IBM Research, Zurich

# *Efficient Attributes for Anonymous Credentials*

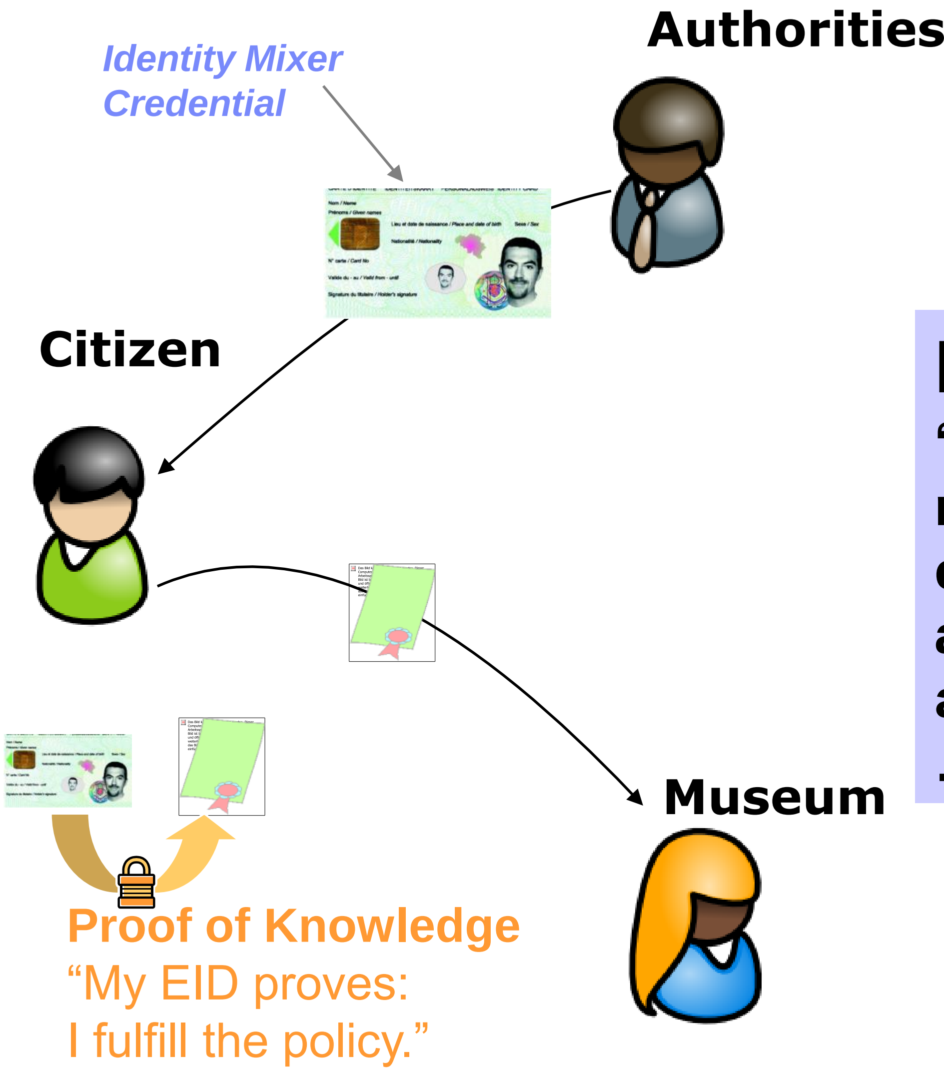
Jan Camenisch and
Thomas Gross

10/29/2008 | ACM CCS 2008

# Overview

- **Introduction:** Access with electronic identity cards
- **Basis:** Camenisch-Lysyanskaya signatures
- **Problem Statement:** Efficient finite set attributes
- **Key Ideas:** Prime number encoding and divisibility
- **Efficiency**

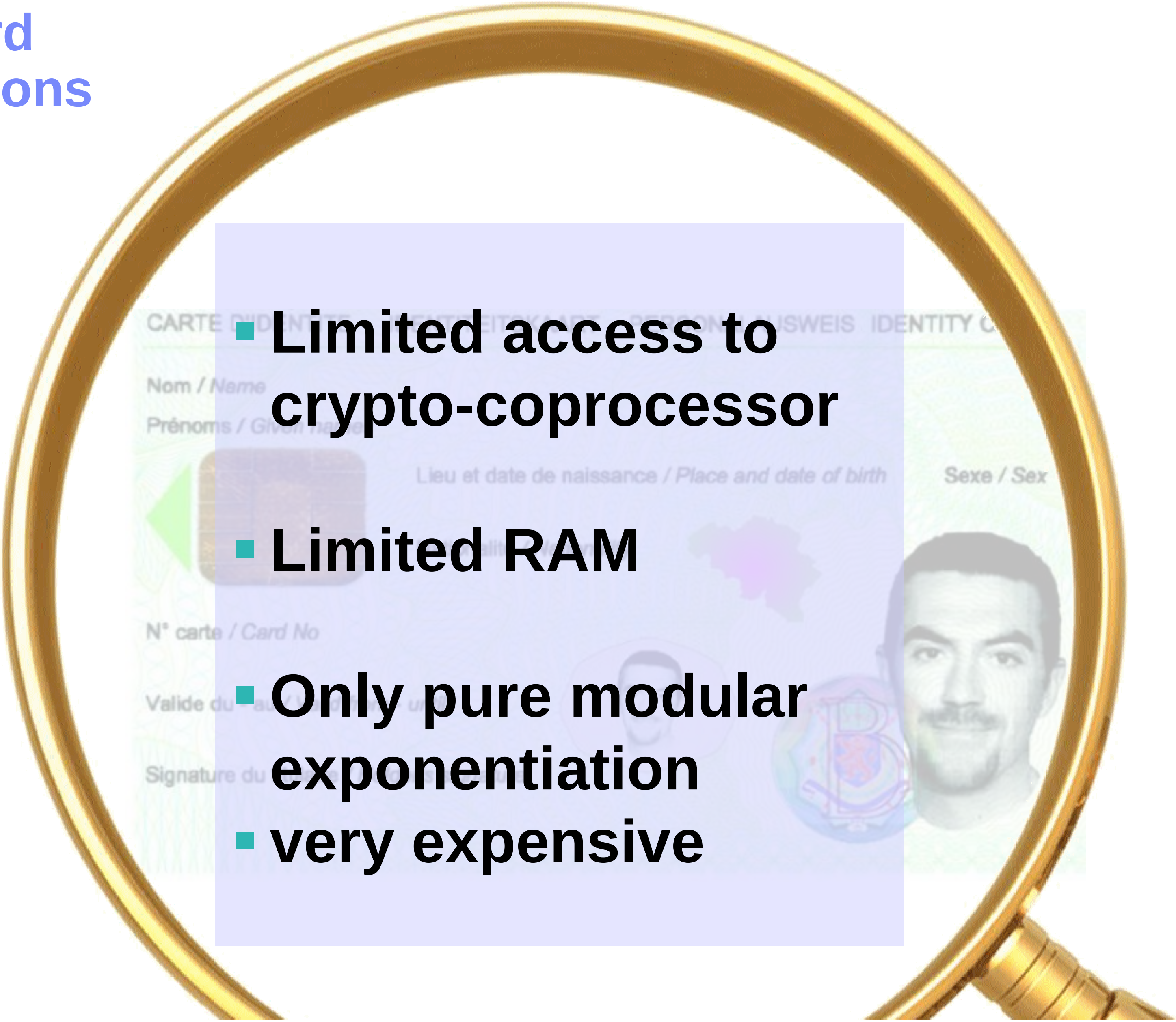
# Getting Access to a Vernissage




**Policy:**
**"free entry: must be retired OR entitled to social benefit OR a teacher OR a poor grad student… … on hunt for free food"**

"Piled Higher and Deeper"
by Jorge Cham
www.phdcomics.com

# EID Card Limitations




- Limited access to crypto-coprocessor
- Limited RAM
- Only pure modular exponentiation
- very expensive

# EID Card Attributes


**Free-form**

- **Identification number**
- **Name, first name**
- **Date of birth**

**Binary & Finite Set**

- **Nationality**
- **Place of birth**
- **Profession**
- **Social benefit status**
- **Eye and hair color**
- **Sex…**

# Basis: Camenisch-Lysyanskaya Signatures

[Camenisch & Lysyanskaya '01]

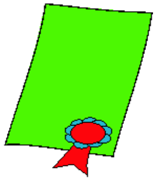
Public key of signer: RSA modulus $n$ and $a_i$, $b$, $d$ $\in QR_n$,

Secret key: factors of $n$

Signature of $L$ attributes $m1, \ldots, mL \in \{0,1\}^{\ell}$ : $(c,e,s)$

For random prime $e > 2^{\ell}$ and integer $s \approx n$, compute $c$ such that

$$d = a_1^{m1} \cdot \ldots \cdot a_L^{mL} \; b^s \; c^e \mod n$$



**Theorem**: ***Signature scheme is secure against adaptively chosen message attacks under SRSA assumption.***

[SRSA: Barić & Pfitzmann '97 and Fujisaki & Okamoto '97]

# Basis: Camenisch-Lysyanskaya Signatures

[Camenisch & Lysyanskaya '01]

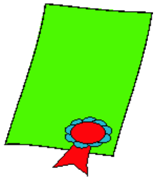
Public key of signer: RSA modulus $n$ and $a_i$, $b$, $d$ $\in QR_n$,

Secret key: factors of $n$

Signature of $L$ attributes $m1, ..., mL \in \{0,1\}^\ell$ : $(c,e,s)$

For random prime $e > 2^\ell$ and integer $s \approx n$, compute $c$ such that

$$d = a_1^{m1} \cdot \ldots \cdot a_L^{mL} \quad b^s \quad c^e \mod n$$



**Theorem**: ***Signature scheme is secure against adaptively chosen message attacks under SRSA assumption.***

[SRSA: Barić & Pfitzmann '97 and Fujisaki & Okamoto '97]

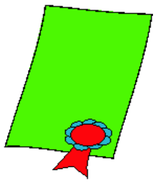
# Basis: Camenisch-Lysyanskaya Signatures

[Camenisch & Lysyanskaya '01]

Signature of L attributes $m1, \ldots, mL \in \{0,1\}^{\ell}$ : **(c,e,s)**

For random prime $e > 2^{\ell}$ and integer $s \approx n$, compute $c$ such that

$$d = a_1^{m1} \cdot \ldots \cdot a_L^{mL} \; b^s \; c^e \mod n$$



| $a_1^{m1} \cdot \ldots \cdot a_L^{mL}$ | $b^s$ | $c^e$ |
|---|---|---|
| L attribute bases<br>**one base per attribute mi** | blinding | SRSA problem instance |
| **Proofs of possession:**<br>*O*(L) mod-exp complexity<br>**➔ Invites for a nap** | constant | constant |

"Piled Higher and Deeper"
by Jorge Cham www.phdcomics.com

# Problem Statement

**Enable Camenisch-Lysyanskaya signatures to compress *all* binary and finite set attributes in *one* dedicated attribute base.**

## Efficiency:

- **Proofs of possession** linear in the free-form attributes: $O(l)$, binary and finite set attributes only as small constant overhead.
- **Proofs of relationships** with efficient toolbox for AND, NOT, OR.

## Security:

- Signature scheme is secure against adaptively chosen message attacks under SRSA assumption.
- Attribute encoding is integer under SRSA assumption.

# Key Ideas: Prime Encoding…

[Compare to Camenisch & Lysyanskaya '02]

## Idea: Encode attribute values as prime numbers.

- **SETUP**: Certify a small public prime number $e_i$ for each value realization of a binary or finite-set attribute.
- **ISSUE**: Product of prime numbers $E=\Pi(e_i)$ in a single dedicated base.

➔ **Compression of $k$ binary and finite-set attributes in one base**

## Realization:

Signature of $L$ attributes $m_1, \ldots, m_L \in \{0,1\}^{\ell}$ : $(c,e,s)$

With $k$ binary or finite set attributes and $l$ string attributes

$$d = a_0^{\Pi e_i} \cdot a_1^{m_1} \cdot \ldots \cdot a_l^{m_l} \quad b^s \quad c^e \mod n$$

# Key Ideas: … and Divisibility

## Idea: Use coprime/divisibility to prove attribute presence and absence.

**PROOF**: Selectively disclose attribute primes $\Pi(ej)$ and prove knowledge of remaining factorization $E' = \Pi_{i \neq j}(ei)$ of the compound attribute $\Pi(ei)$.

➔ **Efficient proof methods for AND, NOT, OR statements.**

## Realization:

**Proof of Knowledge of AND with prime attributes:**

- $PK\{(e, E', m1, \ldots, ml, s) :$

$$d := c'^{e} \cdot (a_0^{\Pi(ej)})^{E'} \cdot a_1^{m1} \cdot \ldots \cdot a_l^{ml} \, b^{s} \bmod n \ \ldots \}$$

# Efficiency: Asymptotic Modular Exponentiations

| | Base Encoding | Bit Vector Encoding | Prime encoding |
|---|---|---|---|
| Bases & Possession | O(L) | O(l) | O(l)* |
| AND (i attributes) | O(L) | O(L+i) | O(l)* |
| NOT | O(L) | O(L) | O(l)* |
| OR (i attributes) | O(L+i) | O(L+i) | O(l)** |

*) Small constant overhead to proof of possession (1-2 mod-exp).

**) Constant overhead of 18 mod-exp. over proof of possession.
Break even points, e.g. k=5 binary attributes, i=2 shown.

# Summary

## Advantages

- Constant mod-exps for binary flags & finite sets
- Efficient proofs for AND, NOT, OR
- Compact credentials: Save k-1 attribute bases

## Limitations

- Free-form attributes
- A priori vocabulary
- Public key overhead: k * |mi| * |ei|

**Conclusion: 80/20 solution where finite sets matter**

# BACKUP

# Recall: The Strong RSA Assumption

Flexible RSA Problem: *Given RSA modulus $n$ and $z \in QR_n$ find integers $e$ and $u$ such that*

$$u^e = z \bmod n$$

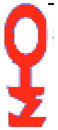
(Recall: $QR_n = \{x : \text{exist } y \text{ s.t. } y^2 = x \bmod n\}$ )

- Introduced by Barić & Pfitzmann '97 and Fujisaki & Okamoto '97
- Hard in generic algorithm model [Damgård & Koprowski '01]

# Signature Scheme based on the SRSA I

[Camenisch & Lysyanskaya '02]

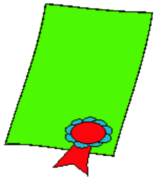
Public key of signer: RSA modulus $n$ and $a_i$, $b$, $d$ $\in QR_n$, 

Secret key: factors of $n$ 

To sign $k$ messages $m1, \ldots, mk \in \{0,1\}^\ell$ :

- choose random prime $e > 2^\ell$ and integer $s \approx n$
- compute $c$ such that

$$d = a_1^{m1} \cdot \ldots \cdot a_k^{mk} \, b^s \, c^e \mod n$$

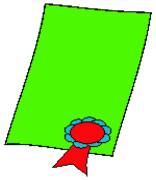


- signature is $(c,e,s)$

# Signature Scheme based on the SRSA II

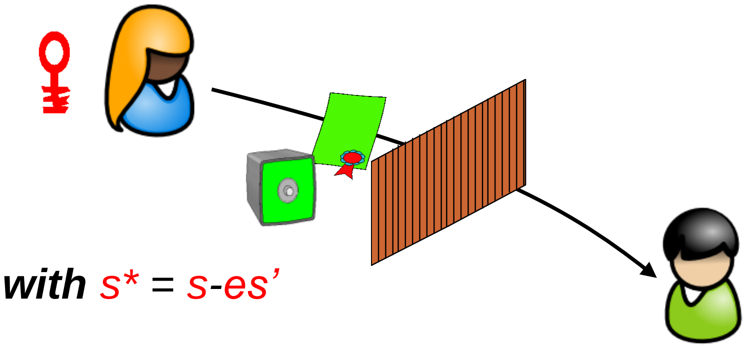
A signature $(c,e,s)$ on messages $m1, \ldots, mk$ is valid iff:

- $m1, \ldots, mk \in \{0,1\}^{\ell}$:
- $e > 2^{\ell}$
- $d = a_1^{m1} \cdot \ldots \cdot a_k^{mk}\; b^s\; c^e \bmod n$



Theorem: *Signature scheme is secure against adaptively chosen message attacks under SRSA assumption.*

# Proof of Knowledge of a Signature



***Observe:***

***Let*** $c' = c\, b^{s'} \bmod n$ ***with random*** $s'$

***then*** $d = c'^{e}\, a_1^{m1} \cdot \ldots \cdot a_k^{mk}\, b^{s*}$ ***(mod*** $n$***), with*** $s^* = s\text{-}es'$

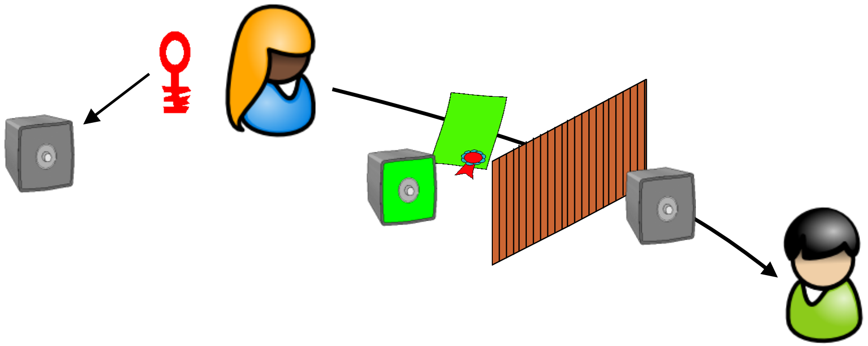
***i.e.,*** $(c', e, s^*)$ ***is a also a valid signature!***

Therefore, to prove knowledge of signature on some m

- provide $c'$
- PK{(e, m1, …, mk, s) : $d := c'^{e}\, a_1^{m1} \cdot \ldots \cdot a_k^{mk}\, b^{s}$

$$\wedge \;\; mi \in \{0,1\}^{\ell} \;\; \wedge \;\; e \in 2^{\ell+1} \pm \{0,1\}^{\ell} \;\; \}$$

# Proof of Knowledge of a Signature



***Using second Commitment***

***assume second group*** $n, a_i, b, n$

***2nd commitment*** $C = a_1^{sk} b^{s*}$

***To prove knowledge of signature on some*** $m$

***provide*** $c'$

$PK\{(e, m1, \ldots, mk, s, s^*):$

$$C = a_1^{m1} b^{s^*} \wedge \quad d := c'^{e} a_1^{m1} \cdot \ldots \cdot a_k^{mk} b^{s} \}$$