Zurich Research Laboratory

An Efficient Anonymous Credentials System

idemix

Jan Camenisch
IBM Research
joint work w/ Anna Lysyanskaya, Ivan Damgård, Victor Shoup

May 30th, 2005

www.zurich.ibm.com

Outline

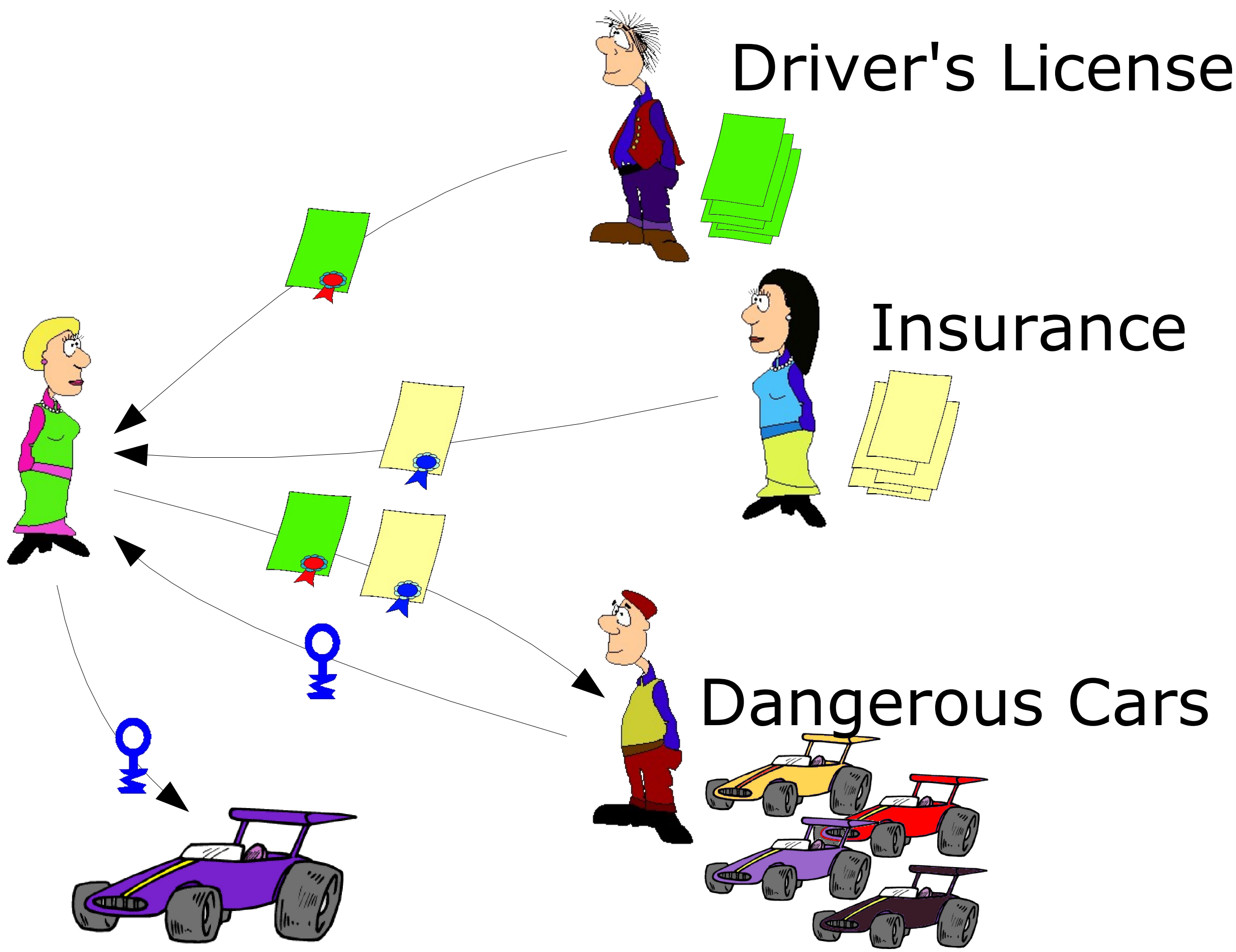
I. Requirements of Anonymous Credential System

II. Abstract Solution

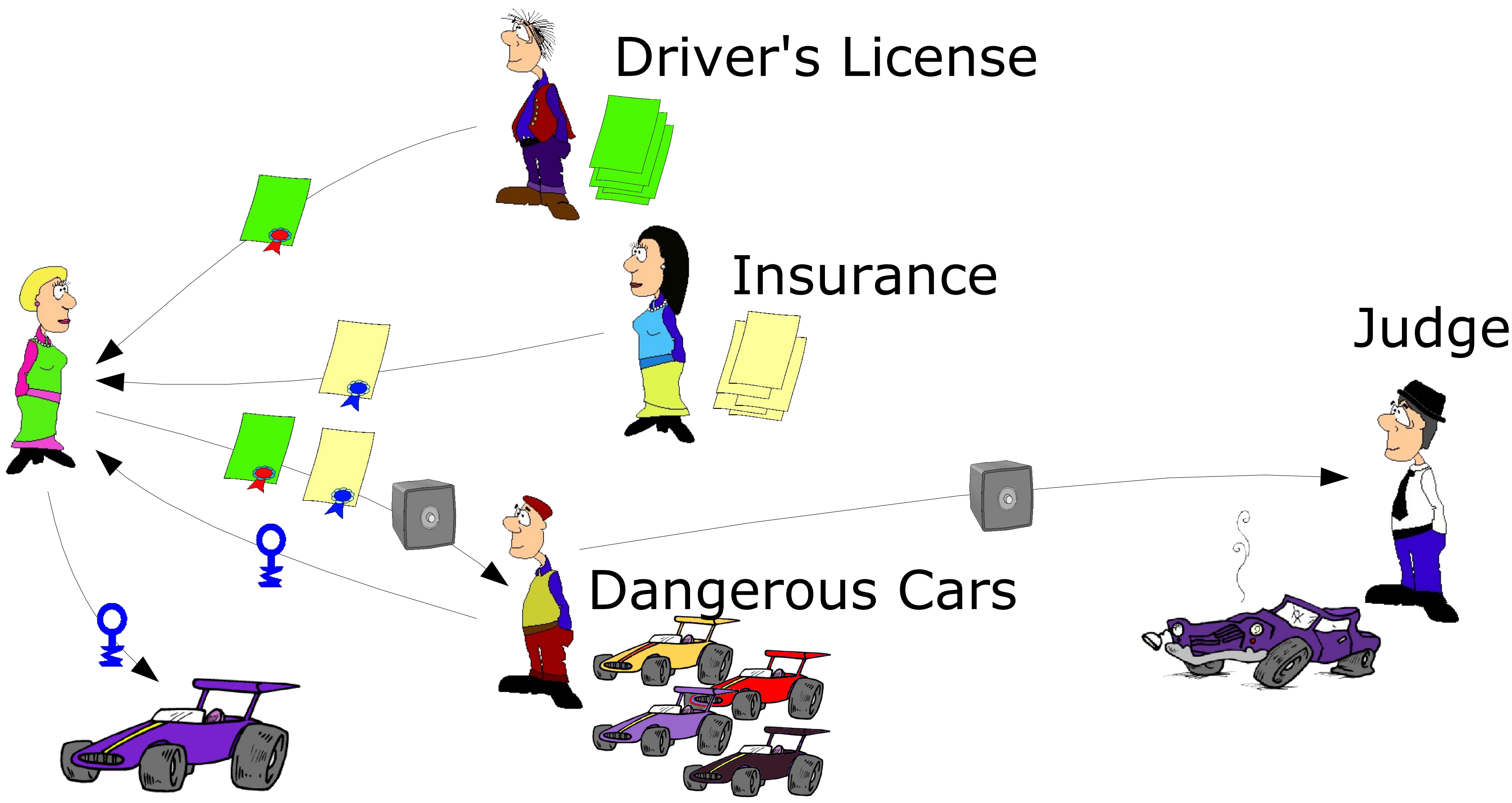
III. The Technical Bit

- Signature Scheme
- Commitments and Proof Protocols
- Encryption Scheme

The Problem: Pseudonym System [Chaum85]

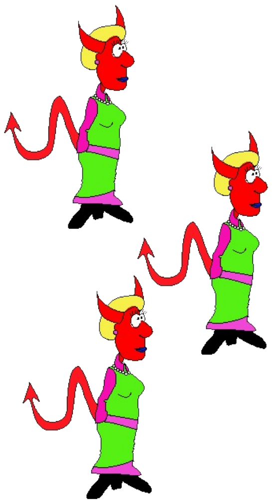


The Problem, Even Larger: Extended Pseudonym System



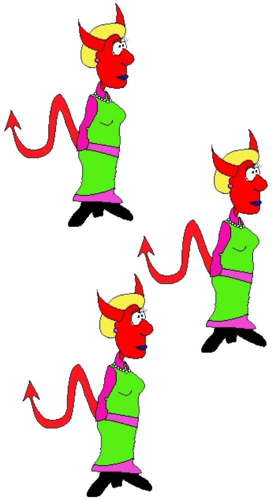
Basic Requirements of Pseudonym System

- Protection of user's privacy
  - anonymity
  - unlinkeability (multi-use)



- Unforgeability of credentials
- Consistency of credentials (no pooling)

Extra Requirements of Pseudonym System



- Sharing of credentials
- Anonymity revocation
  - local
  - global

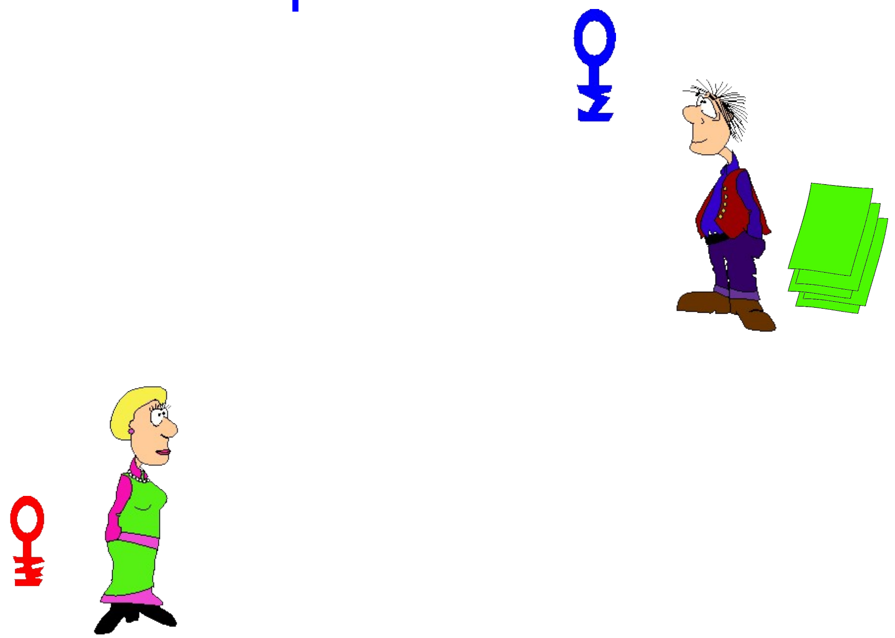
- Revocation of credentials
- Encoding of attributes
- One-show credential (e-cash)
  - off-line & on-line
- k-spendable credentials
- ......

Some History

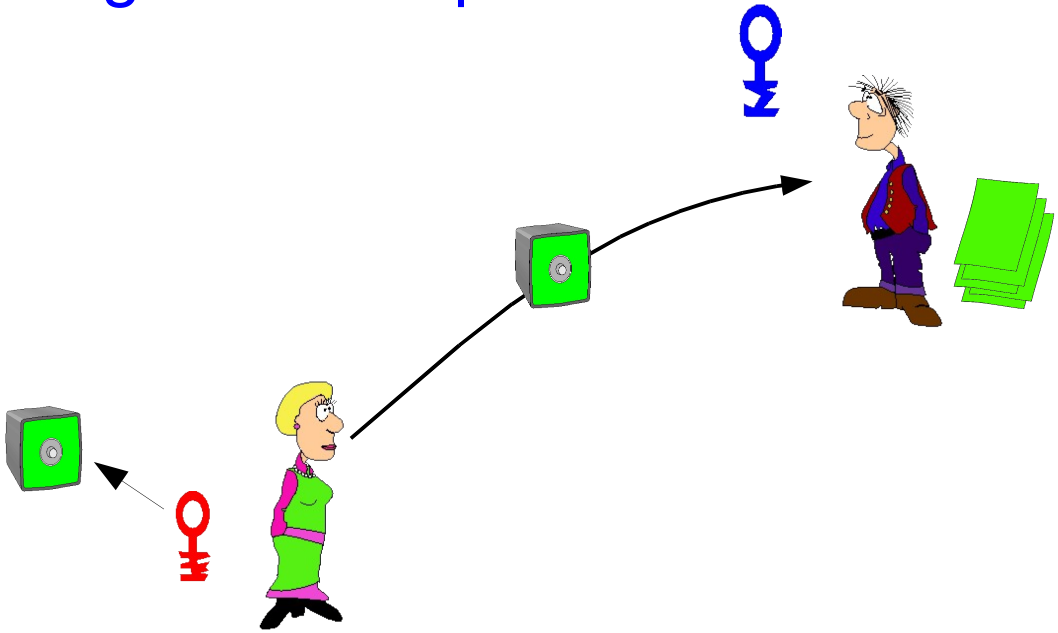
- Chaum ’85: introduced scenario
- Chaum & Evertse ’87: solution based on a semi-trusted party
- Damgård ’90: theoretical solution
- Brands ’95-’99: one-show credentials with different attributes
- LRSW ’99: practical solution for one-show credentials
- Camenisch-Lysyanskaya '00: efficient multi-show w/ attributes
- Verheulen '01: bi-linear map multi-show
- Camenisch-Lysyanskaya '04: Discrete log based.

Special cases: e-cash, group signatures, identity escrow

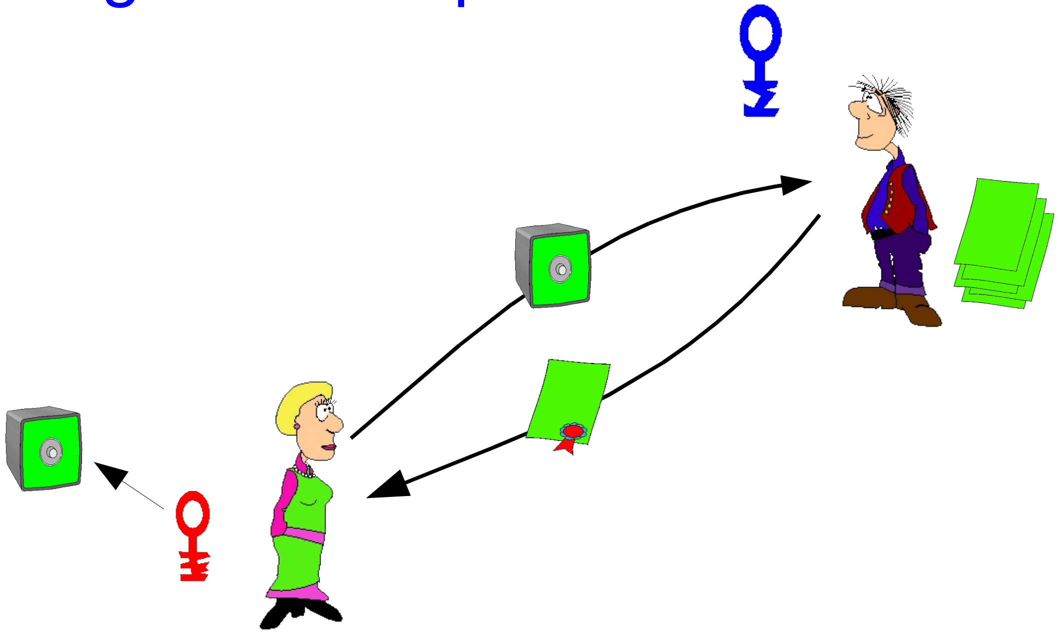
Proving Ownership Solution



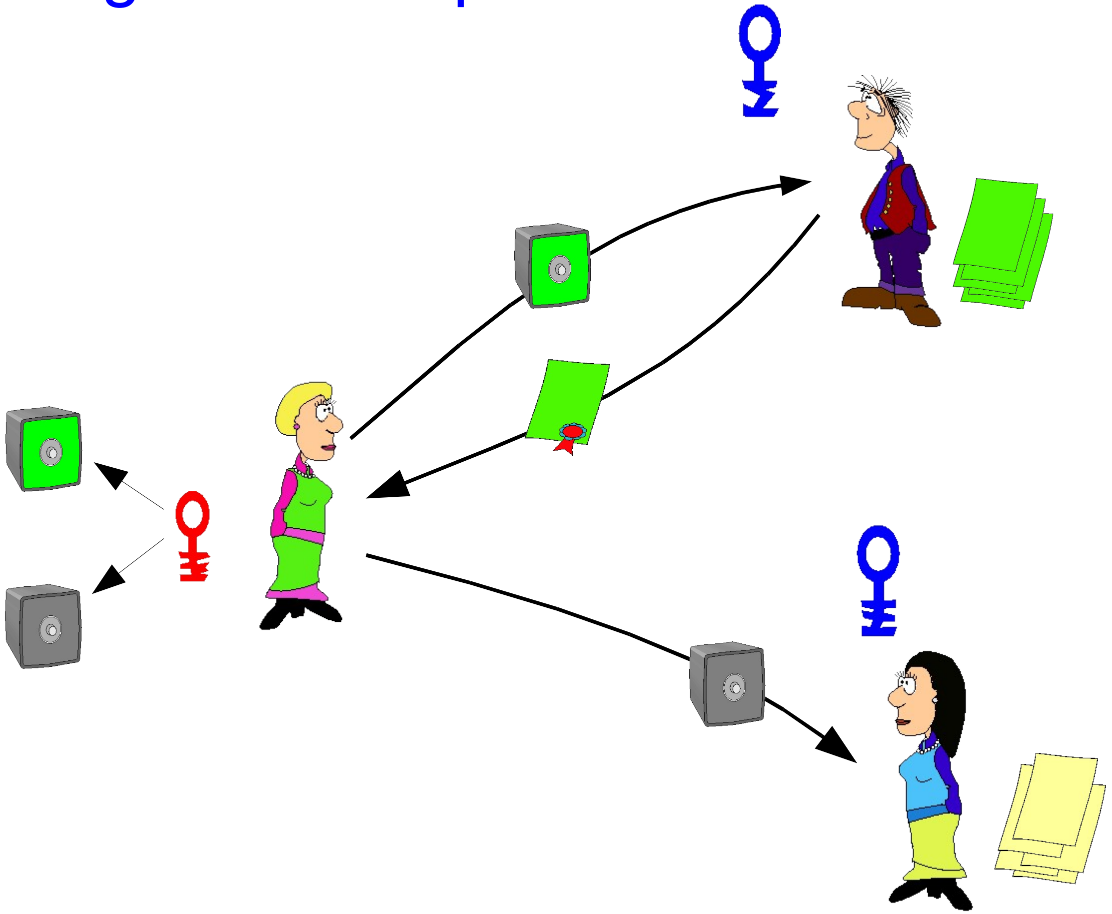
Proving Ownership Solution



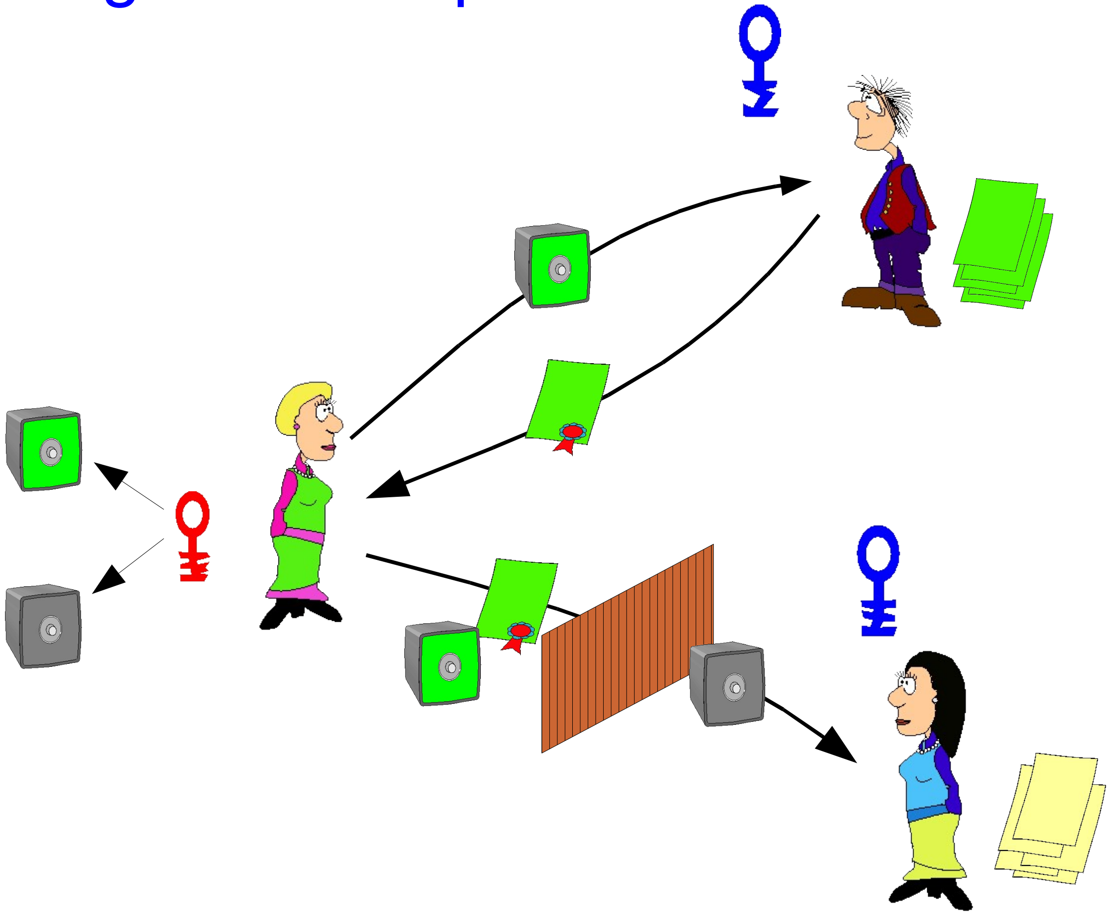
Proving Ownership Solution



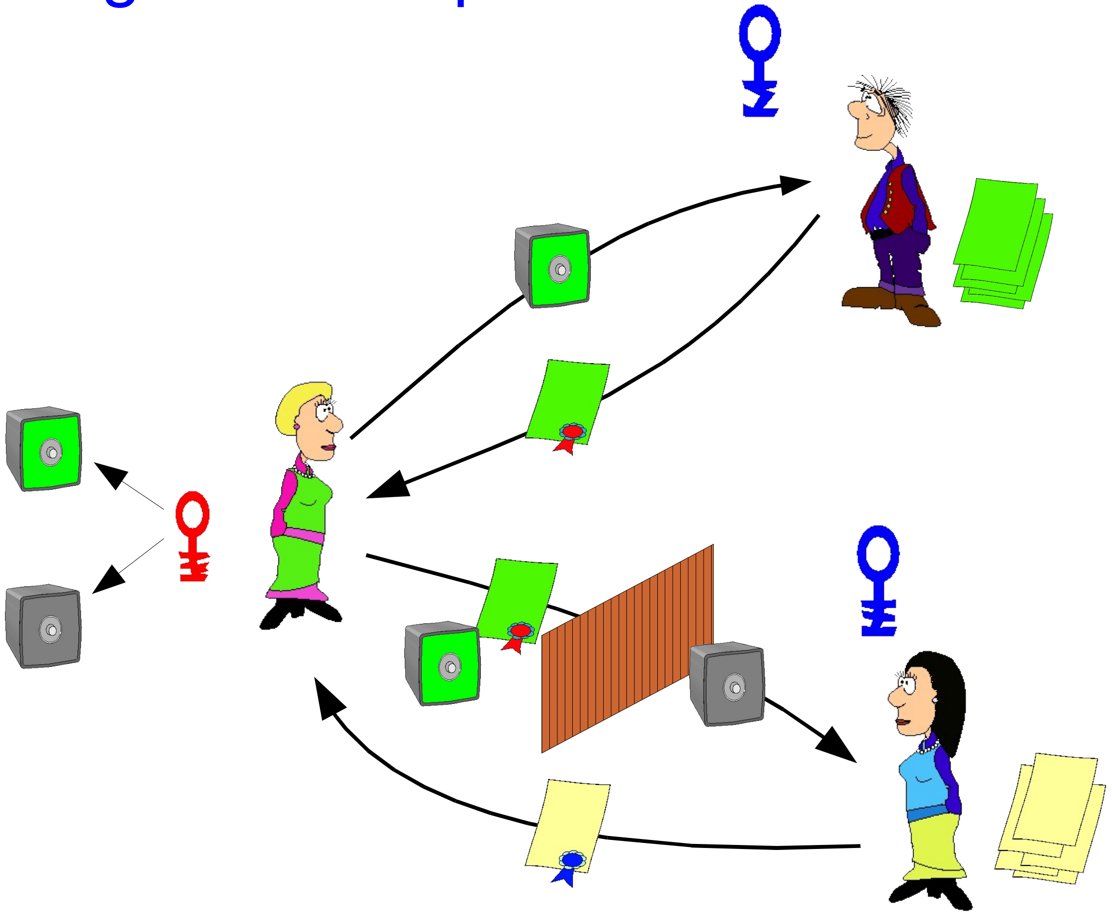
Proving Ownership Solution



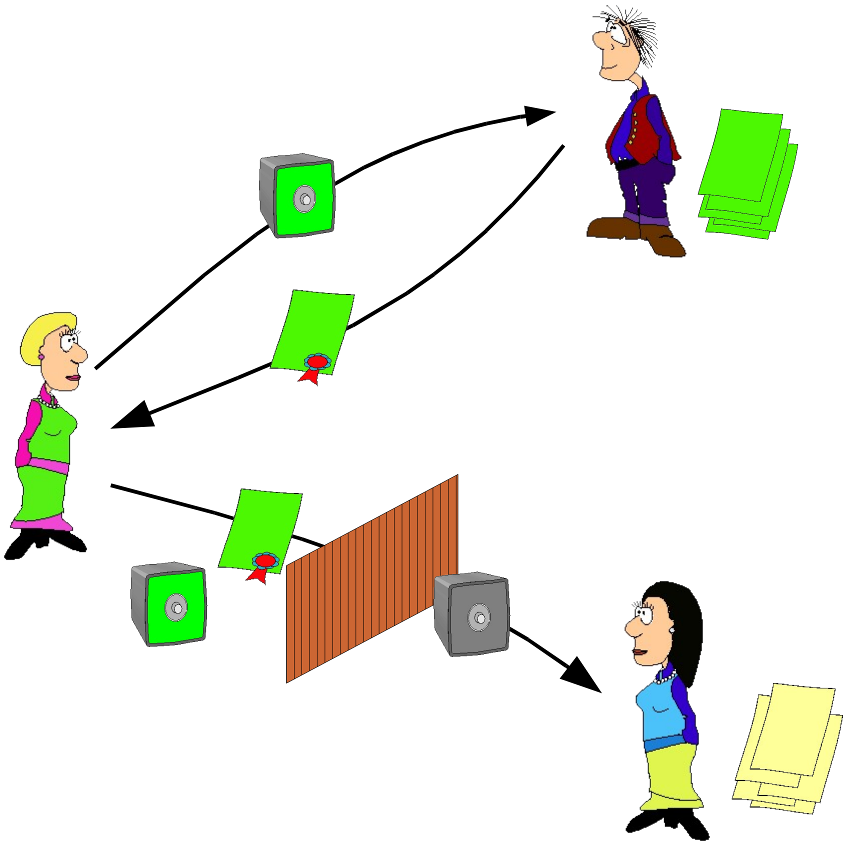
Proving Ownership Solution

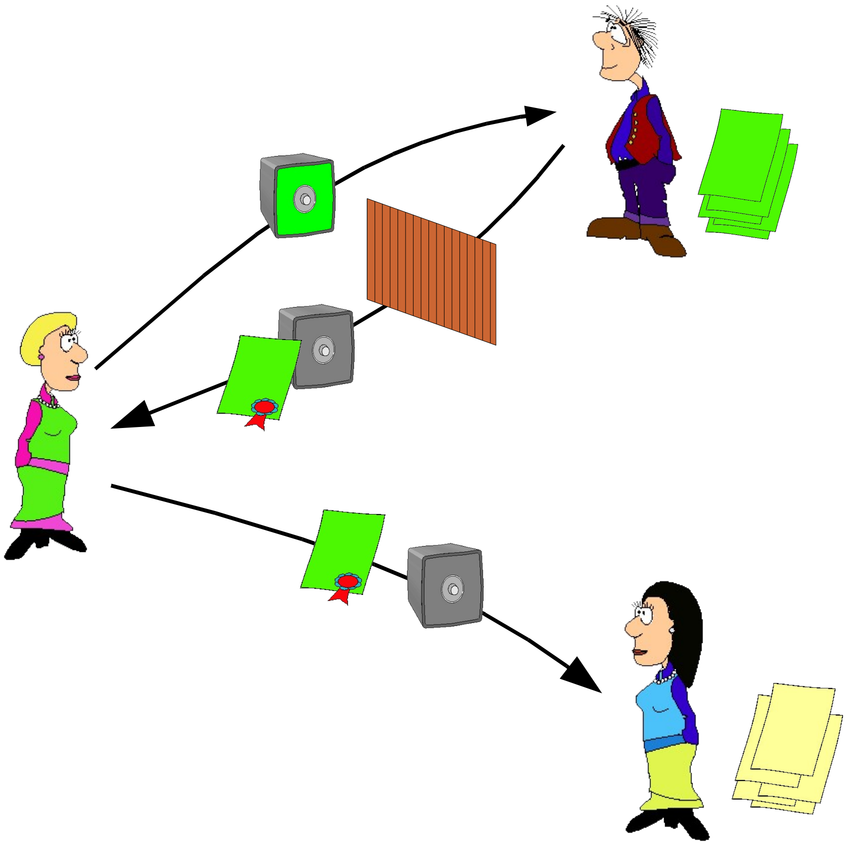


Proving Ownership Solution



Proving Ownership Vs. Using Blind Signatures

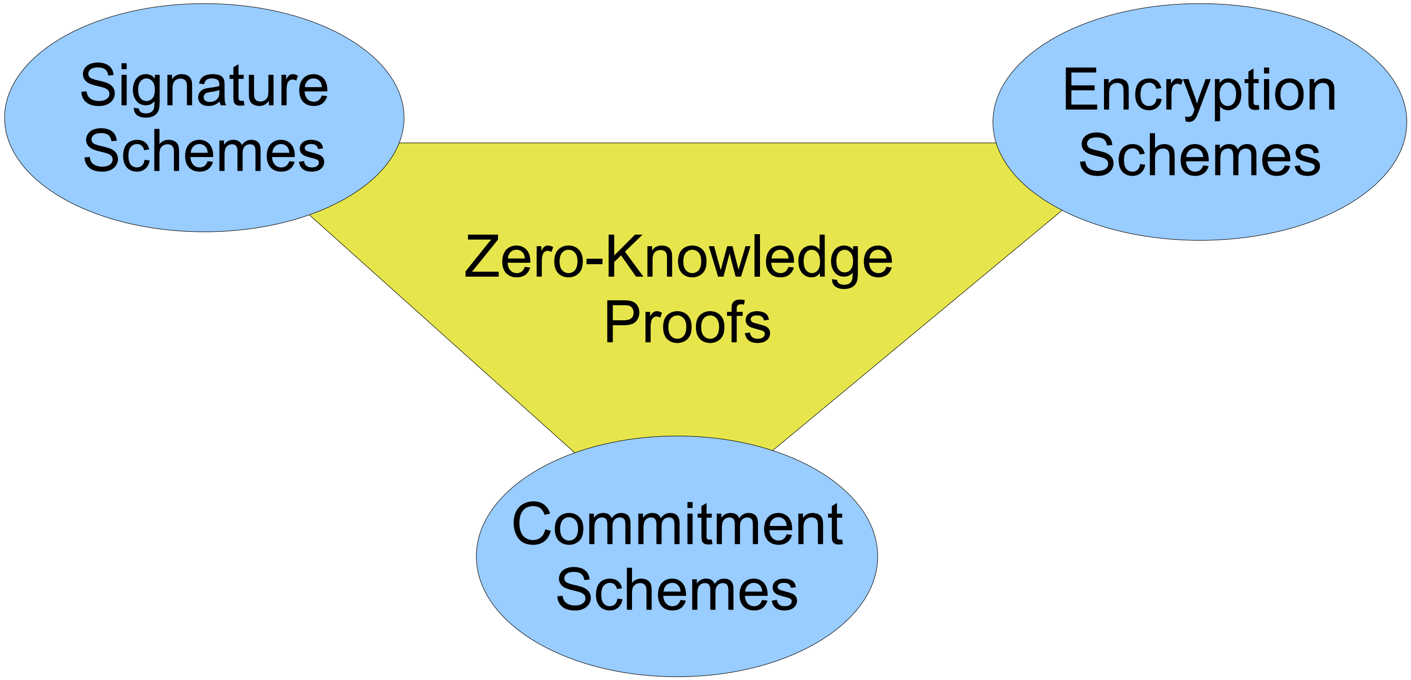




Certificates can be used *multiple* times!

Certificates can be used only *once*!

Required Technologies



..... challenge is to do all this efficiently!

Zero-Knowledge Proofs of Knowledge of Discrete Logarithms

[Schnorr '91,Chaum & Pedersen '92,....]

Given group $\langle g \rangle$ and element $y \in \langle g \rangle$.

Prove *knowledge* of $x = \log_g y$ such that verifier only learns y and g.

$PK\{(\alpha): \ y = g^{\alpha}\}$

Prover:		Verifier:
random r		
$t := g^r$	$\xrightarrow{\quad t \quad}$	
	$\xleftarrow{\quad c \quad}$	random c
$s := r - cx$	$\xrightarrow{\quad s \quad}$	
		$t = g^s y^c$

Zero Knowledge Proofs II

Non-interactive (Fiat-Shamir heuristic):

$$PK\{(\alpha): \; y = g^{\alpha}\}(m)$$

Logical combinations:

$$PK\{(\alpha,\beta): \; y = g^{\alpha} \wedge z = g^{\beta} \wedge u = g^{\beta}h^{\alpha}\}$$

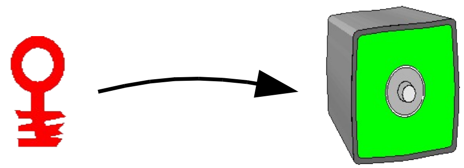
$$PK\{(\alpha,\beta): \; y = g^{\alpha} \vee z = g^{\beta}\}$$

Intervals and groups of different order (under SRSA):

$$PK\{(\alpha): \; y = g^{\alpha} \wedge \alpha \in [A,B]\}$$

$$PK\{(\alpha): \; y = g^{\alpha} \wedge \mathcal{z} = \mathcal{g}^{\alpha} \wedge \alpha \in [0,\min\{\mathrm{ord}(g),\mathrm{ord}(\mathcal{g})\}]\}$$

Commitment Schemes



Group $G = \langle g \rangle = \langle h \rangle$ of order q

To commit to element $x \in Z_q$:

- perfectly hiding, computationally binding (Pedersen):

  choose $r \in Z_q$ and compute $c = g^x h^r$

- computationally hiding, perfectly binding:

  choose $r \in Z_q$ and compute $c = (g^x h^r, g^r)$

To commit to integer $x \in Z$ (Damgård, Fujisaki):

- similarly, if order of G is not known, e.g., $G = QR_n$

The Strong RSA Assumption

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

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

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

Signature Scheme based on the SRSA Assumption I

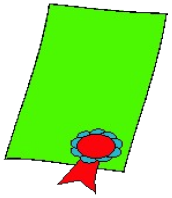
Public key of signer: RSA modulus n and a_i, b, $d \in QR_n$,

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

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

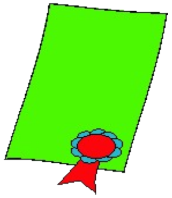


- signature is (c,e,s)

Signature Scheme based on the SRSA Assumption II

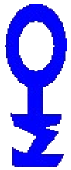
A signature (c,e,s) on messages $m1, \ldots, mk$ is valid iff:

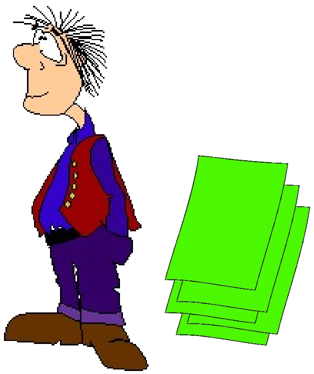
- $m1, \ldots, mk \in \{0,1\}^{\ell}$:
- $e > 2^{\ell}$
- $d = a_1^{m1} \cdot \ldots \cdot a_k^{mk} \; b^s \; c^e \bmod n$

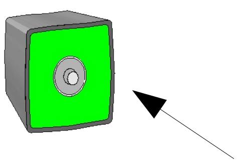


Theorem: *Signature scheme is secure against adaptively chosen message attacks under SRSA assumption.*

Getting a Signature on a Secret Message

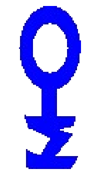


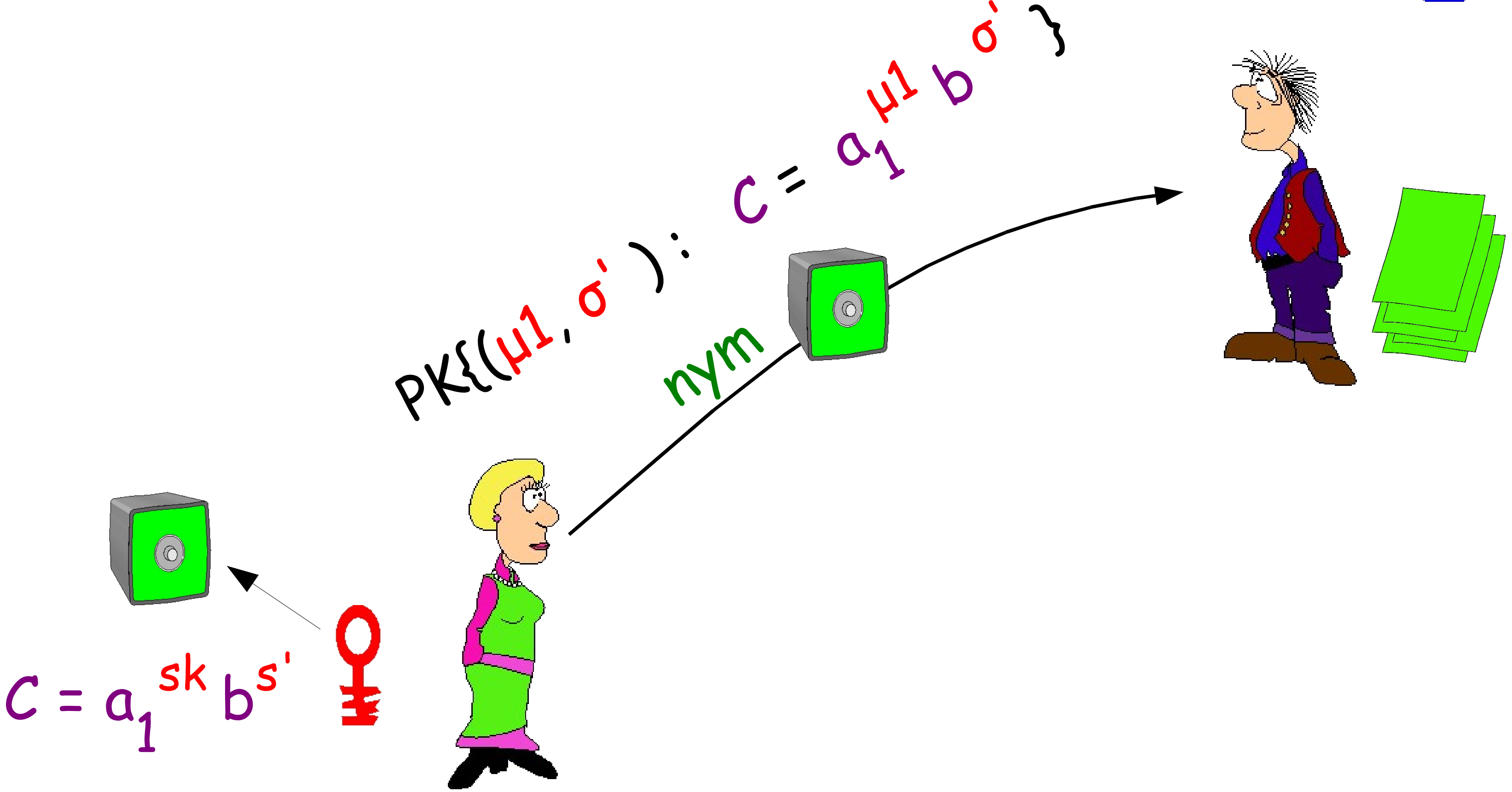




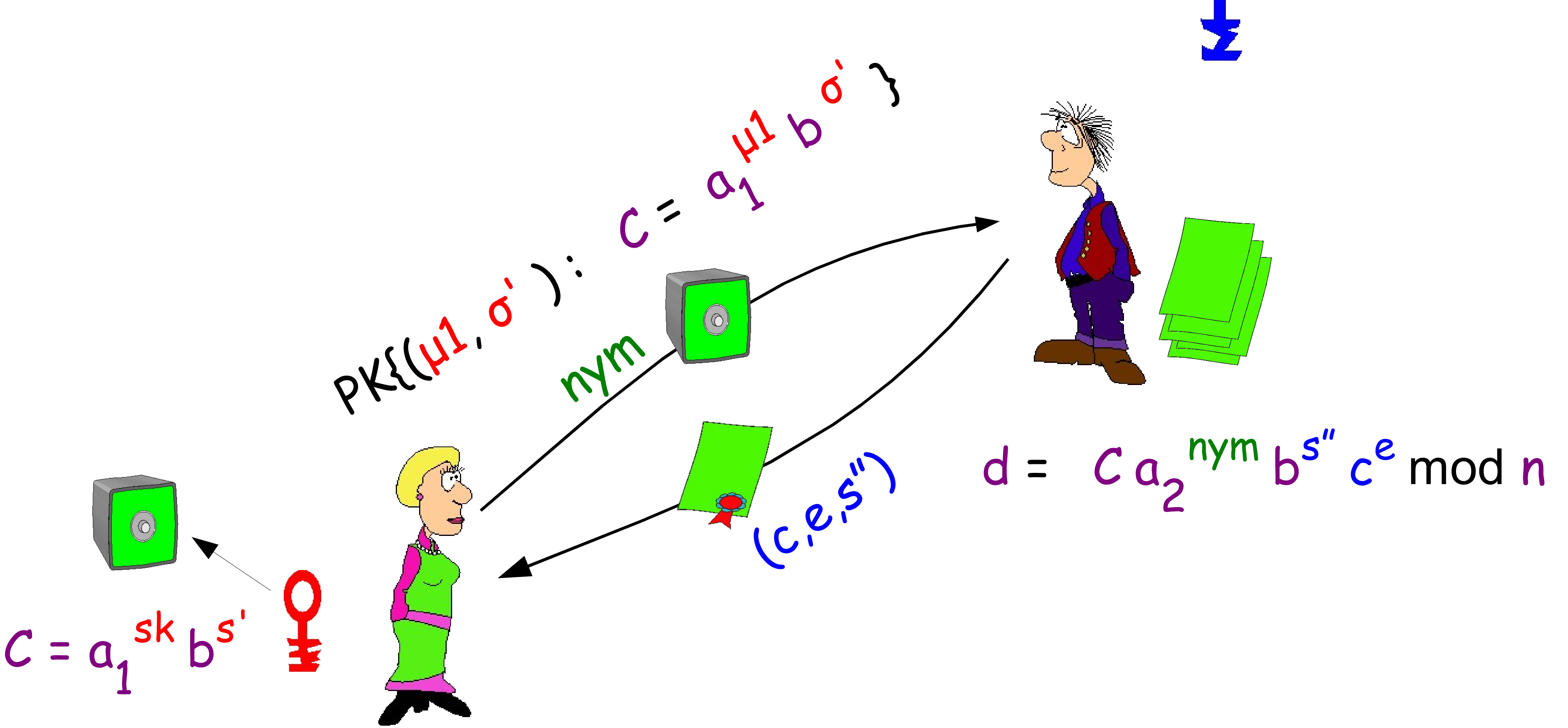
$C = a_1^{sk} b^{s'}$

Getting a Signature on a Secret Message



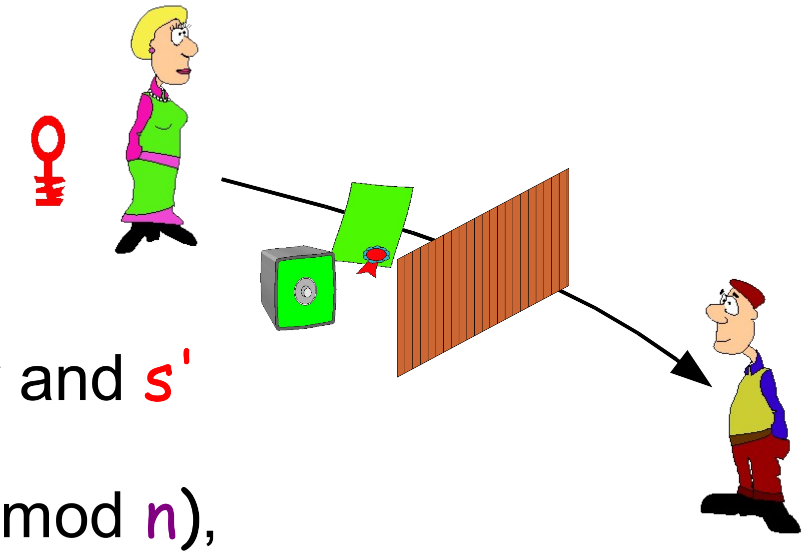


Getting a Signature on a Secret Message



$$d = a_1^{sk} a_2^{nym} b^{s'' + s'} c^e \pmod{n}$$

Proof of Knowledge of a Signature



Observe:

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

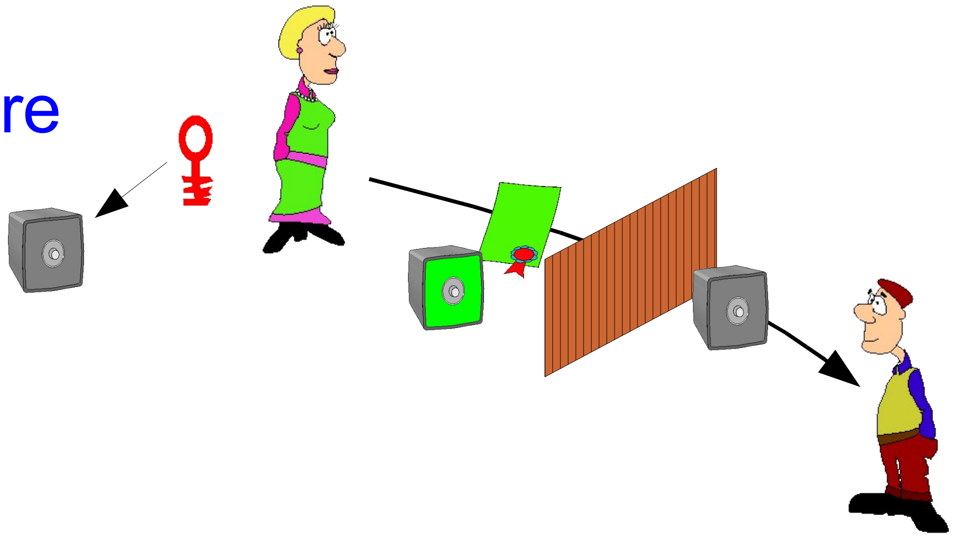
  i.e., (c', e, s^*) is a also a valid signature!

Therefore, to prove knowledge of signature on some m

- provide c'
- $PK\{(\varepsilon, \mu 1, \ldots, \mu k, \sigma) : \quad d := c'^{\varepsilon} a_1^{\mu 1} \cdot \ldots \cdot a_k^{\mu k} b^{\sigma}$

  $\wedge \quad \mu 1 \in \{0,1\}^{\ell} \quad \wedge \quad \varepsilon \in 2^{\ell+1} \pm \{0,1\}^{\ell} \quad \}$

Proof of Knowledge of a Signature



Using second Commitment

– $C = a_1^{sk} b^{s*}$

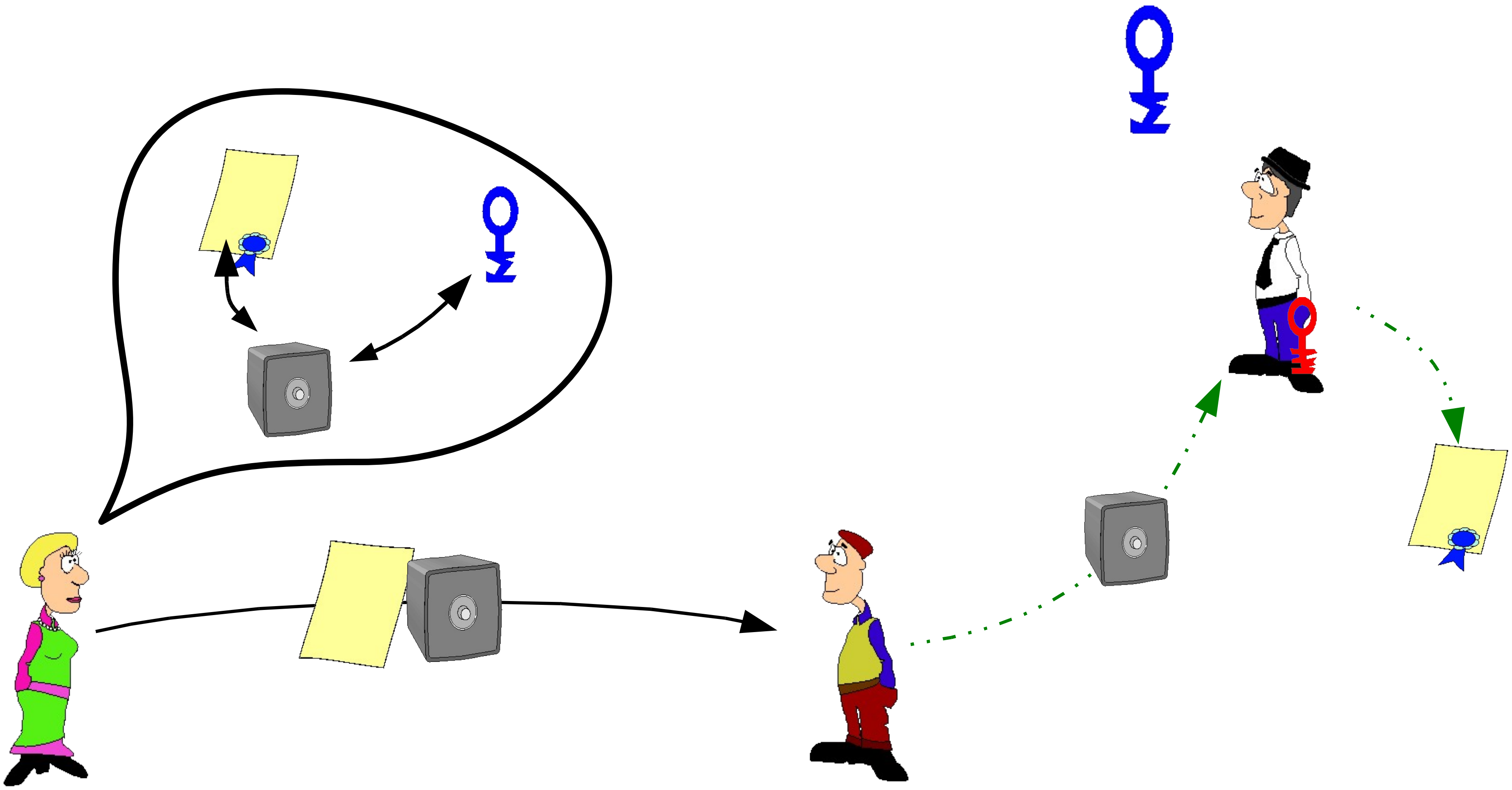
To prove knowledge of signature on some m

– provide c'

– PK{(ε, μ1, ..., μk, σ, σ*,) :

$$C = a_1^{\mu 1} b^{\sigma *} \quad \wedge \quad d := c'^{\varepsilon} a_1^{\mu 1} \cdot \ldots \cdot a_k^{\mu k} b^{\sigma} \}$$

Verifiable Encryption



The Decision Composite Residuosity Assumption

The DCR Problem: *Given n and x, decide whether or not*

$$x \in (Z^*_{n^2})^n \; .$$

- Introduced by Paillier '99.
- If $n = (2p'+1)(2q'+1)$ then $Z^*_{n^2} = Z_2 \times Z_2 \times Z_n \times Z_{p'q'}$.
- $(1+n)^u = (1+un) \bmod n^2$.

An Encryption Scheme

Public Key: n and $g, y_1, y_2, y_3 \in \langle (g')^{2n} \rangle$, where $g' \in Z^*_{n^2}$,

Secret Key: $x_i = \log y_i$

Encryption message $m \in [0,n]$ under label L:

- choose $r \in [0,n/4]$
- $u := g^r$, $e := y_1^r (1+n)^m$, $v :=$ abs$(y_2 y_3^{H(u,e,L)})^r$
- output (u,e,v).

where abs() maps ($a \bmod n^2$) to ($n^2 - a \bmod n^2$) if $a > n^2/2$, and ($a \bmod n^2$) otherwise, where $0 < a < n^2$.

An Encryption Scheme

Decryption of ciphertext (u,e,v) under label L:

- verify $v = \mathrm{abs}(v)$ and $u^{2(x_2 + H(u,e,L)x_3)} = v^2$.
- $\hat{c} := (e/u^{x_1})^{2t}$ where $t = 2^{-1} \bmod n$,
- if $n \mid (\hat{c}-1)$ output $m := (\hat{c}-1)/n$, otherwise output $\perp$

Intuition: remember $(1+n)^a = 1+an \pmod{n^2}$

so $(e/u^{x_1}) = y_1^r (1+n)^m / (g^r)^{x_1} = (1+n)^m = 1+mn$)

Theorem: *Encryption scheme is secure against adaptively chosen ciphertext attacks under DCR assumption.*

Verifiable Encryption of a Discrete Logarithm

Let $d = a_1^{sk} a_2^{nym}\ b^s\ c^e \pmod n$ be a driver's license

and (u,v,e) be an encryption of nym.

To prove that (u,v,e) indeed encrypts m:

$PK\{(\varepsilon, \mu 1, \mu 2, \rho, \sigma):$

$$d := c'^{\varepsilon}\ a_1^{\mu 1}\ a_2^{\mu 2}\ b^{\sigma} \ \wedge\ \mu 1, \mu 2 \in \{0,1\}^{\ell} \quad \wedge$$

$$u^2 = g^{2\rho} \wedge\ e^2 = y_1^{2\rho}\ (1+n)^{2\mu 2} \wedge\ v^2 = (y_2 y_3^{H(u,e,L)})^{2\rho} \quad \}$$

Conclusion & Outlook

- Efficient Anonymous Credentials and more!
- TCG TPM V1.2 will have some of this

  Was known in theory; soon your computer will have it.

- EU Project PRIME will have all of this

  www.prime-project.eu.org

- Plans:
  - Open source
  - Lots of more research :-)

Thanks for your attention!