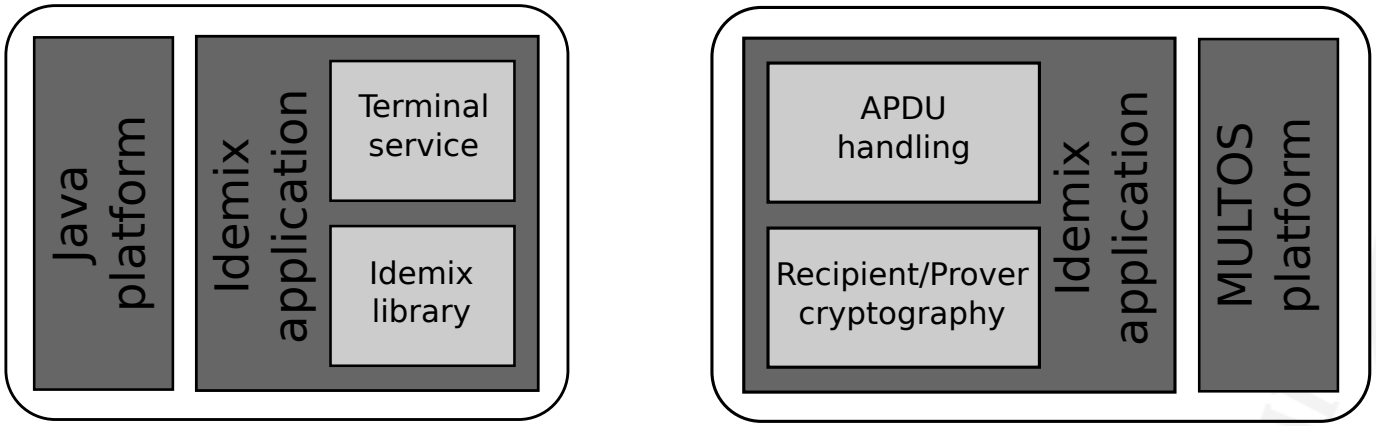
Java Card

+ High-level (object-oriented) programming language
+ Widely spread / high availability
– Limited cryptographic API / no mathematical API

MULTOS

+ Low-level access to the cryptographic co-processor
+ Proper cryptographic/mathematical API
+ Very flexible memory management
– Low-level language causes a steep learning curve.
– Limited amount of RAM available

Design of the System



(a) Terminal (b) Card

Figure : System architecture for Idemix on a smart card.

- Terminal service translates IBM's Idemix commands and data types into APDU commands for smart card communication
- MULTOS implementation, limited by smart card characteristics, is 95% compatible with Idemix Library

Outline

Related Work on Smart Cards

Related work

- Bichsel et al. (IBM Research, 2009), ± 7.5 sec
  Camenisch & Lysyanskaya anonymous credential system
- Sterckx et al. (KU Leuven, 2009), ± 3 sec
  Direct anonymous attestation

Our previous results

- Batina et al. (RU Nijmegen, 2010), ± 1.5 sec
  Hoepman et al. (RU Nijmegen, 2010), ± 0.6 sec
  Self-blindable certificates of Verheul
- Mostowski and Vullers (RU, 2011), ± 0.5 - 0.9 sec
  U-Prove selective disclosure (2-5 attributes)

Issuance Performance

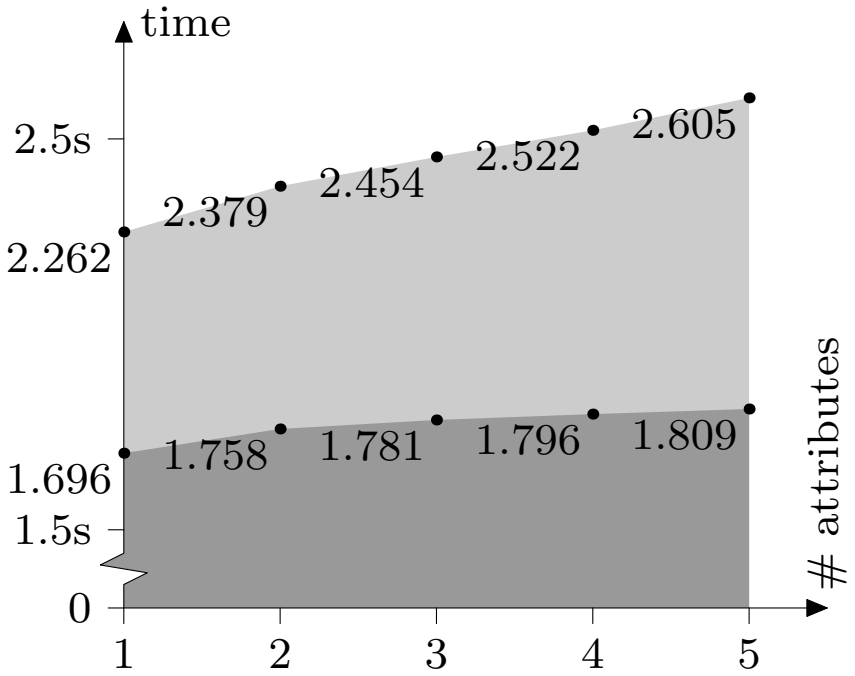
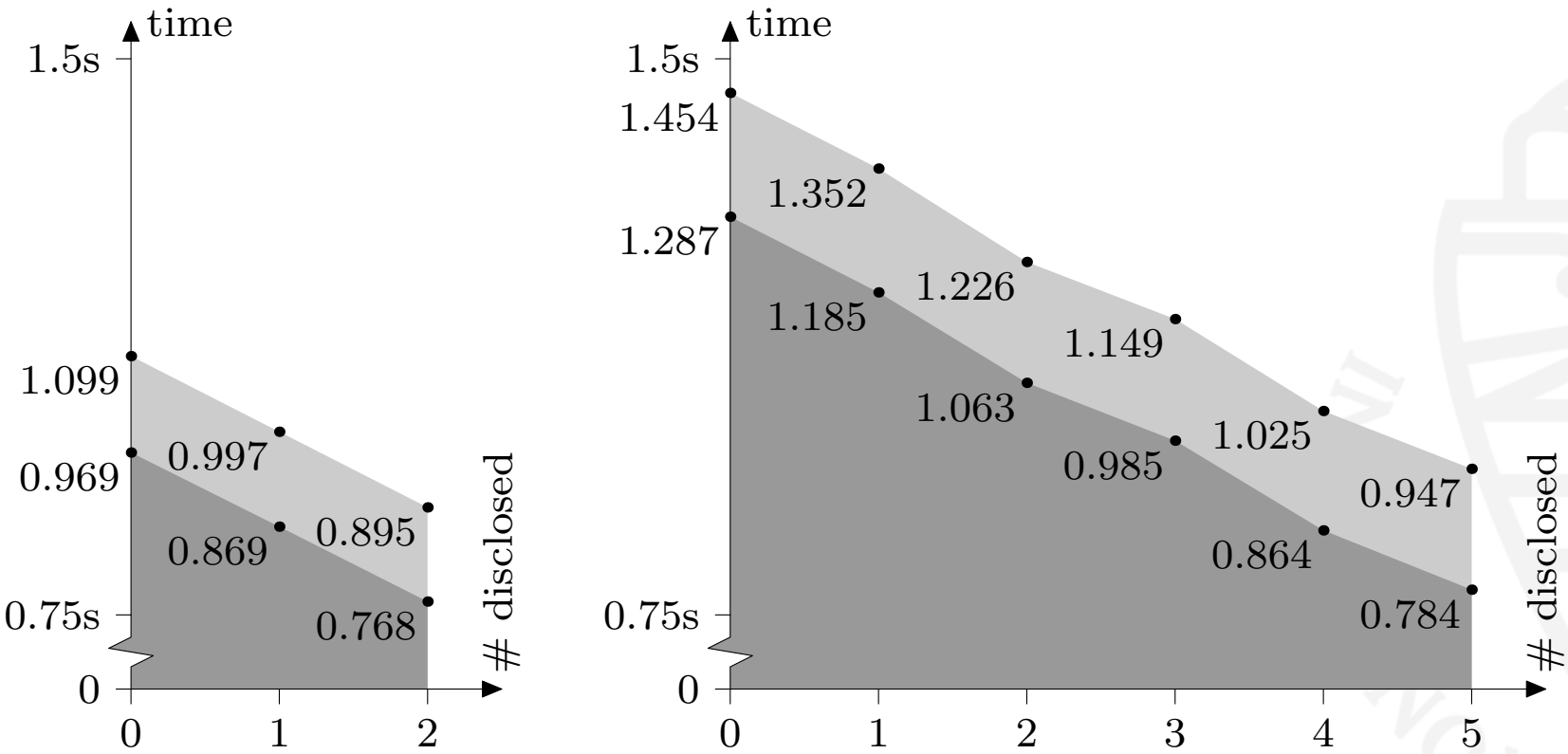


Figure : Credential issuance times (■: computation, ■: overhead).

Presentation Performance

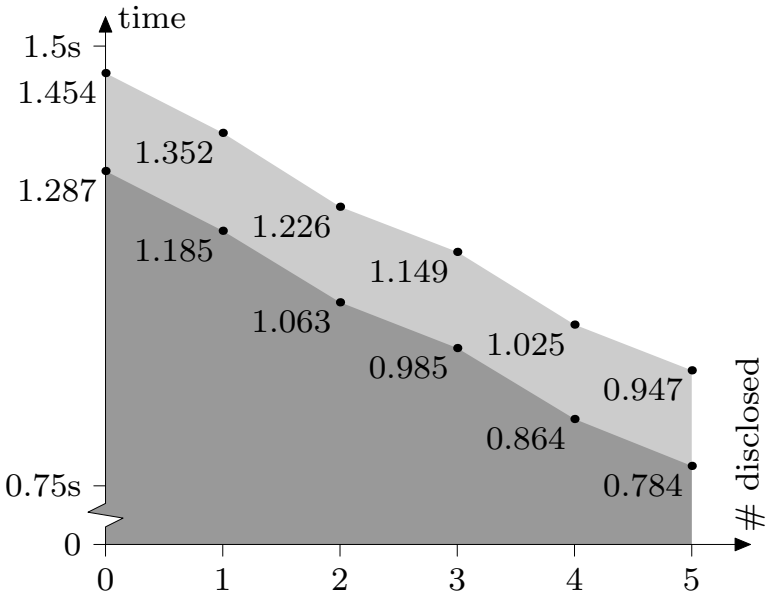


(a) 2 stored attributes

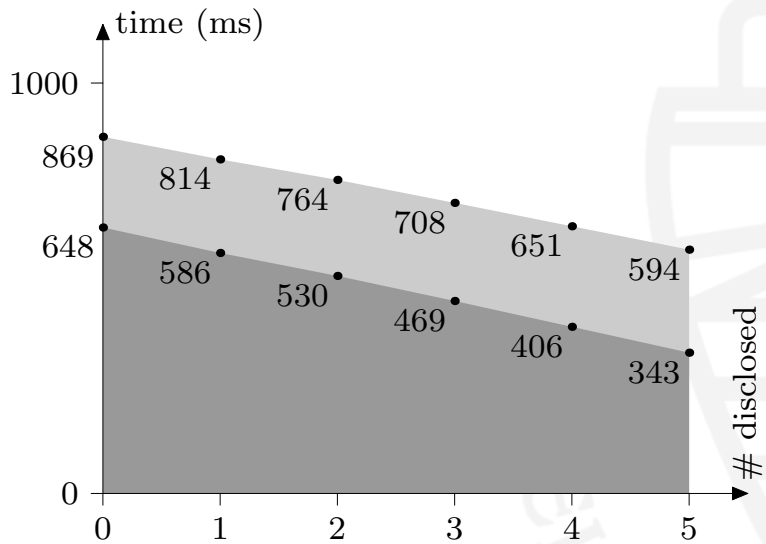
(b) 5 stored attributes

Figure : Attribute verification times (: computation, : overhead).

U-Prove Comparison



(a) Idemix



(b) U-Prove

Figure : Attribute verification times (: computation, : overhead).

Summary

- *Efficient MULTOS implementation* of the Idemix technology
- *Multi-show unlinkability* of the credentials on the smart card

- Attribute-based credentials on smart cards are possible
- Major improvement over IBM's DAA implementation

Next steps:

- Studying other technologies
- Practicing with other platforms

- Making anonymous credentials *usable*: IRMA

IRMA – I Reveal My Attributes

Tuesday 9th April 2013

09:15 – 10:15 Second keynote session: Bart Jacobs

Towards Practical Attribute-Based Identity Management: the IRMA Trajectory.

`https://www.irmacard.org/`

Demo

Questions