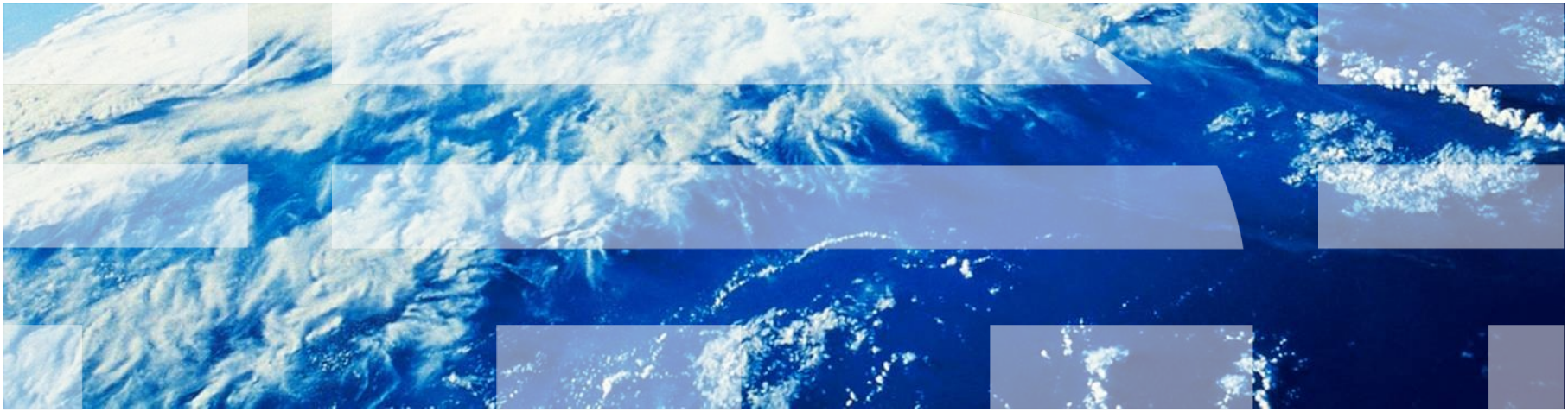
Jan Camenisch and Gregory Neven, IBM Research – Zurich
IFIP Summer School, Trento, Italy, September 7, 2011
(Credit for slides to Anja Lehmann, IBM Research - Zurich)

# Cryptography Tutorial

## Part I – Credential System Overview



# Outline

## Part I – Overview of Credential Systems

- Classical Identification
- Anonymous Credentials
  - Basic Functionality
  - Idemix vs. U-Prove
  - Extended Functionality

## Part II – Crypto & Math Basics

- Zero-Knowledge Proofs
- Basics in Number Theory


© 2011 IBM Corporation

# Introduction

credential / certificate

- signed list of attribute-value pairs

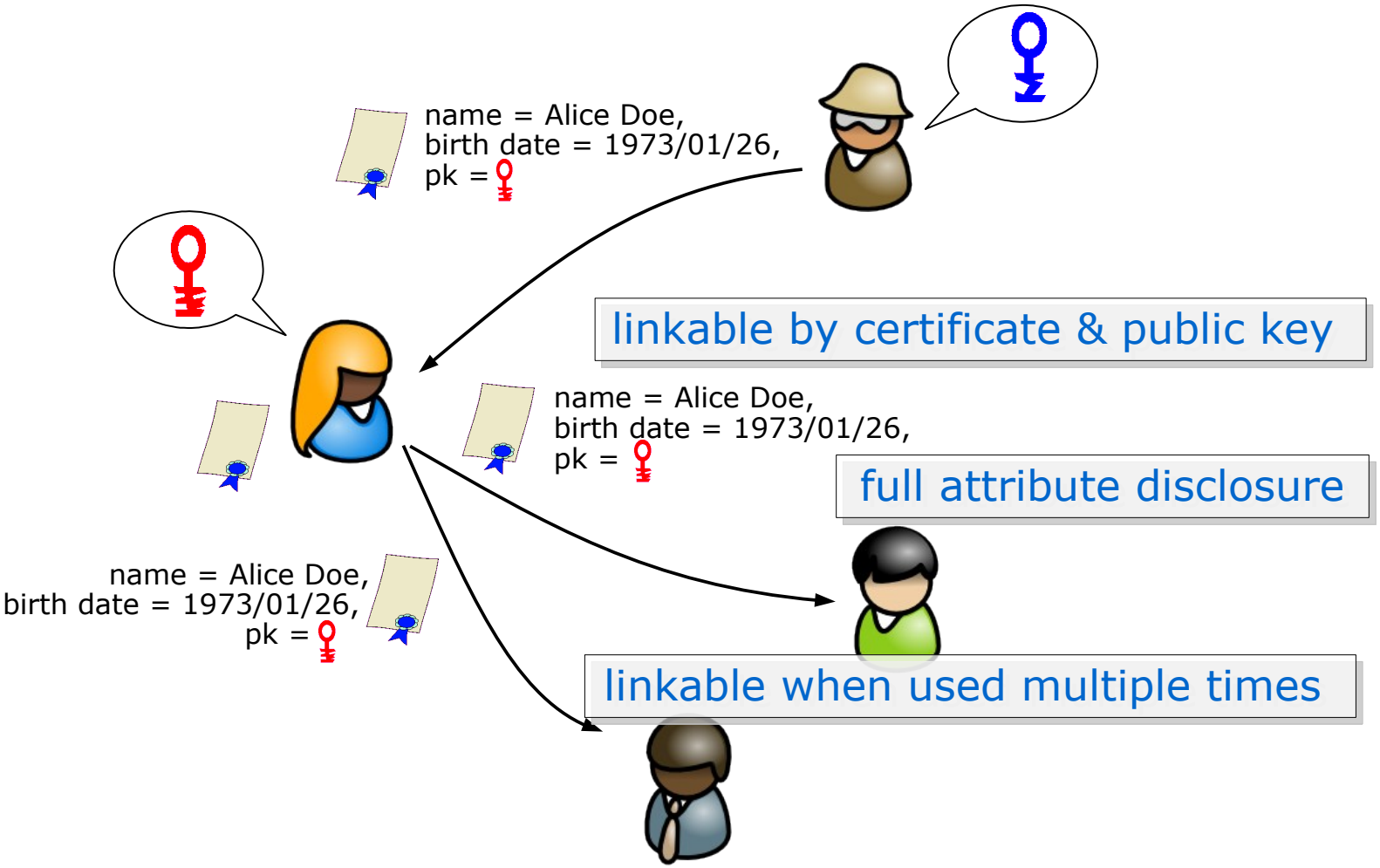





© 2011 IBM Corporation

# Standard Public-Key Certificates

e.g., X.509 certificates



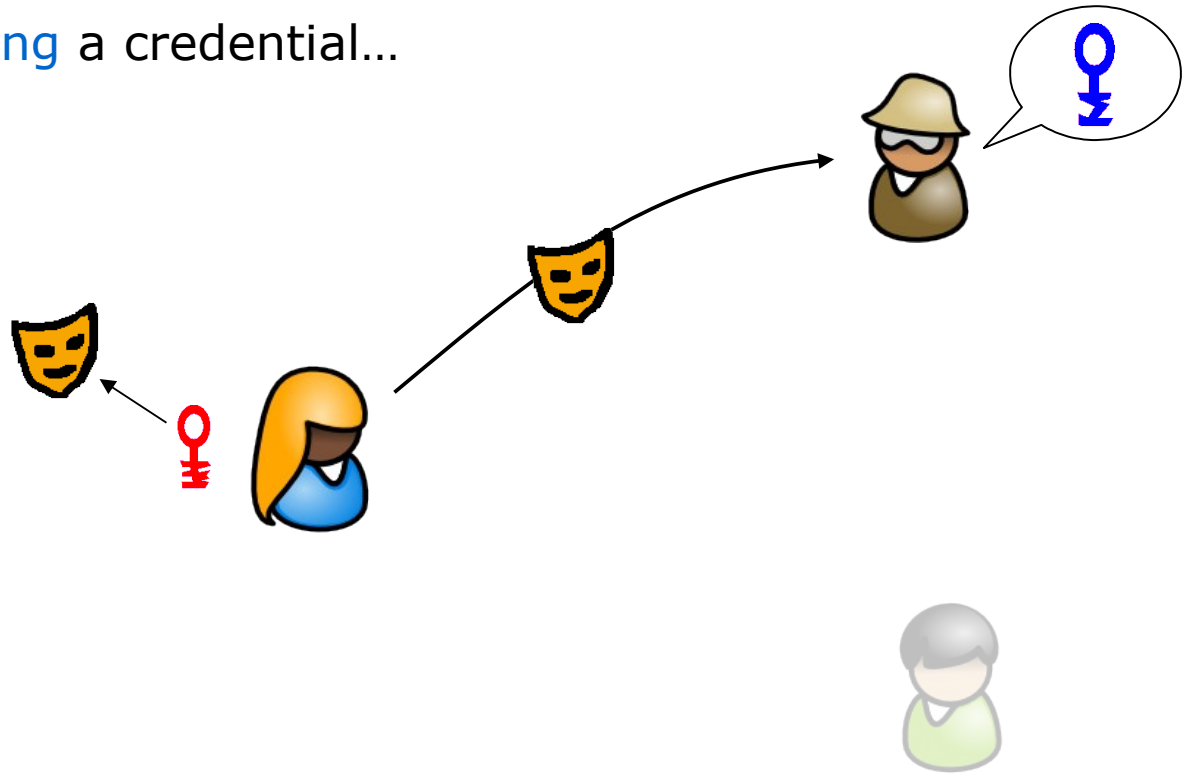



© 2011 IBM Corporation

# Anonymous Credentials

e.g., Identity Mixer, U-Prove

Obtaining a credential…



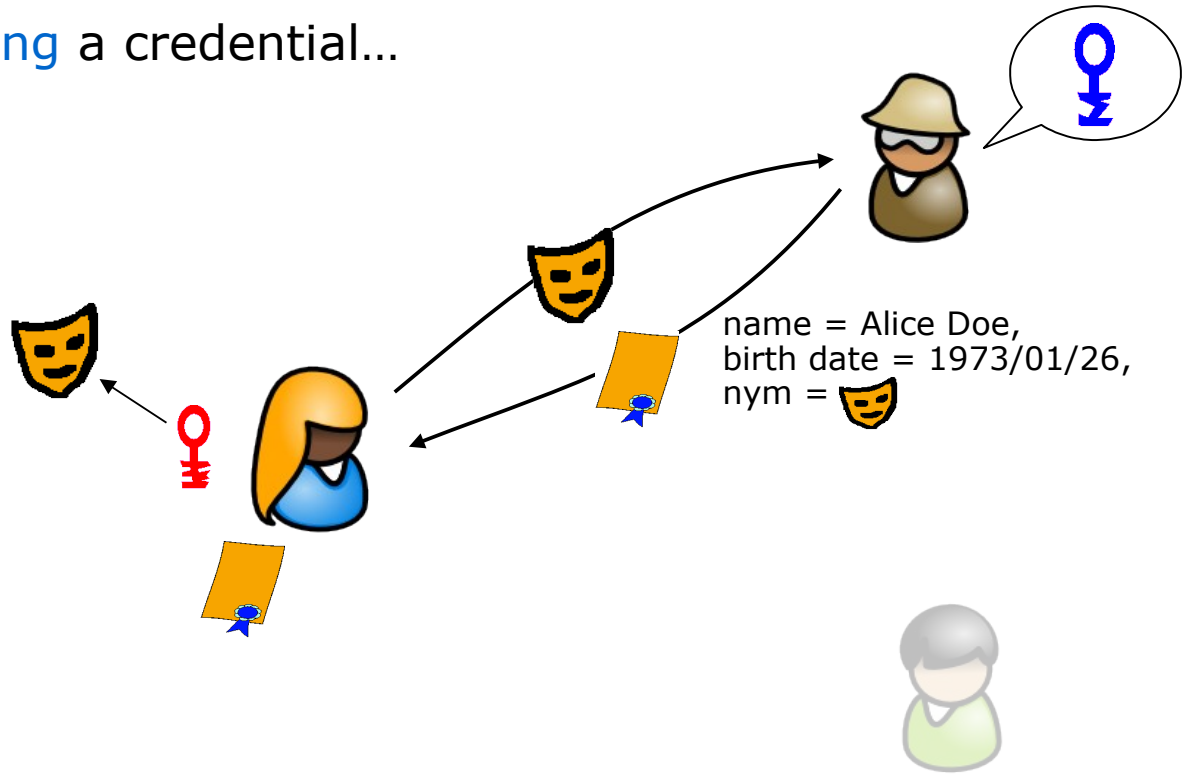


© 2011 IBM Corporation

# Anonymous Credentials

e.g., Identity Mixer, U-Prove

Obtaining a credential…



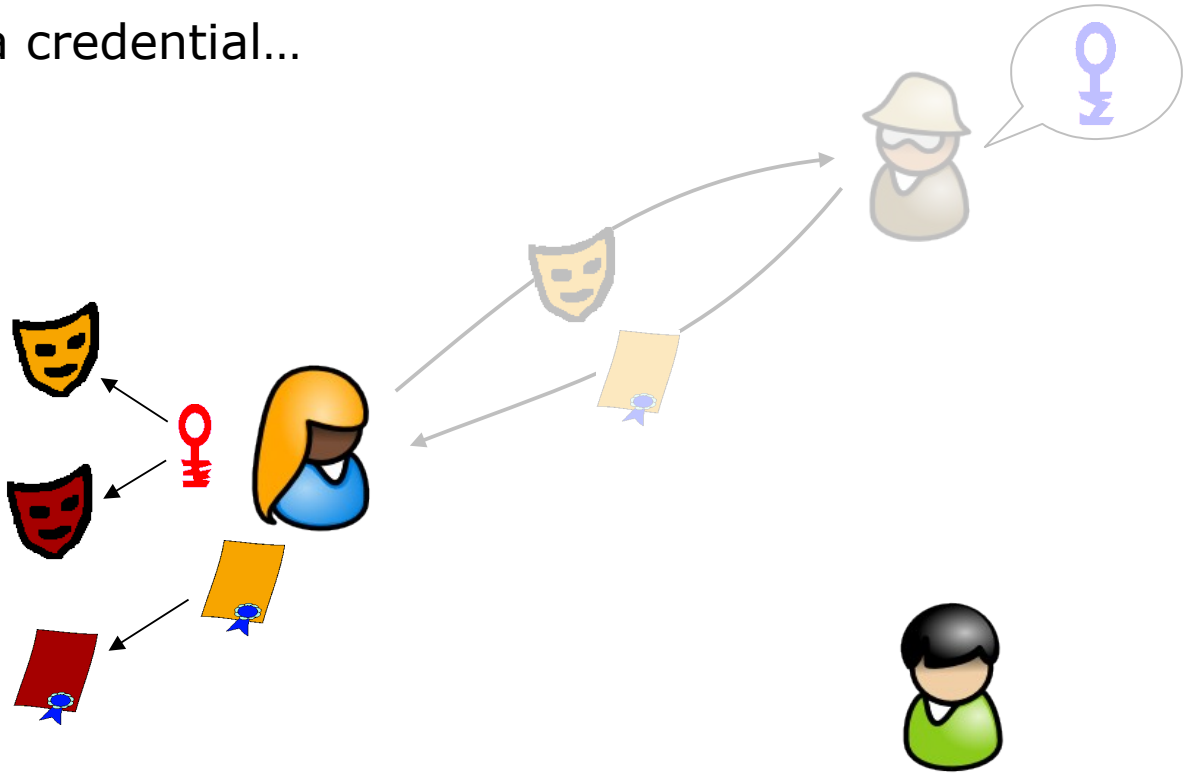


© 2011 IBM Corporation

# Anonymous Credentials

e.g., Identity Mixer, U-Prove

Using a credential…



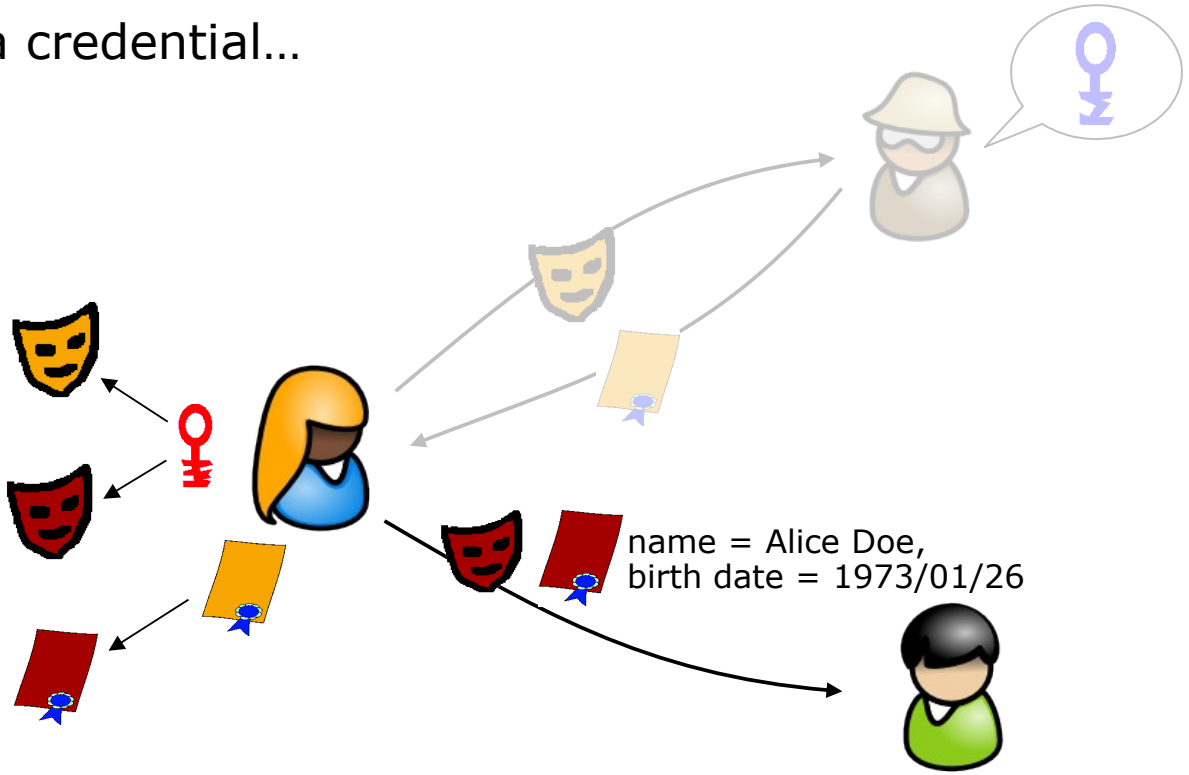


© 2011 IBM Corporation

# Anonymous Credentials

e.g., Identity Mixer, U-Prove

Using a credential…



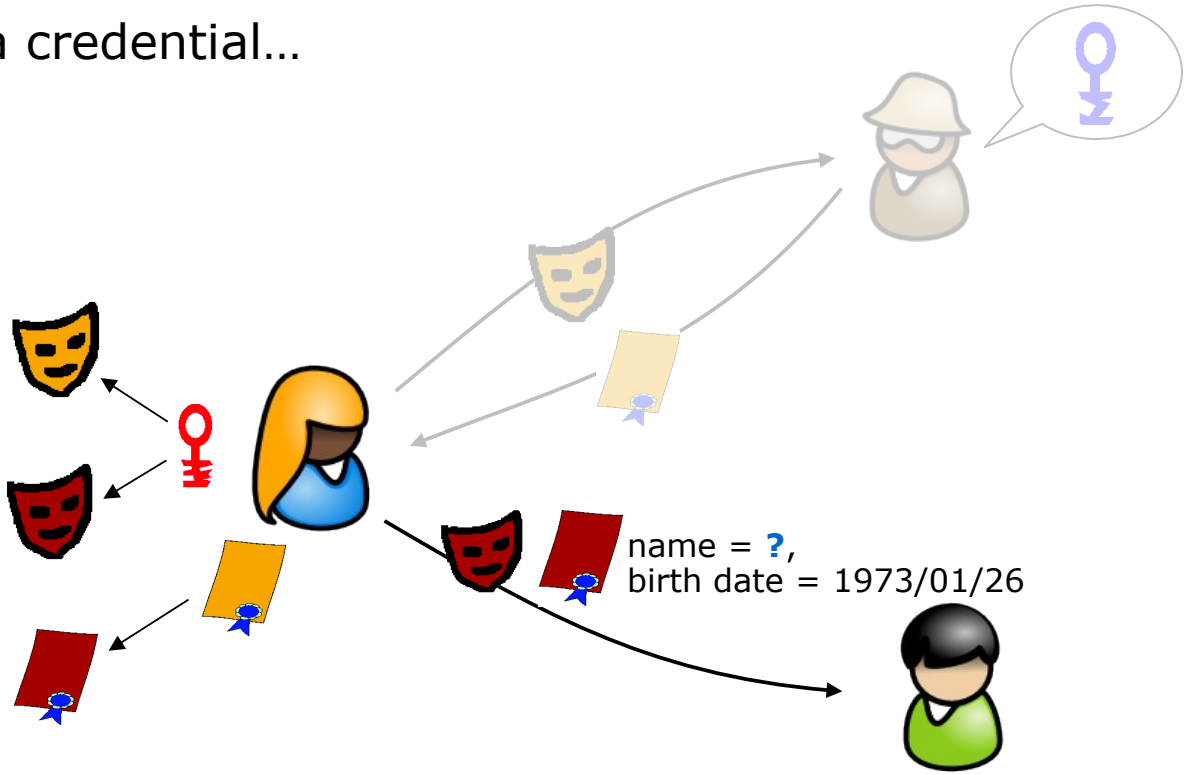

issuance and showing are unlinkable


© 2011 IBM Corporation

# Anonymous Credentials

e.g., Identity Mixer, U-Prove

Using a credential…



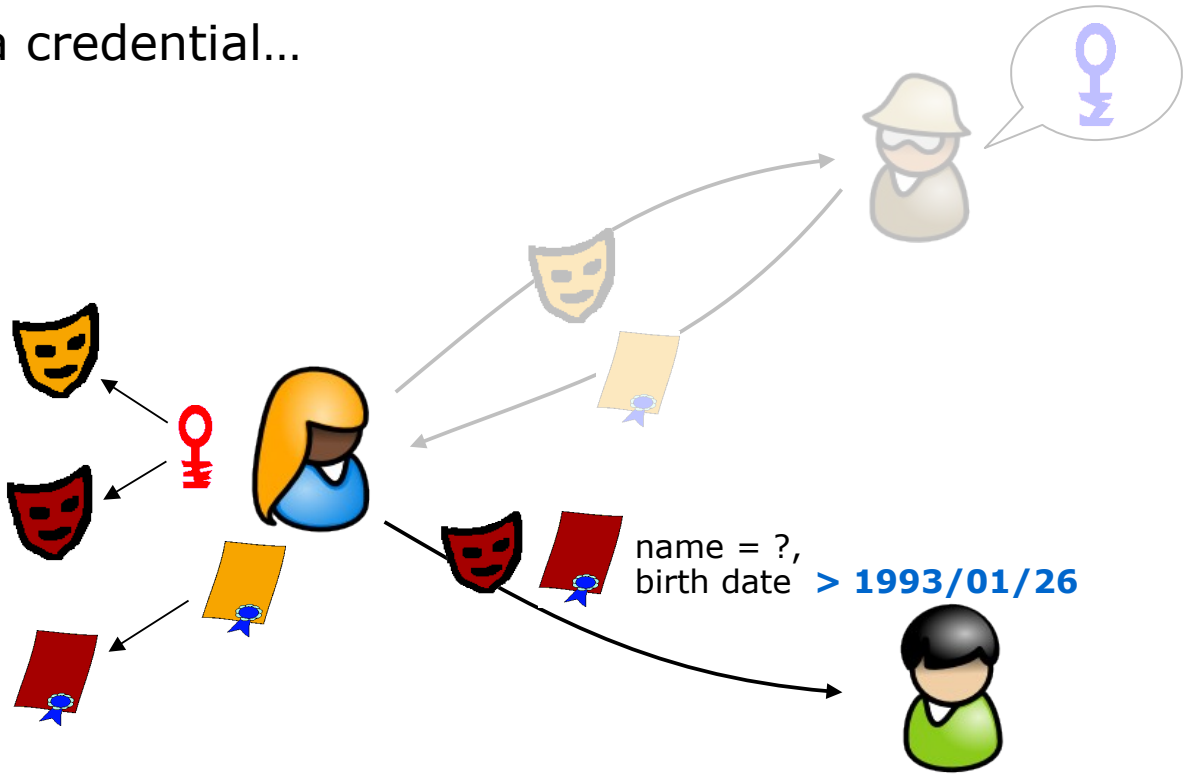

selective attribute disclosure


© 2011 IBM Corporation

# Anonymous Credentials

e.g., Identity Mixer, U-Prove

Using a credential…



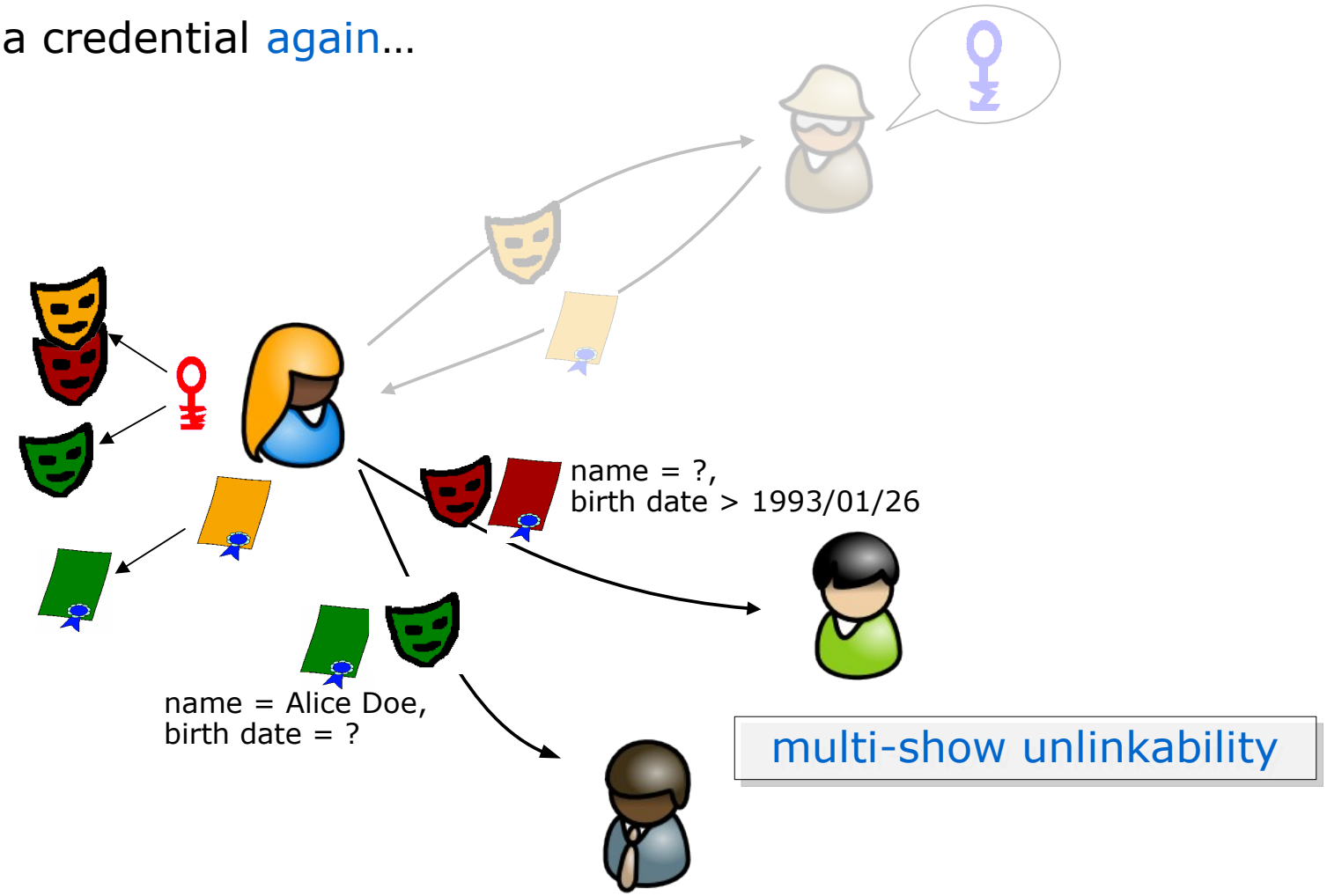

attribute predicate disclosure


© 2011 IBM Corporation

# Anonymous Credentials

e.g., Identity Mixer, U-Prove

Using a credential again…



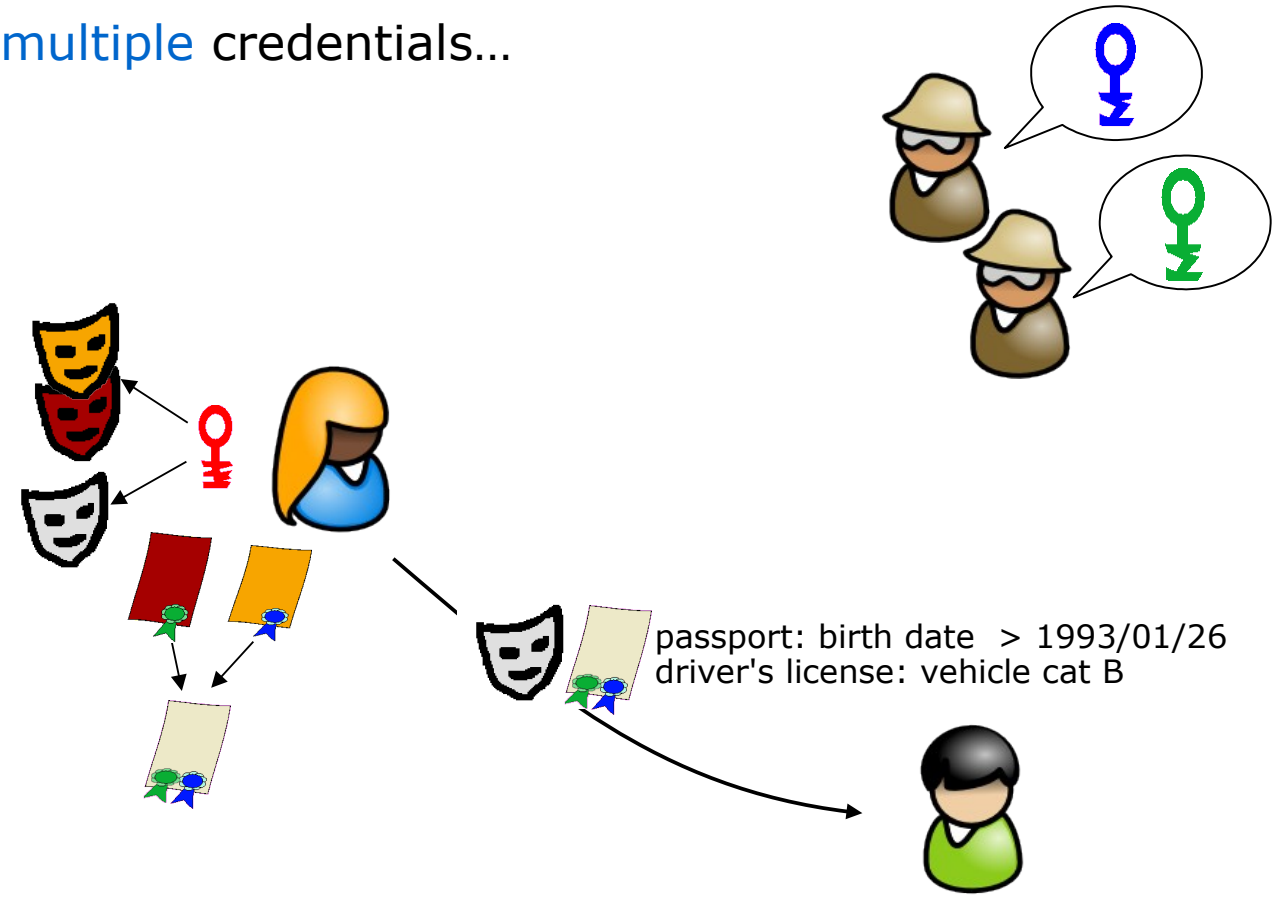


© 2011 IBM Corporation

# Anonymous Credentials

e.g., Identity Mixer, U-Prove

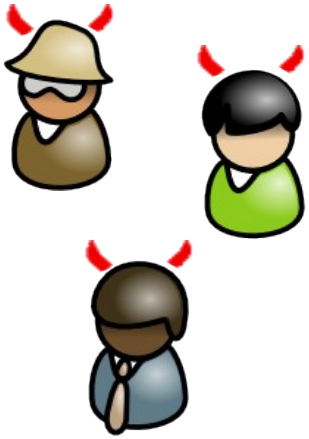
Using multiple credentials…





© 2011 IBM Corporation

# Anonymous Credentials - Basic Functionality



- Protection of user's privacy
  - anonymity
  - unlinkability (multi-use)
  - selective disclosure

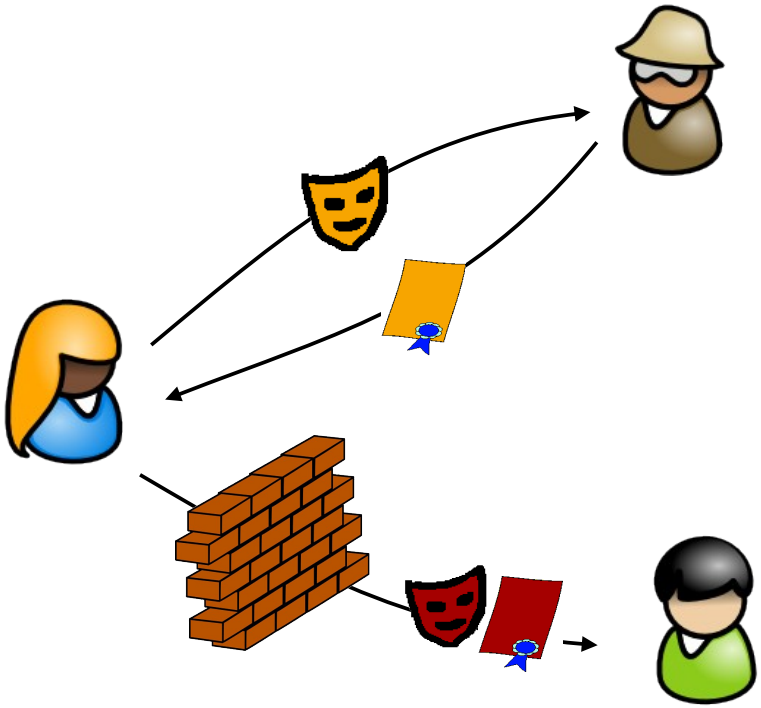


- Unforgeability of credentials
- Consistency of credentials (no sharing)


© 2011 IBM Corporation

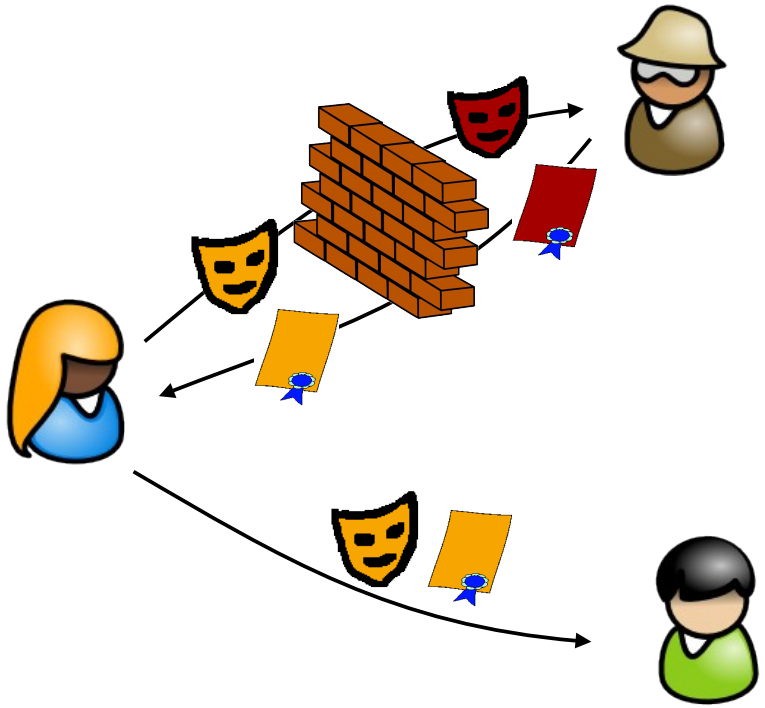
# Anonymous Credentials - Two Approaches

## Zero-Knowledge Proofs



Idemix

## Blind Signatures



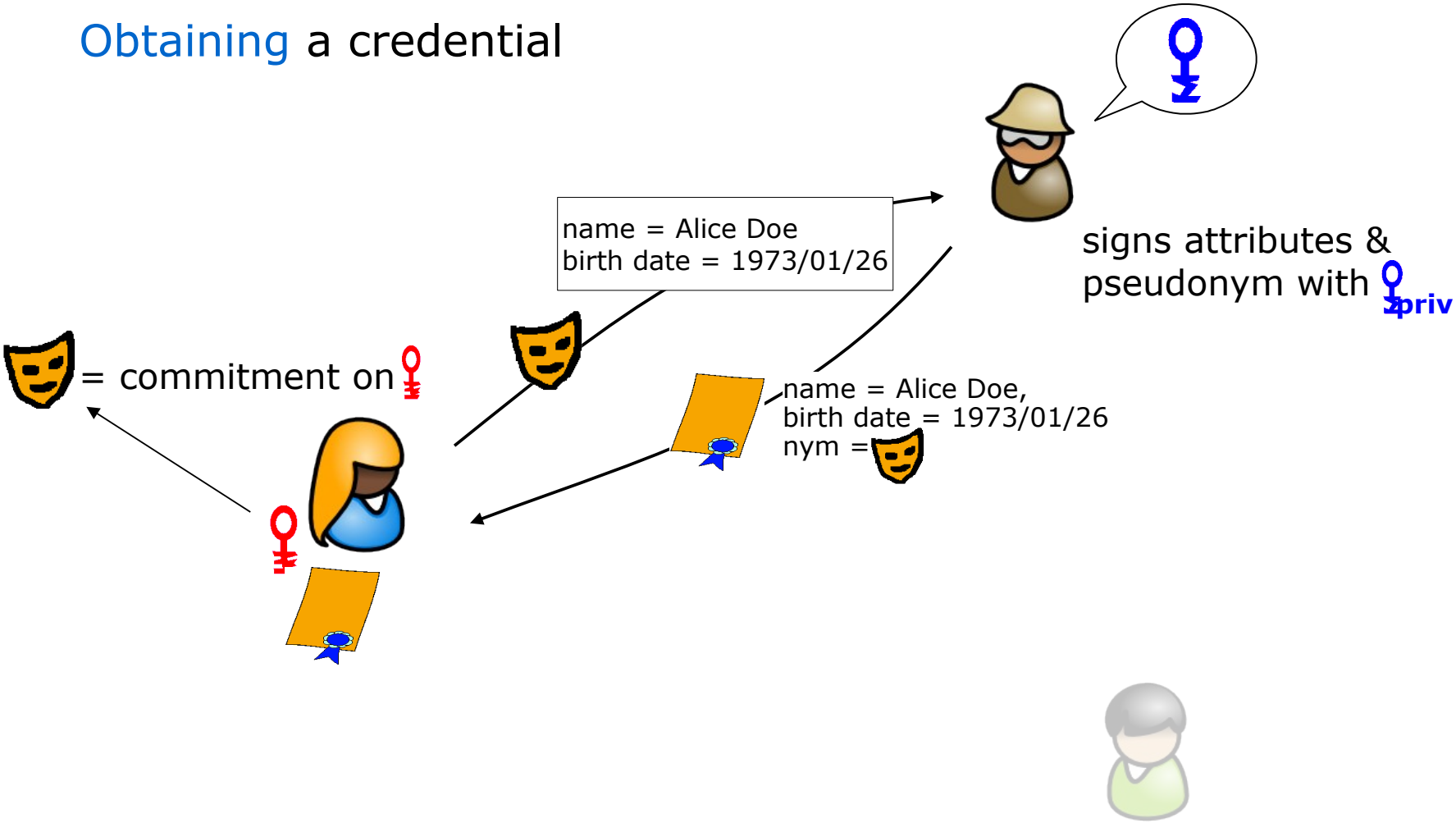
U-Prove



© 2011 IBM Corporation


Identity Mixer

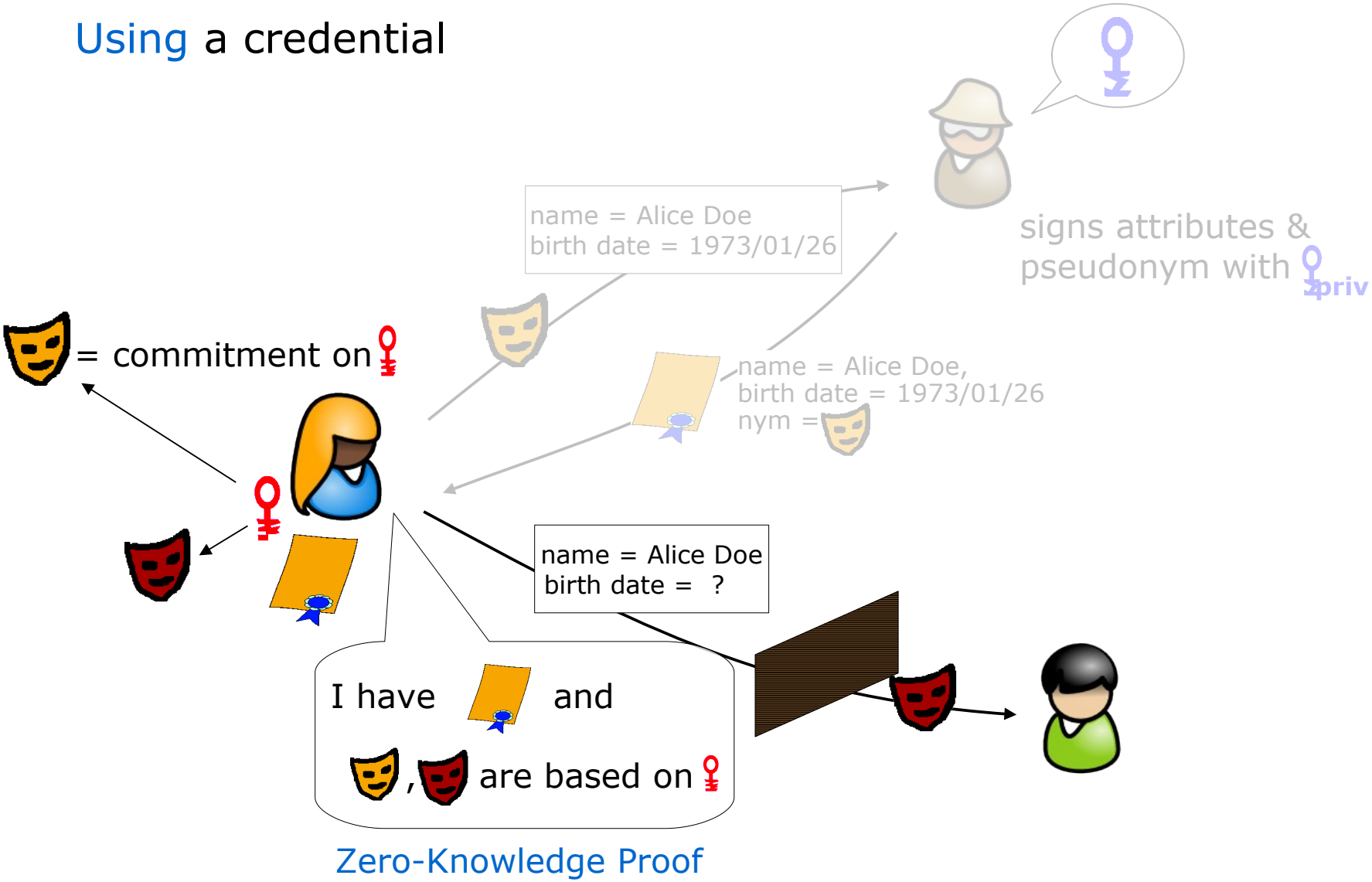
## Obtaining a credential





© 2011 IBM Corporation

## Using a credential



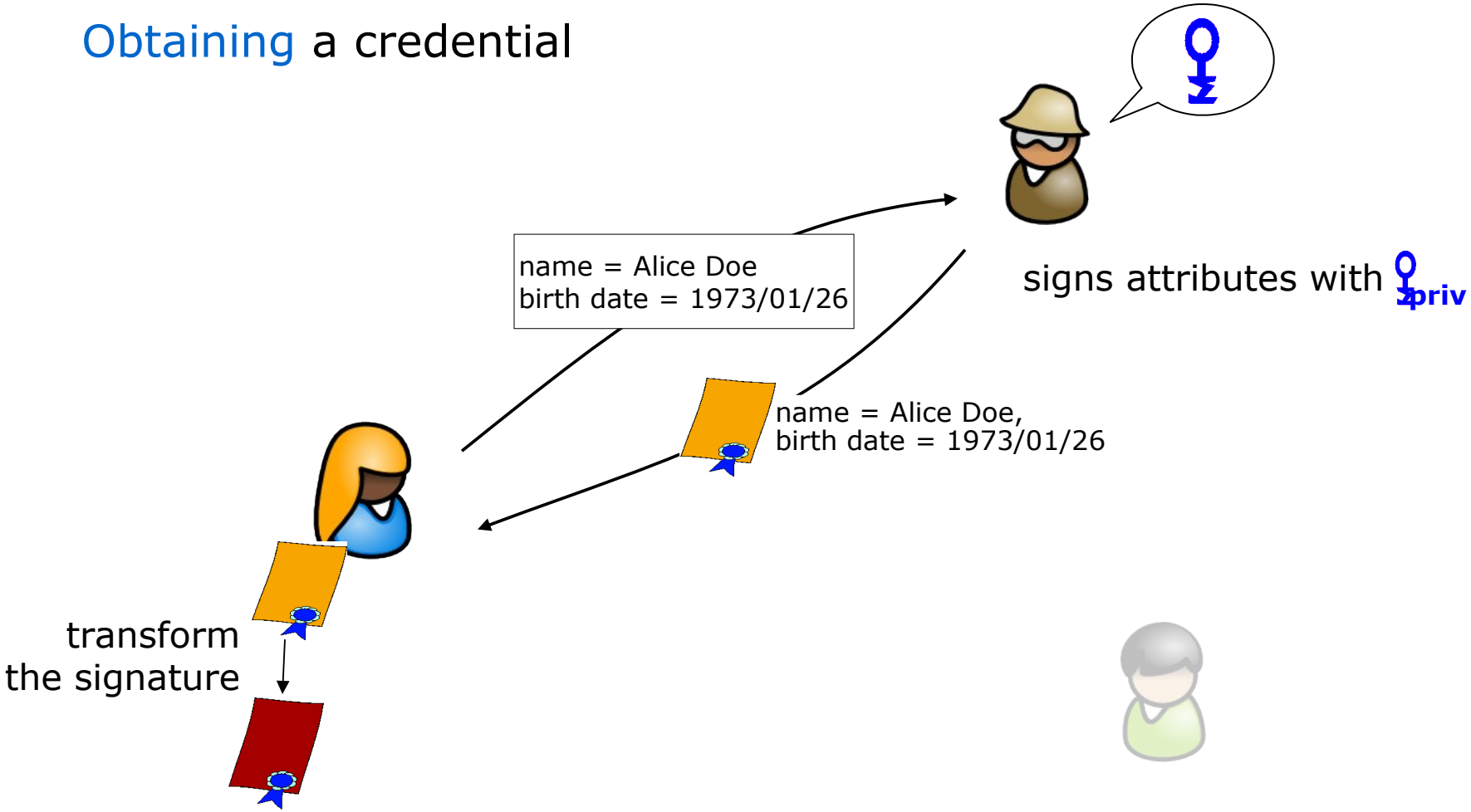

Zero-Knowledge Proof



© 2011 IBM Corporation


U-Prove

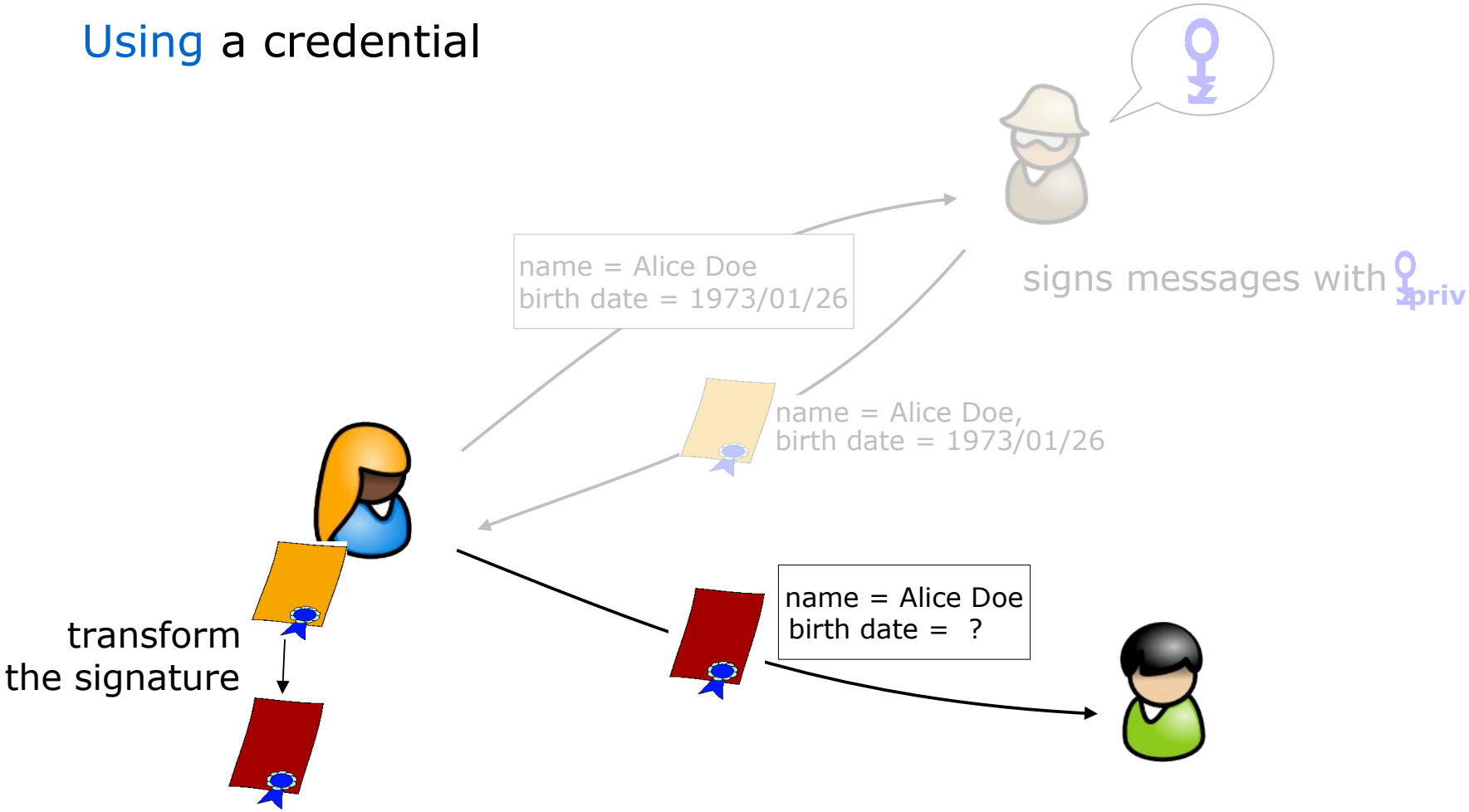
## Obtaining a credential





© 2011 IBM Corporation

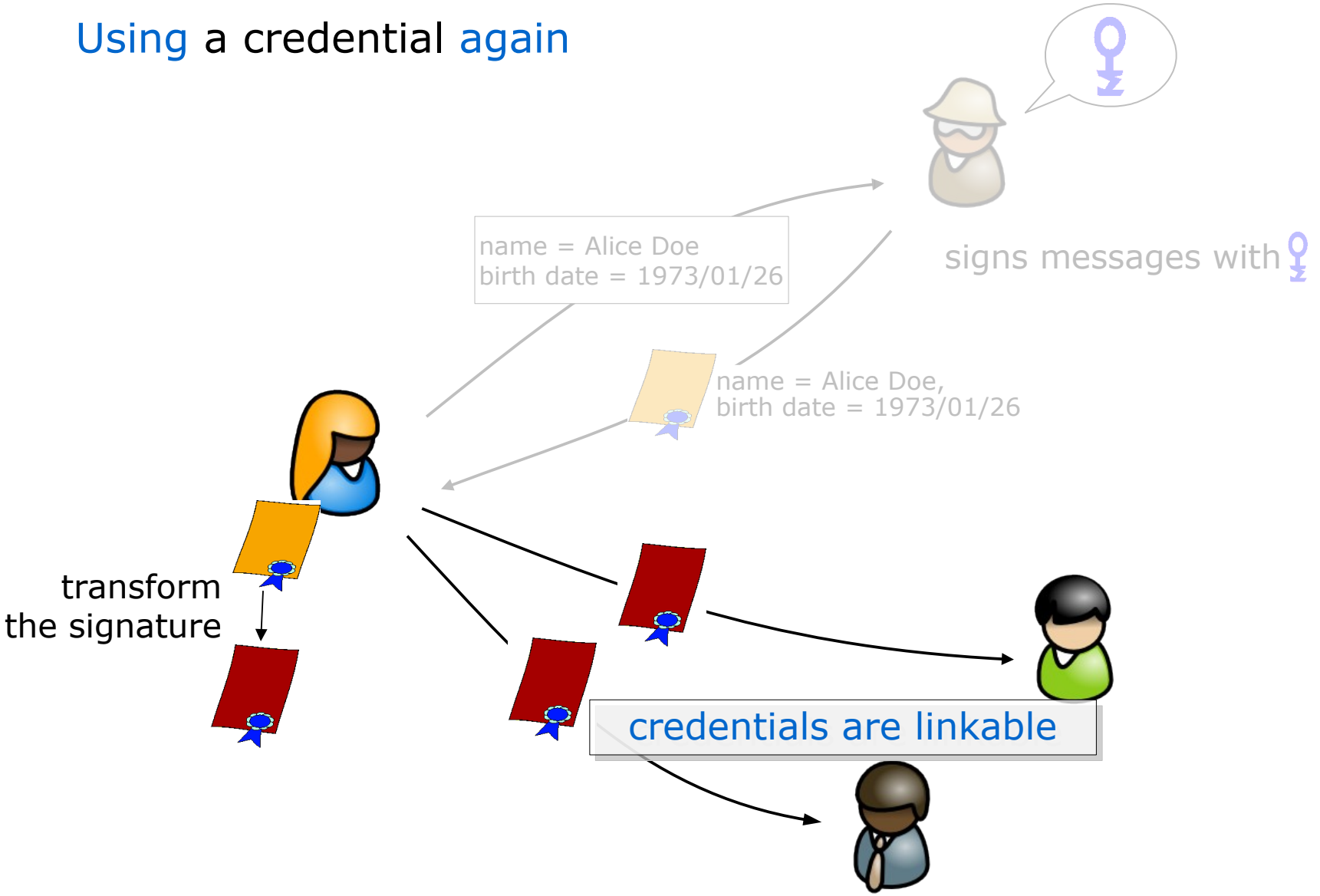
## Using a credential





© 2011 IBM Corporation

## Using a credential again

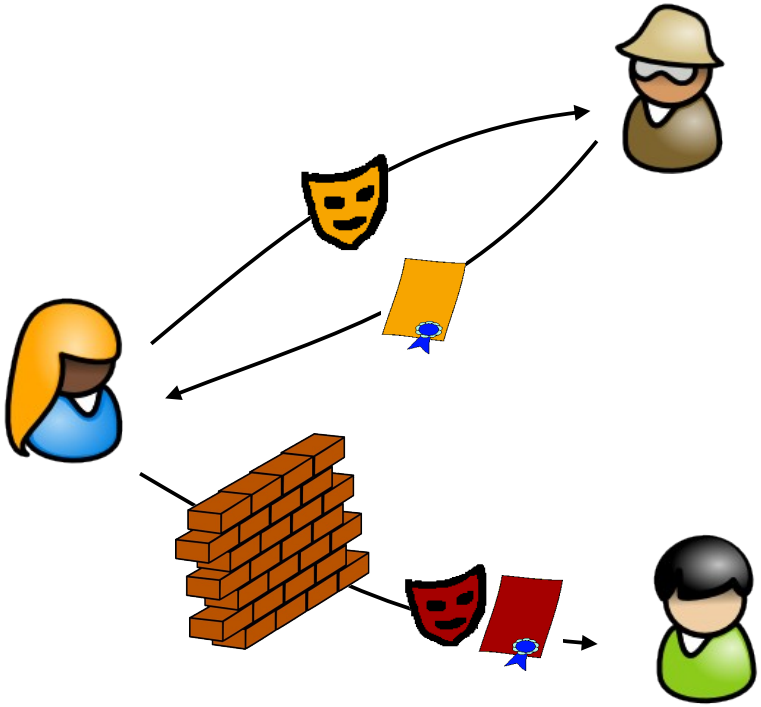




© 2011 IBM Corporation

# Anonymous Credentials - Two Approaches

## Zero-Knowledge Proofs



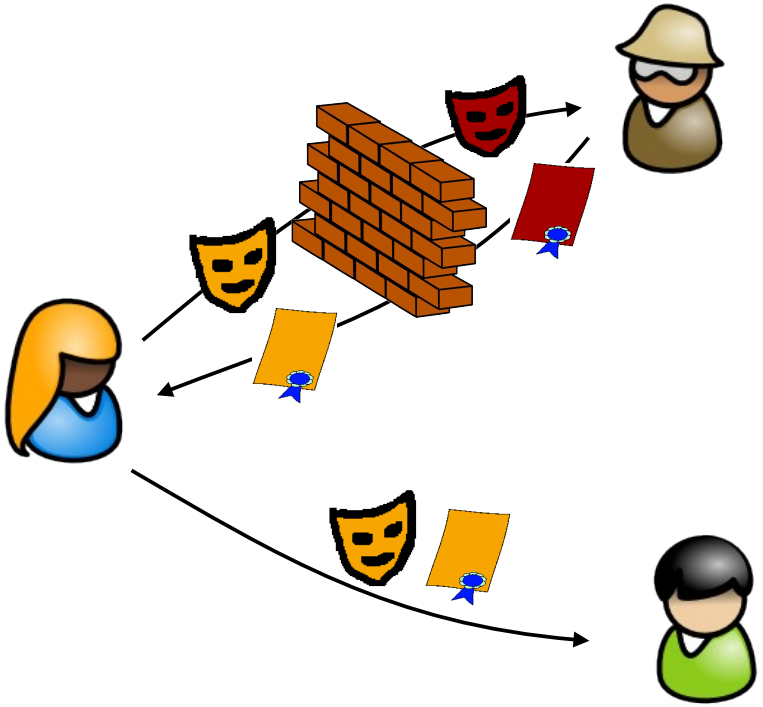
multiple presentations **unlinkable**

Damgard, Camenisch&Lysyanskaya

(Identity Mixer)

Strong RSA, pairings (LMRS, q-SDH)

## Blind Signatures



multiple presentations **linkable**

but can be obained in batches

Chaum, Brands et al. (U-Prove)

Discrete Logs, RSA,..



© 2011 IBM Corporation



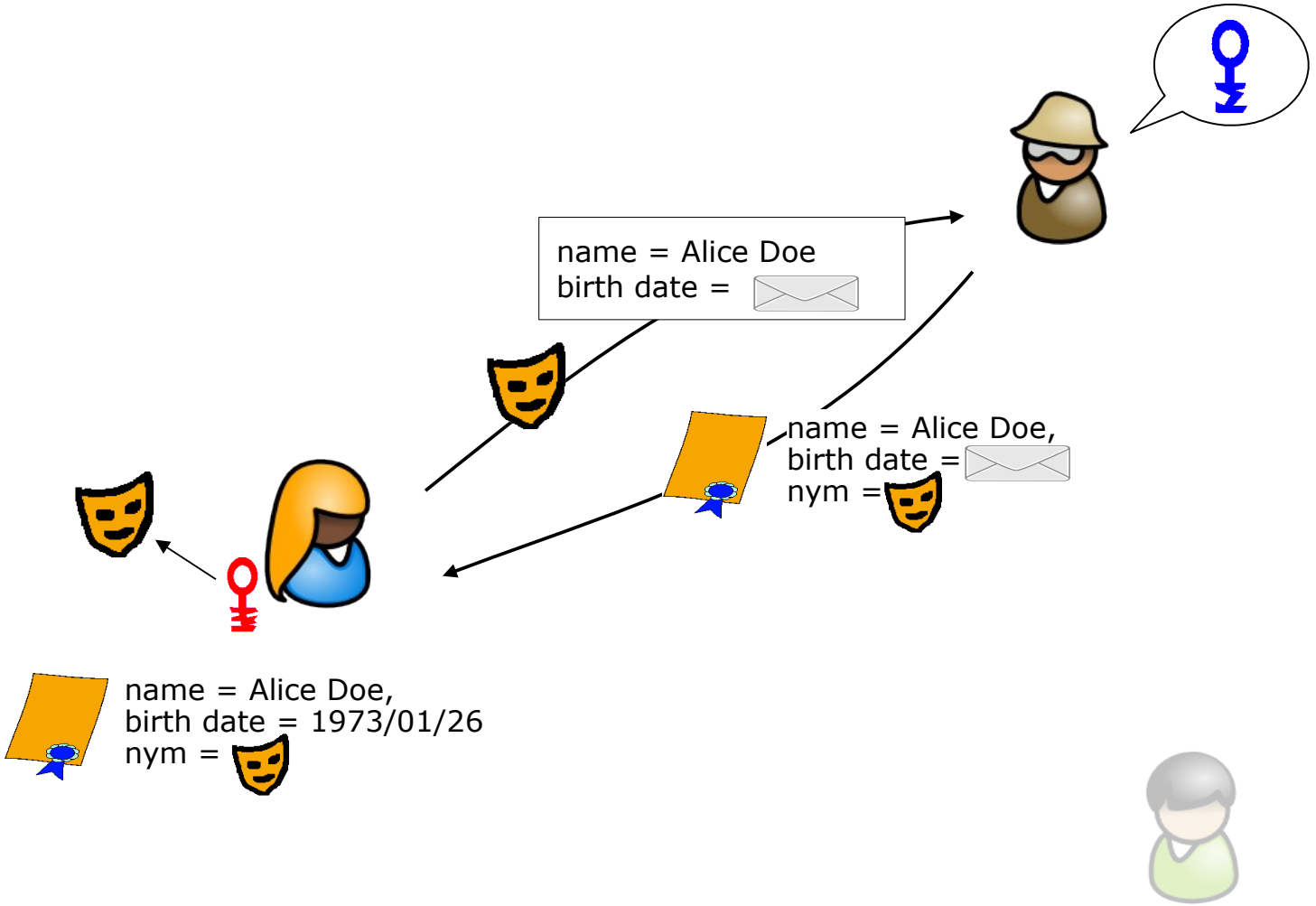
# Extended Functionality

## Extended Functionality

- Credentials on hidden attributes
- Tracing of user/attribute
- Revocation of credentials
- Limited spending
- ...


© 2011 IBM Corporation

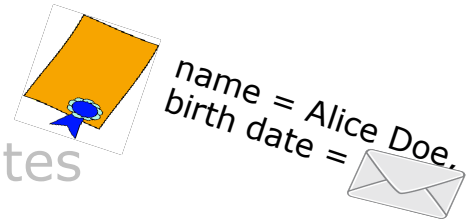
# Credential on hidden attributes





© 2011 IBM Corporation

# Extended Functionality

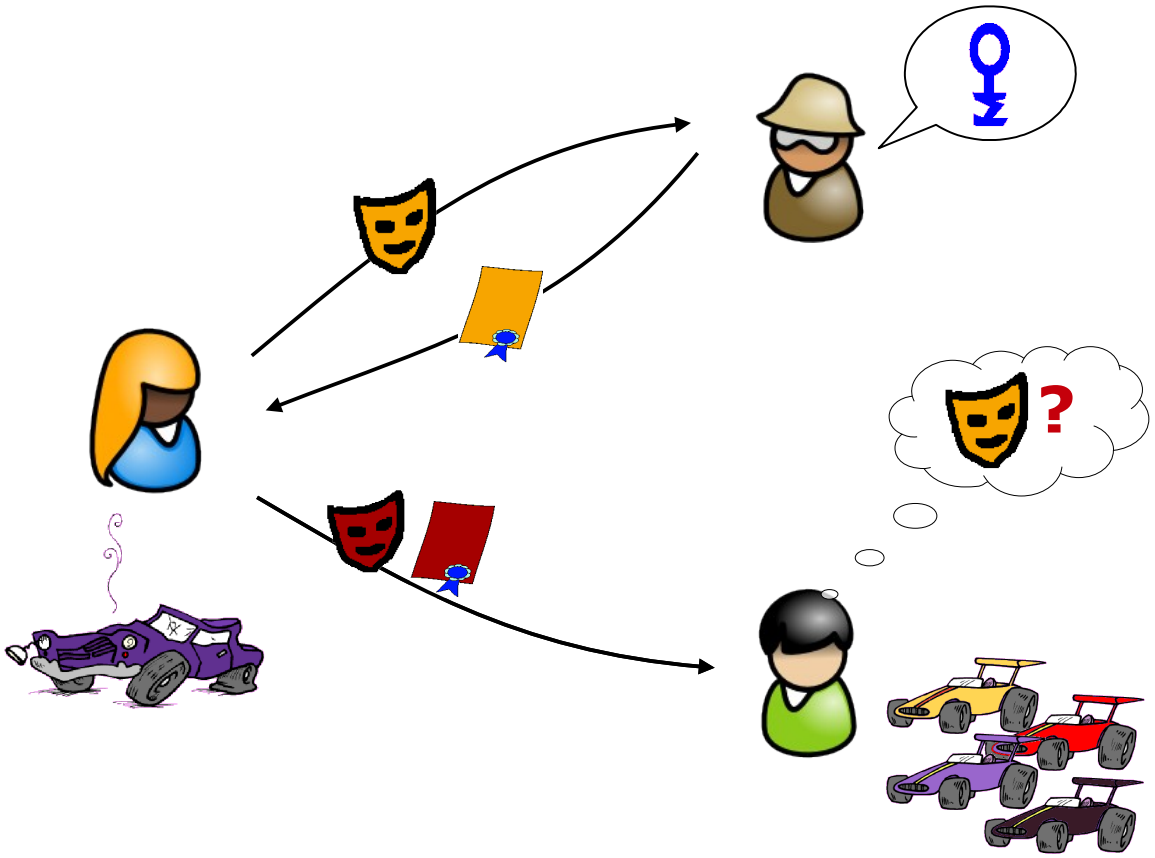



- Credentials on hidden attributes
- Tracing of user/attribute
- Revocation of credentials
- Limited spending
- ...


© 2011 IBM Corporation

# Tracing (Attribute/Identity Escrow)

## Tracing through verifiable encryption



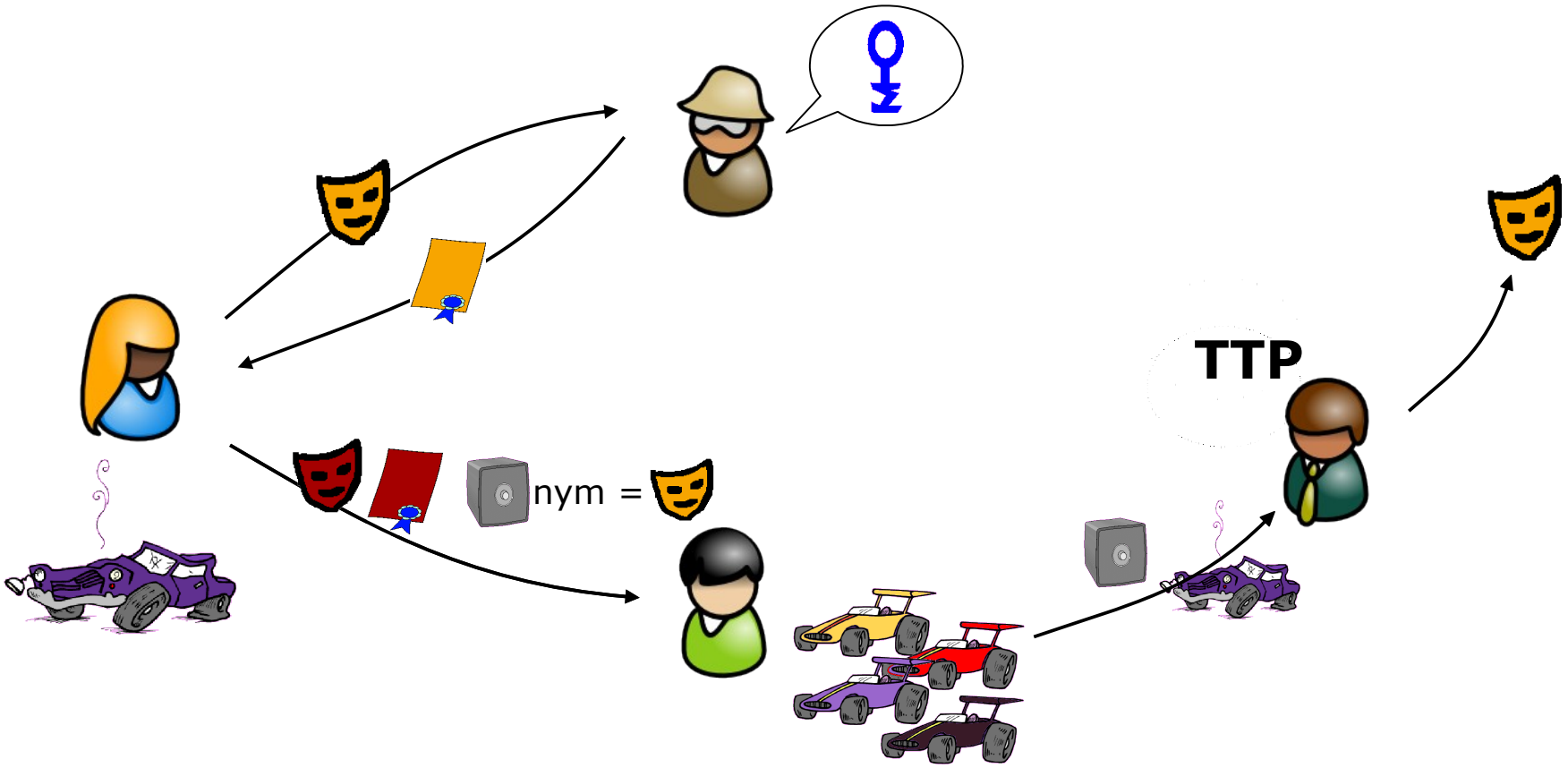





© 2011 IBM Corporation

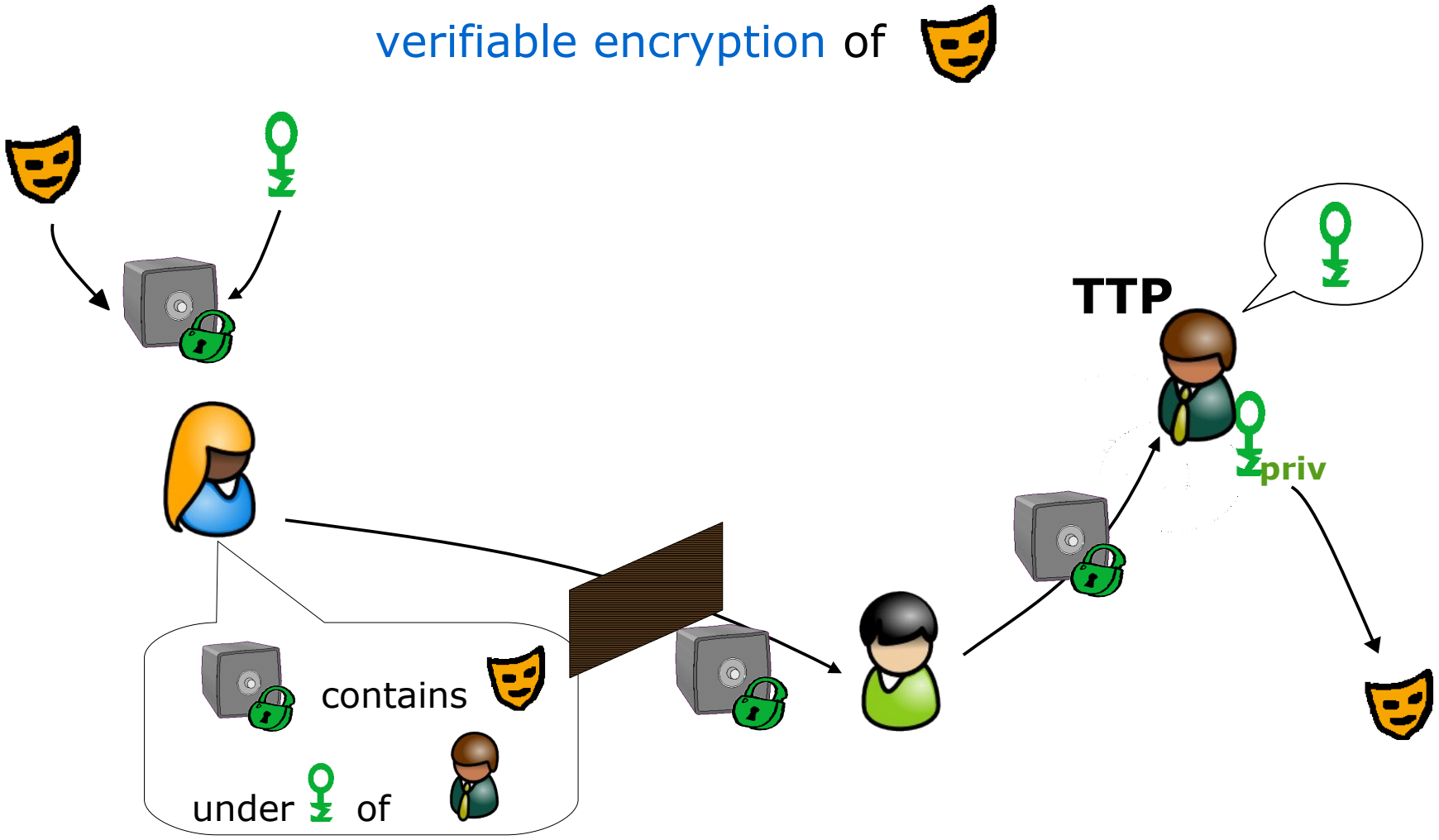
# Tracing (Attribute/Identity Escrow)

## Tracing through verifiable encryption





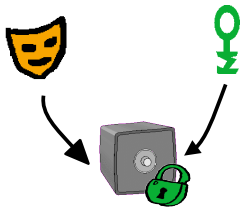

© 2011 IBM Corporation

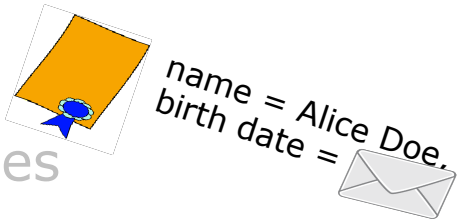




© 2011 IBM Corporation

# Extended Functionality



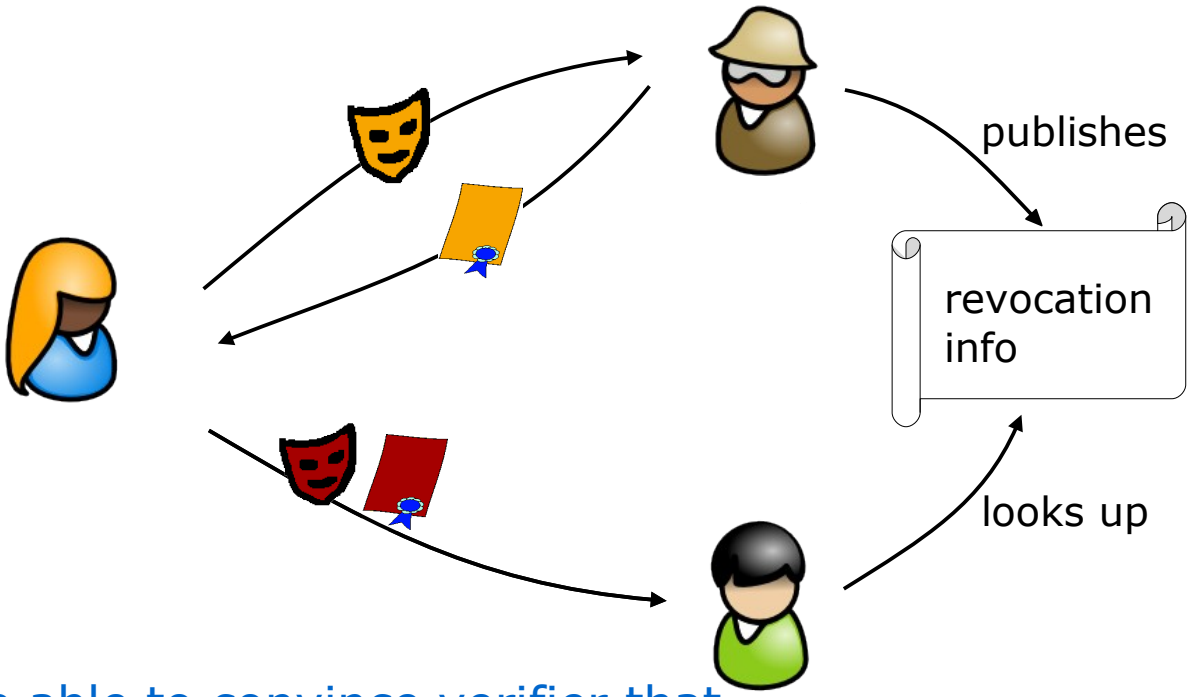



- Signatures on hidden attributes
- Tracing of user/attribute
- Revocation of credentials
- Limited spending
- ...


© 2011 IBM Corporation

# Anonymous Credential Revocation

- various reasons to revoke credential
  - user lost credential / secret key
  - misbehavior of user

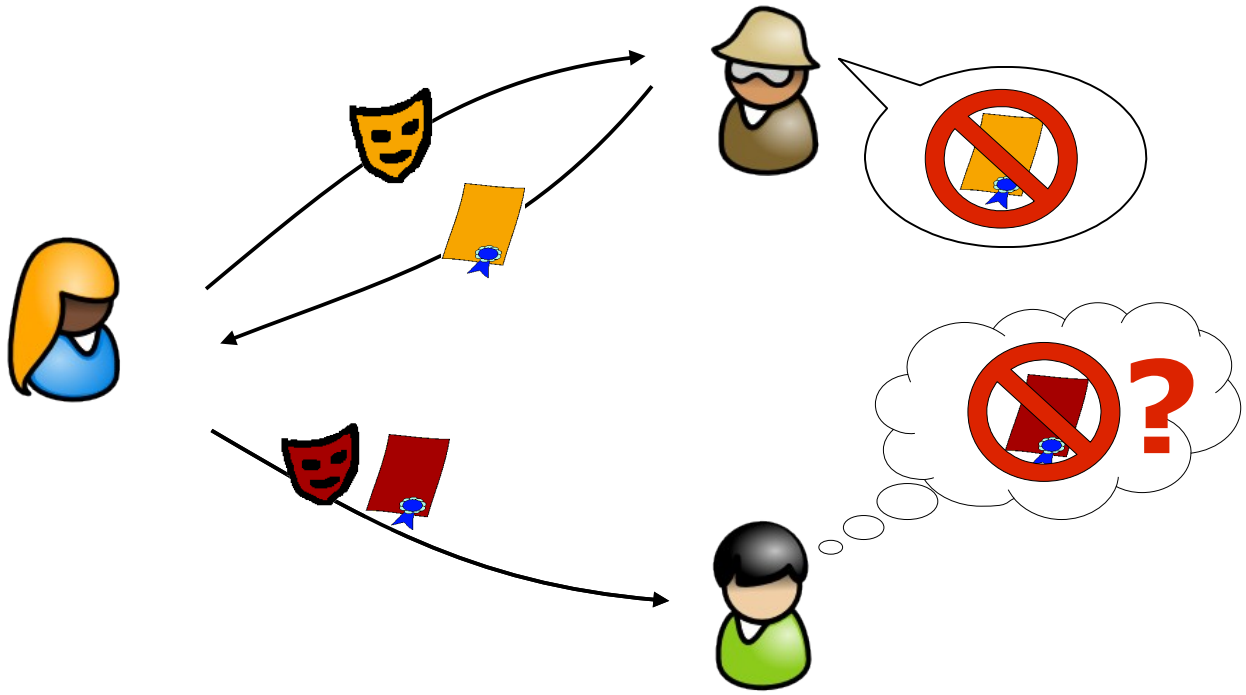



Alice should be able to convince verifier that her credential is among the good ones!


© 2011 IBM Corporation

# Anonymous Credential Revocation

- Unlinkability → standard revocation lists don't work






© 2011 IBM Corporation

# Approaches for anonymous credential revocation

- Accumulators
- Signed intervals
- Validity time

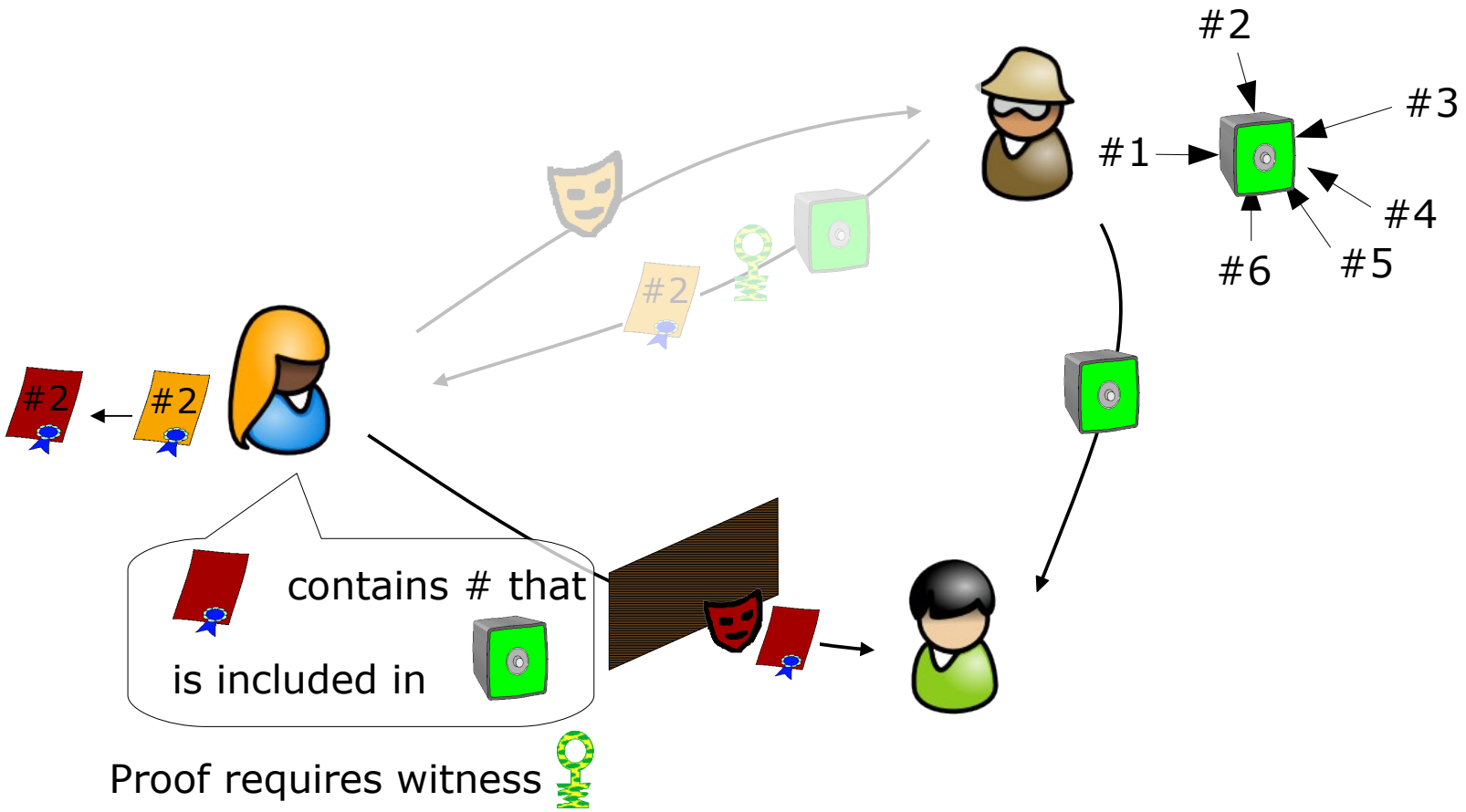

© 2011 IBM Corporation

# Anonymous Credential Revocation | First Solution

Using cryptographic accumulators:

credentials contain random serial number #

Issuer accumulates all "good" serial numbers



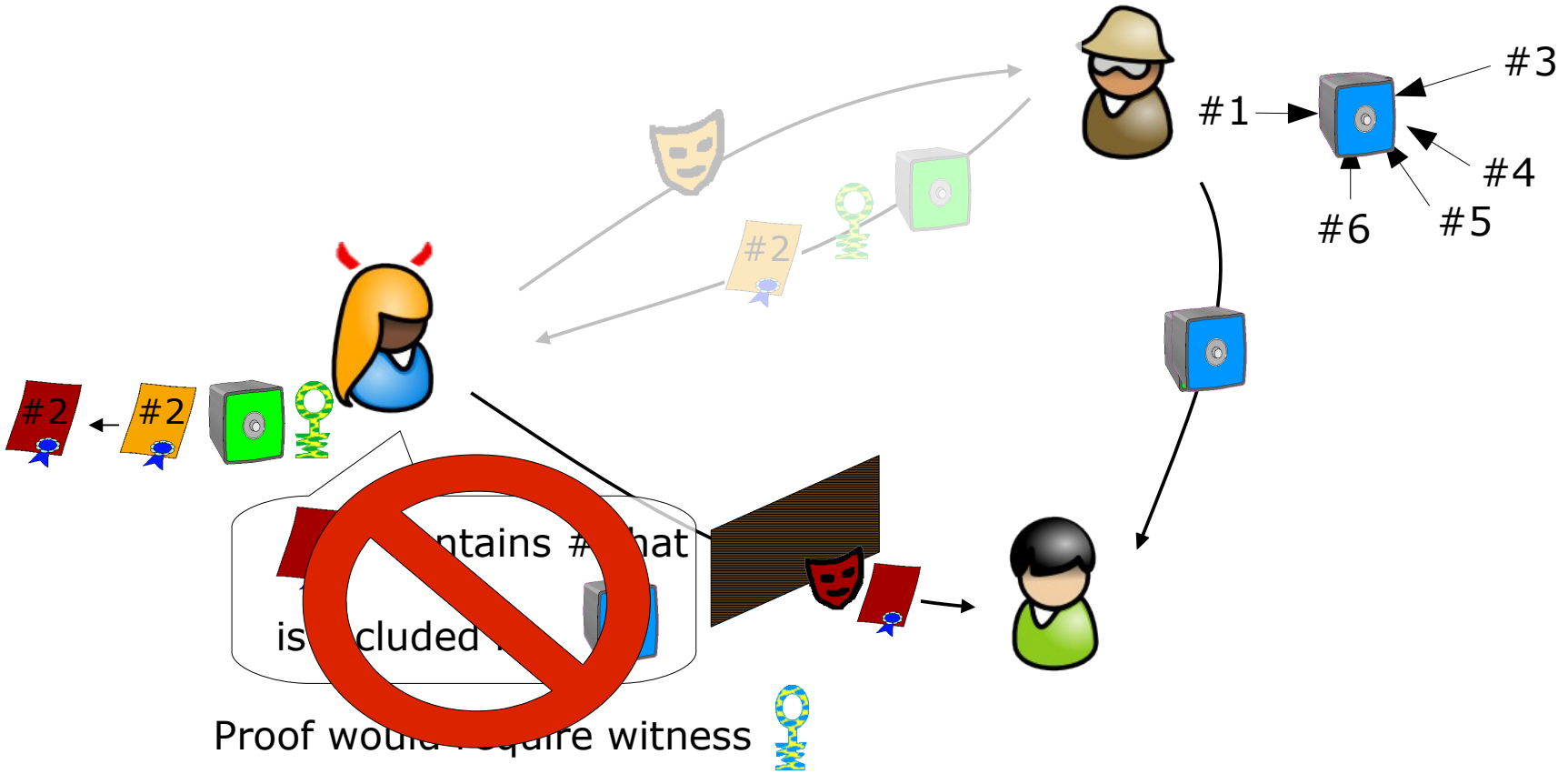



© 2011 IBM Corporation

# Anonymous Credential Revocation | First Solution

Using cryptographic accumulators:

to revoke #2 issuer publishes new accumulator & new witnesses for unrevoked credentials



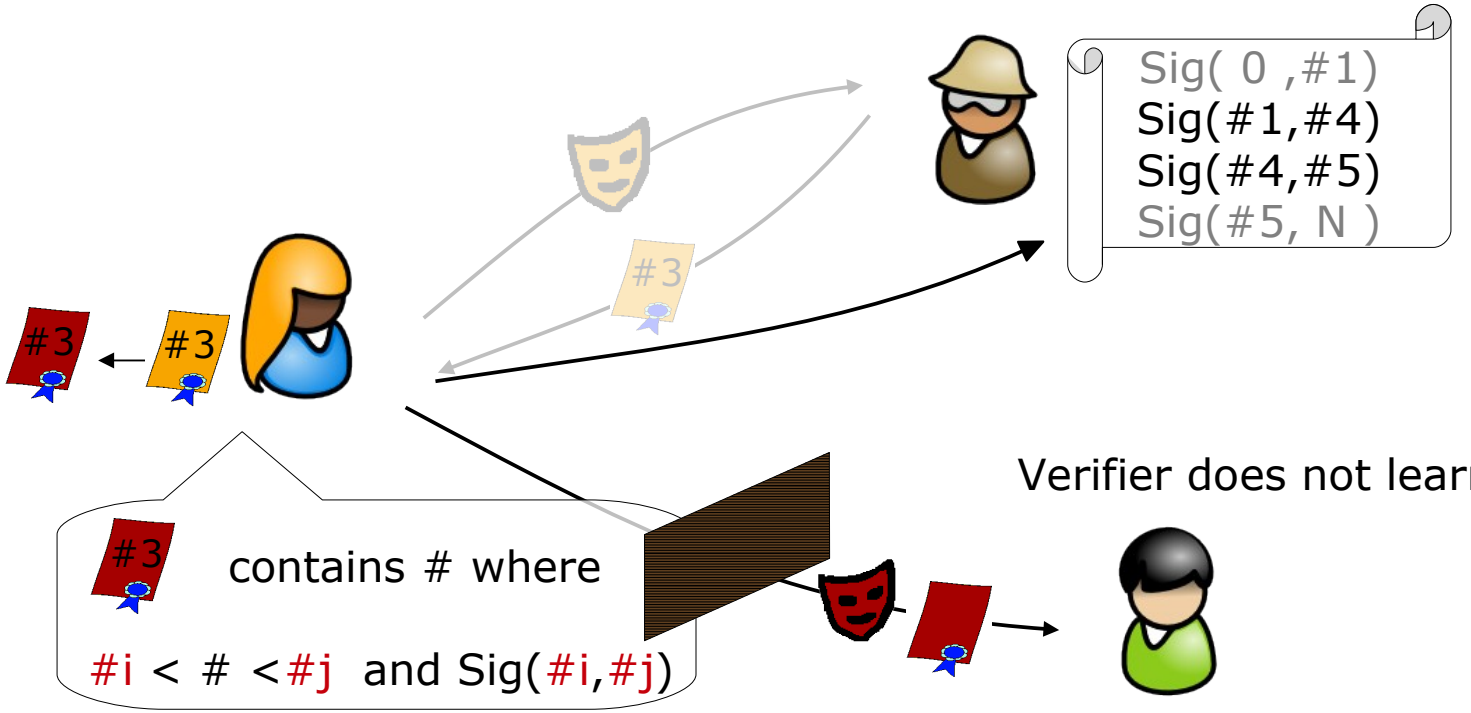


© 2011 IBM Corporation

## Signed intervals

each credential has serial number #1,#2,#3,#4,#5,#6,...

Issuer signs intervals between revoked #

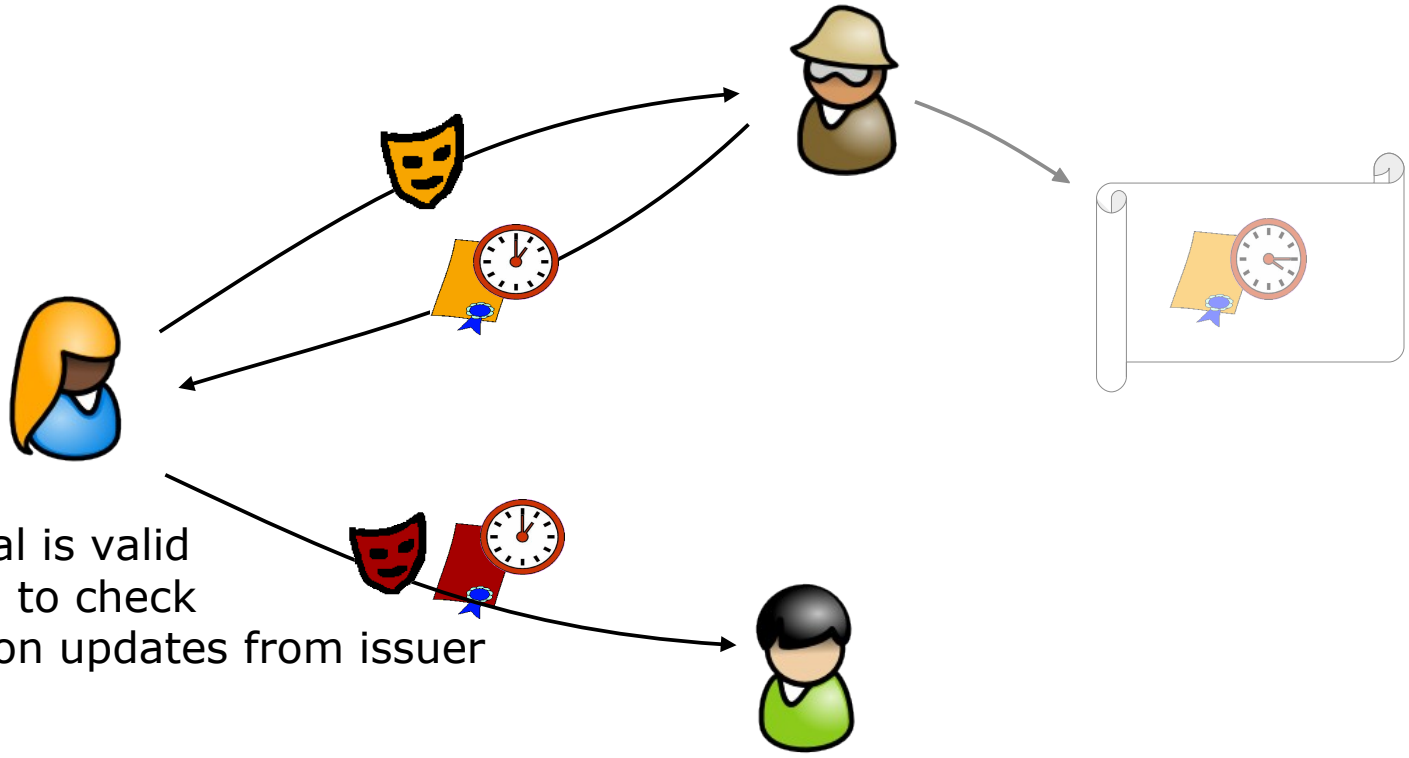




© 2011 IBM Corporation

# Anonymous Credential Revocation | Third solution

## Validity time: short-lived credentials



if credential is valid
→ no need to check
revocation updates from issuer

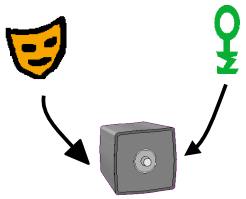
no additional effort for verifier

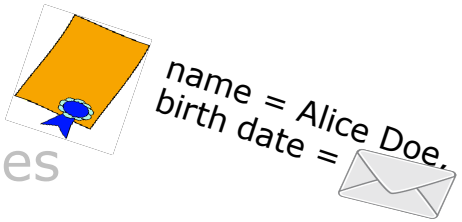




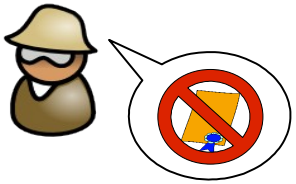
© 2011 IBM Corporation

# Extended Functionality






- Signatures on hidden attributes
- Tracing of user/attribute
- Revocation of credentials
- Limited spending
- …




© 2011 IBM Corporation

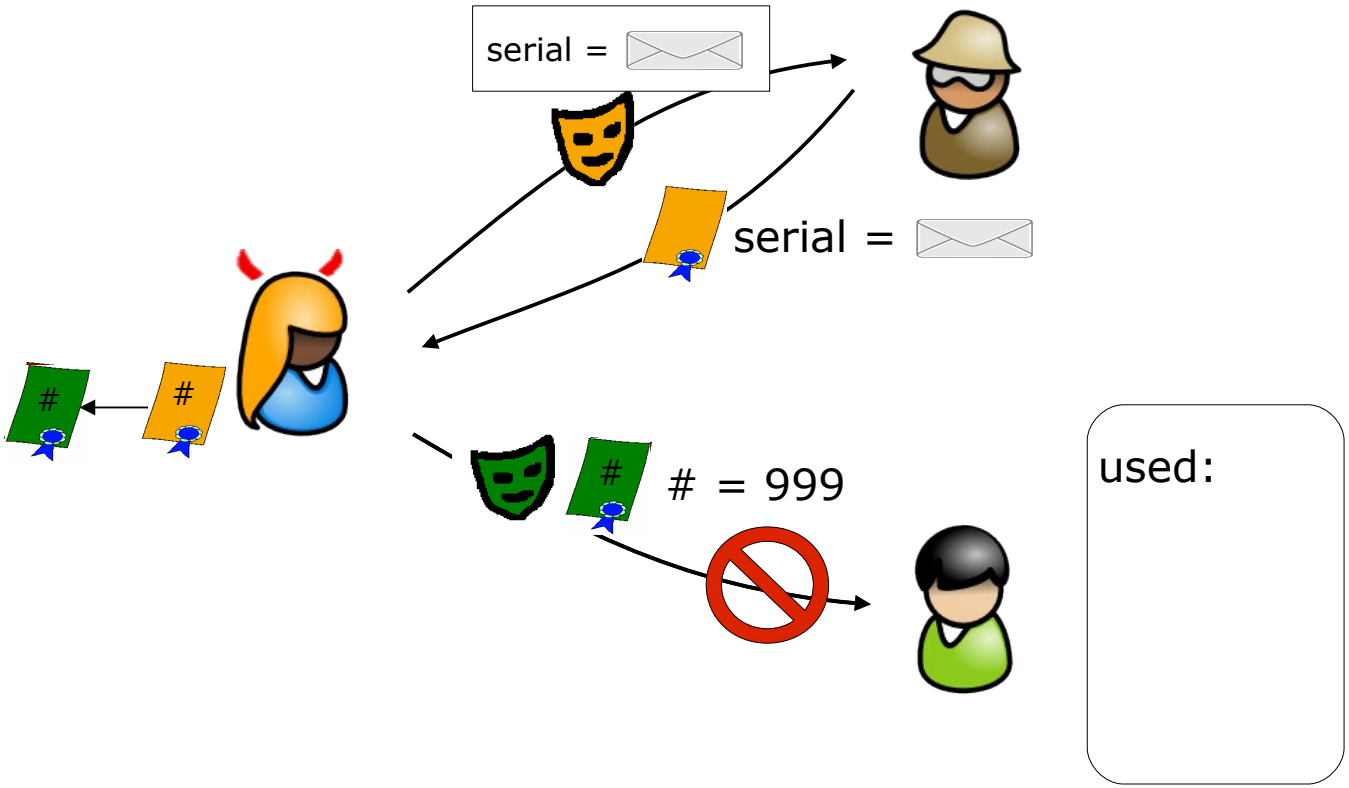
# Approaches for limited spending

- Hidden serial number
- Domain pseudonyms
- Offline identity recovery
- Verifiable random functions


© 2011 IBM Corporation

# Limited Spending: Approach 1

- Hidden serial numbers



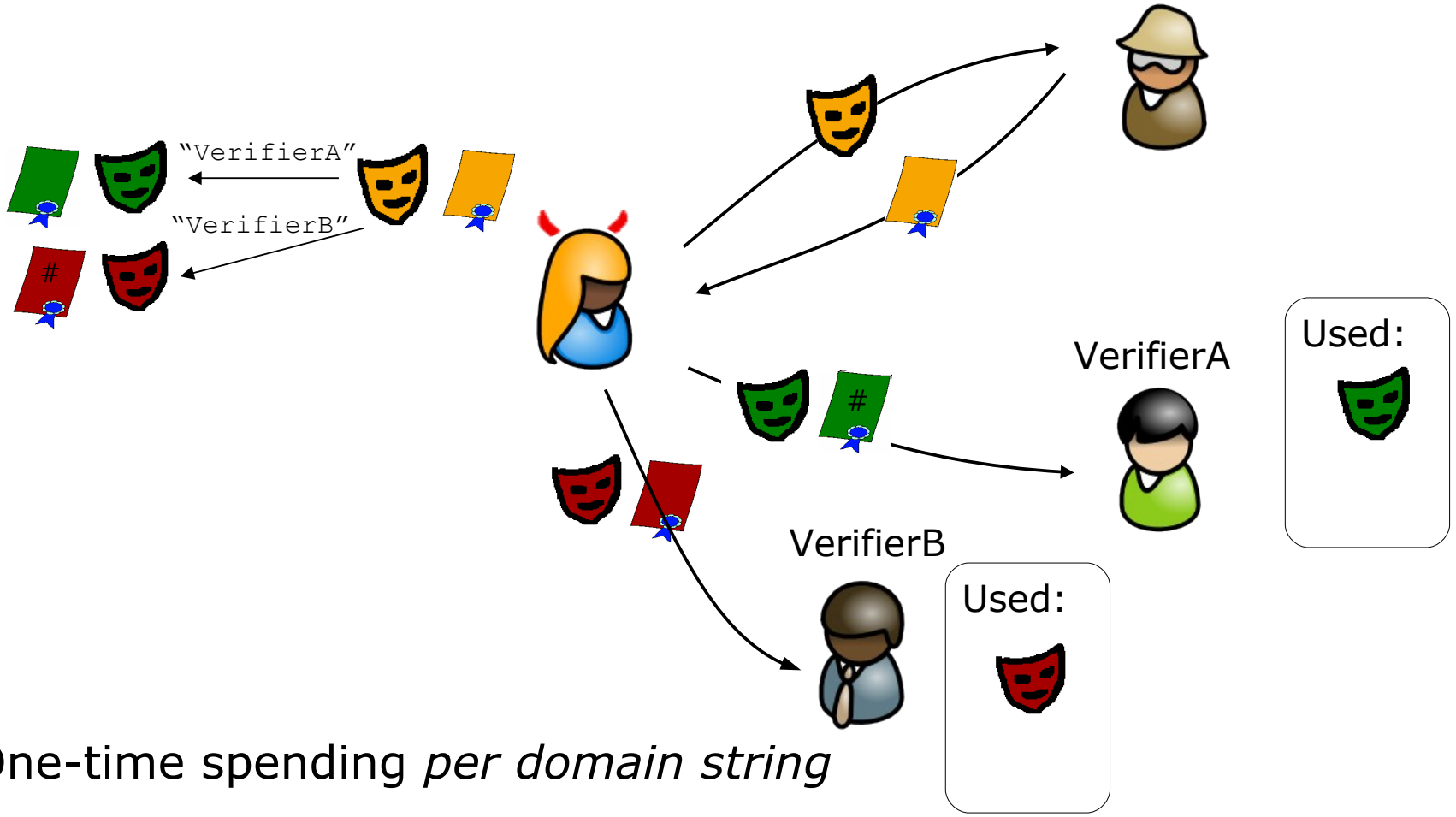

- One-time spending (globally)
- Requires online repository of used serial numbers


© 2011 IBM Corporation

# Limited Spending: Approach 2

- Domain pseudonyms

  cryptographically unique pseudonym per "domain string"




- One-time spending *per domain string*
- Requires online repository of used pseudonyms


© 2011 IBM Corporation

# Limited Spending: Approach 3

## Offline identity recovery

- overspending credential → anonymity gets lifted

main idea:

- Include attribute (#, id, r ) in credential
- showing credential:

  reveal # and t = id + r c  where c randomly chosen by verifier
- spending once: t does not reveal anything about id!
- spending twice: two equations for the same (#, id, r)

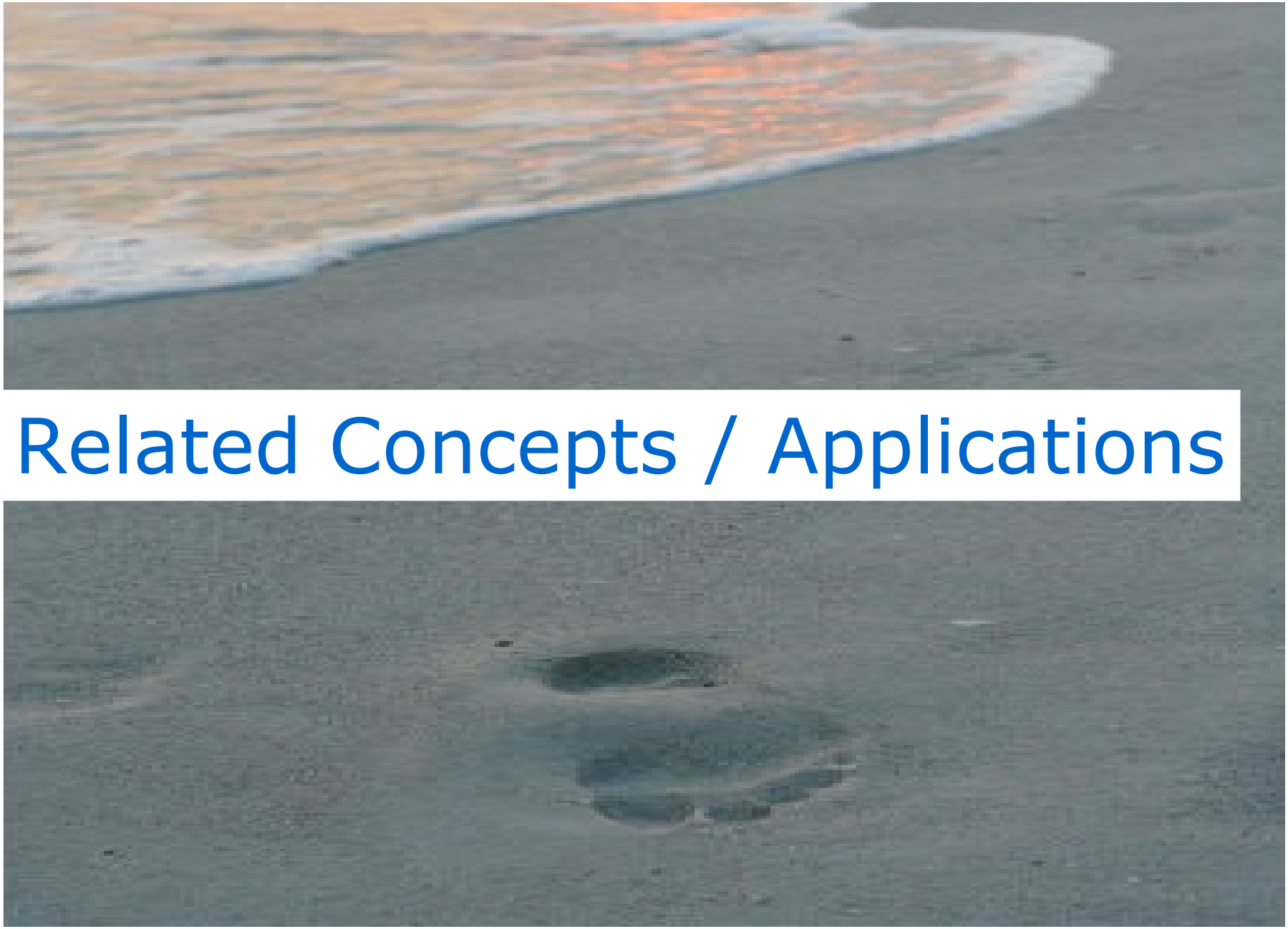
  t1 = id + r c1

  t2 = id + r c2

  → allows computation of id

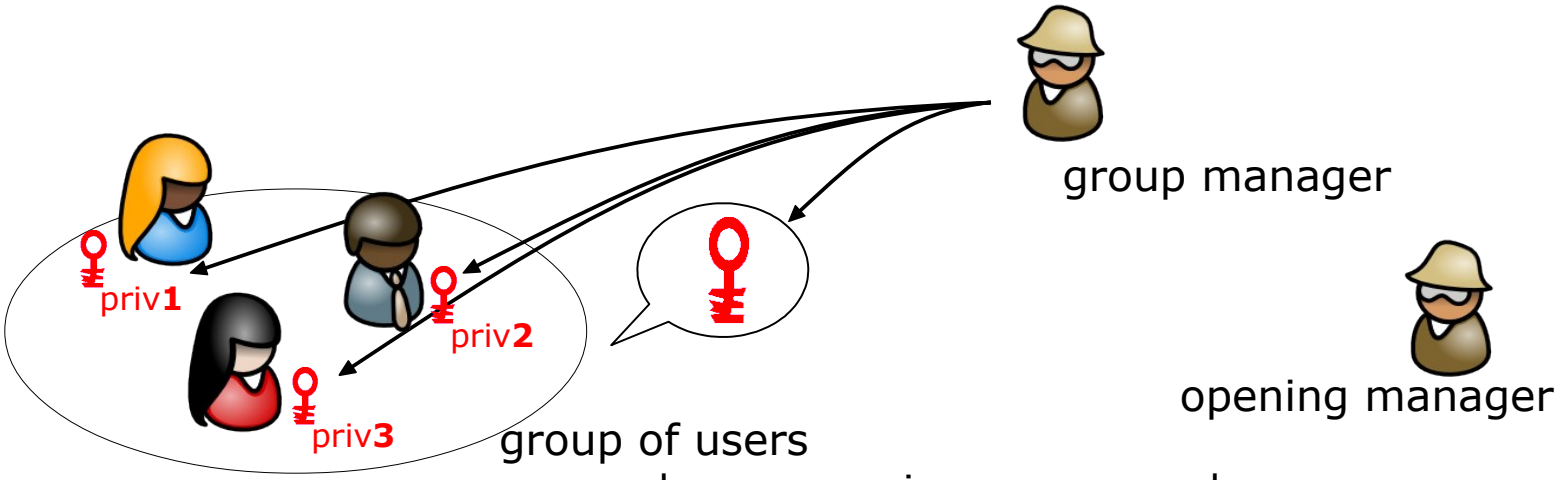
can be extended to n-time spending by deriving #,r from PRF


© 2011 IBM Corporation



# Related Concepts / Applications

# Group Signatures



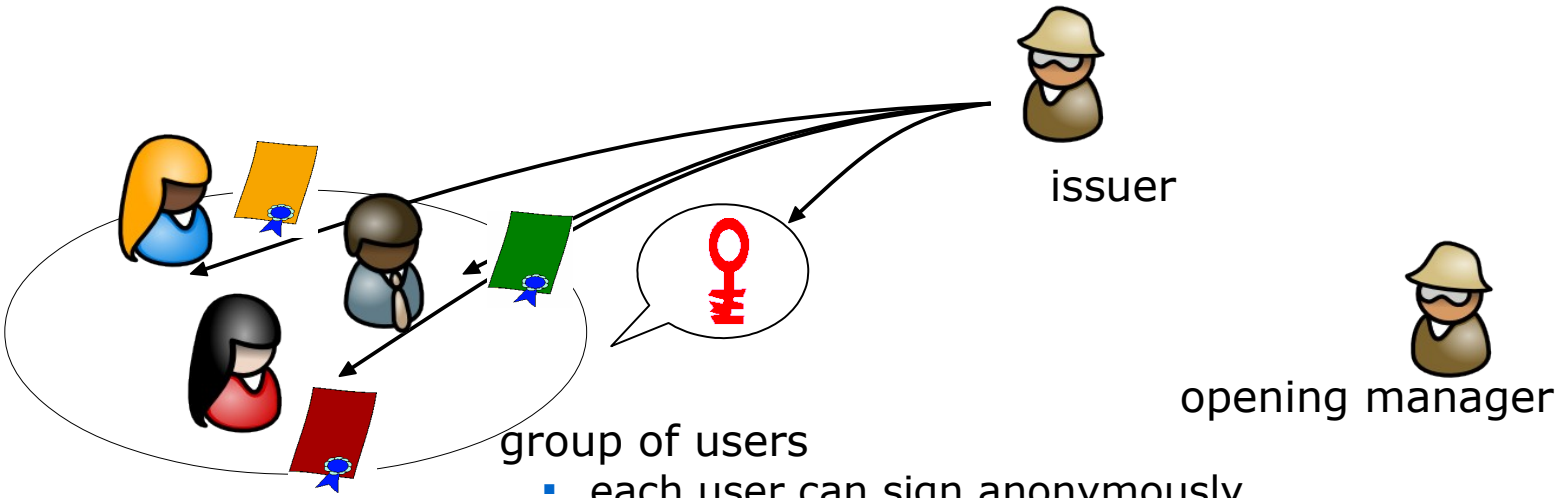

- each user can sign anonymously on behalf of the group

Properties of Group Signatures:

- unforgeablity — no outsider can forge signature on behalf of group
- unlinkability — signatures by the same signer can not be linked
- anonymity — nobody except opening manager can tell which signer created a signature
- traceability — opening manager can trace back any valid signature to a signer
- accountability — cheating group manager can not create signature that opens to an honest user


© 2011 IBM Corporation

# Group Signatures using Credential System




- each user can sign anonymously on behalf of the group

showing protocol of credential scheme → signature scheme

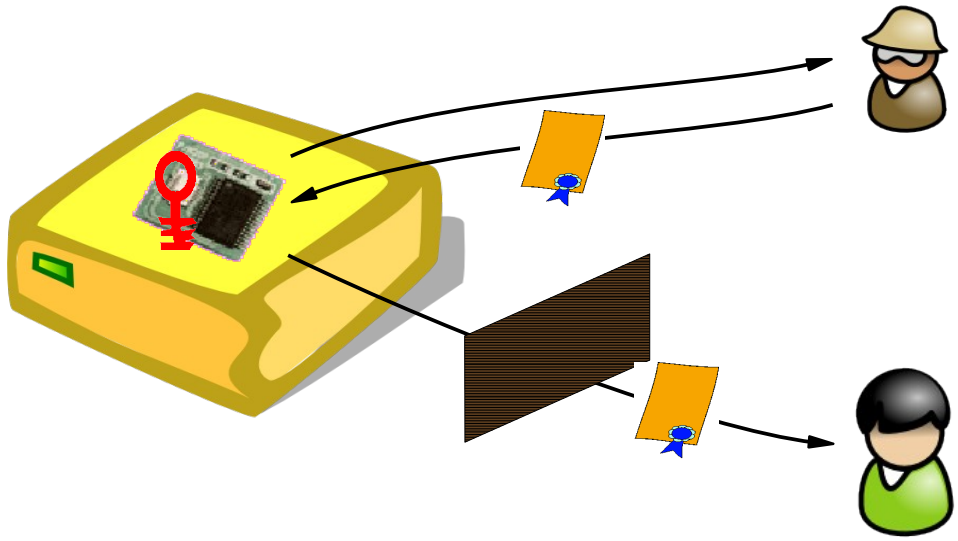
(inherits all the anonymity features of credential system)

- issuer = group manager: issues each member credential with attribute = identity
- group members verifiably encrypt their identity under pk of opening manager


© 2011 IBM Corporation

# Direct Anonymous Attestation

remote authentication of a trusted platform (TPM) that securely generates keys



group signature scheme without the opening functionality

(i.e. anonymity cannot be revoked)

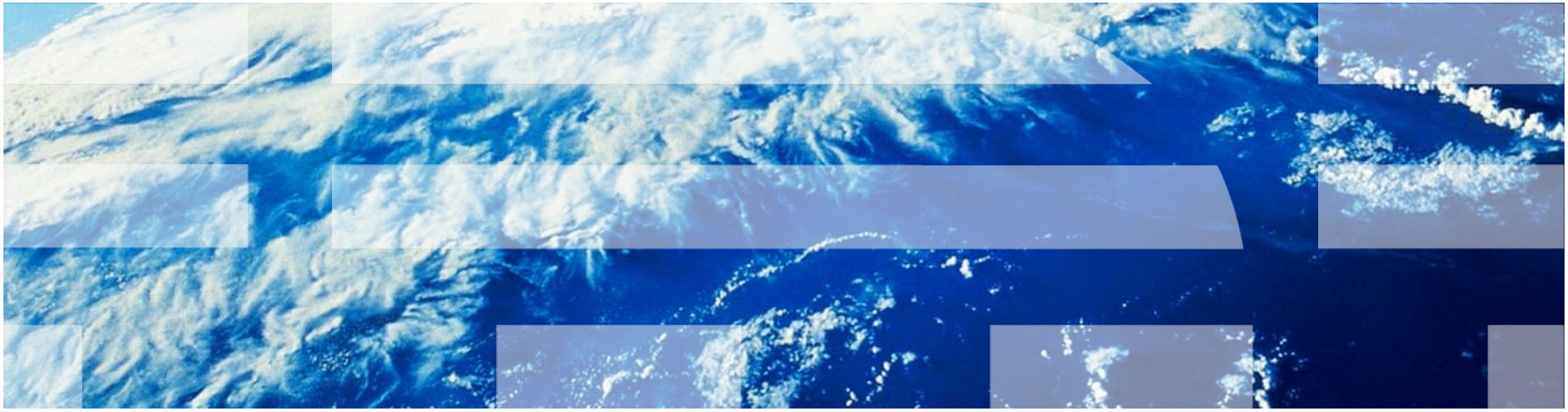
but with a revocation feature such that stolen keys can be identified and rejected


© 2011 IBM Corporation

# ABC4Trust

# Tutorial

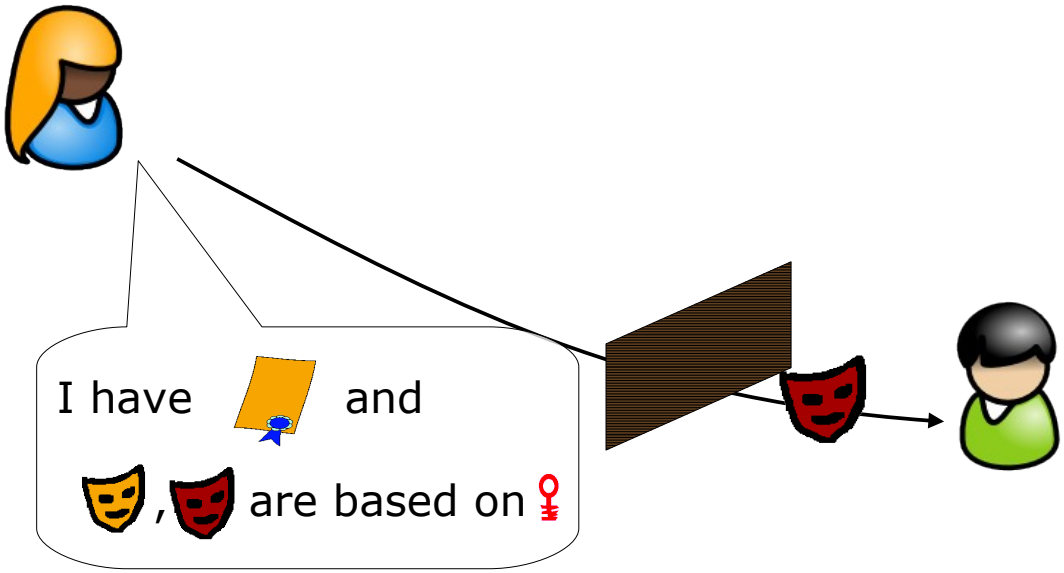
## Part II – Crypto & Math Basics



# Zero-Knowledge Proof

Prover Alice wants to convince verifier Bob that she knows a secret.

How can she convince Bob without him learning the secret?





© 2011 IBM Corporation

# Excursus: Number Theory | Cyclic Groups

- exponentiation = repeated application of • , e.g., $a^3 = a \bullet a \bullet a$
- a group is cyclic if every element is power of some fixed element:
  - i.e. for each a in G, there is unique i such that $g^i = a$
  - g = generator of the group
  - define $g^0 = 1$ = identity element

$$G = \langle g \rangle = \{1=g^0, g^1, g^2, \ldots, ., g^{q-1}\}$$

  - q = |G|= order of group

    if q is a prime number than G is cyclic

    → computation in exponents can be done modulo q:

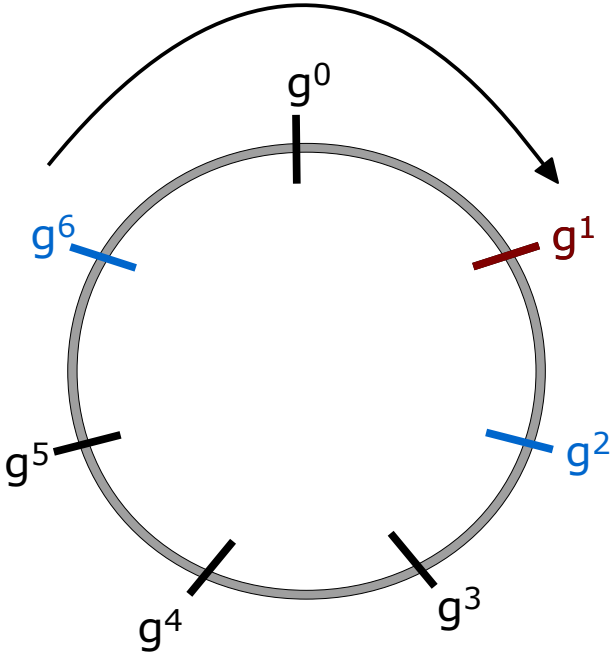
$$g^i = g^{i \bmod q}$$

$g^i \rightarrow i$ is discrete logarithm of *a* to base *g*: $i = \log_g(a)$


© 2011 IBM Corporation

# Excursus: Number Theory | Cyclic Groups

- *Example*: G = <g> = {1=$g^0$, $g^1$, $g^2$, ..., ., $g^6$} with |G| = q = 7




$g^6 \bullet g^2 =$


© 2011 IBM Corporation

# Excursus: Number Theory | Discrete Logarithm

given g, x it is easy to compute $g^x$, $g^{1/x}$, ....

given $g^x$ ,$g^y$ it is easy to compute $g^x g^y = g^{x+y}$

## Discrete Log Assumption

- given $g^x$ it is hard to compute x

## Diffie-Hellman Assumption

- given $g^x$ ,$g^y$ it is hard to compute $g^{xy}$

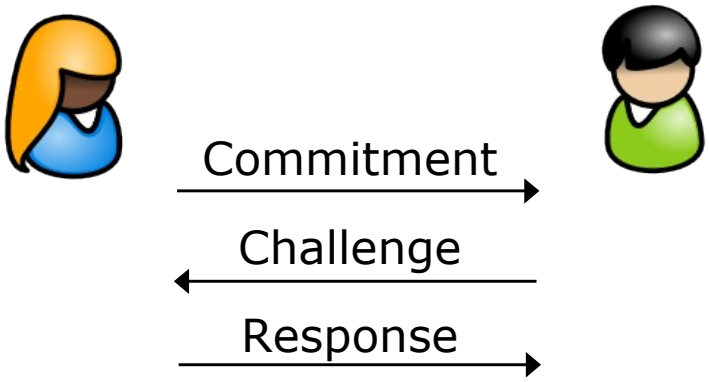
## Decisional Diffie-Hellman Assumption

- given $g^x$ ,$g^y$, $g^z$ it is hard to decide if $g^z = g^{xy}$


© 2011 IBM Corporation

# Zero-Knowledge Proofs

- interactive proof




- properties:

  zero-knowledge

  verifier learns nothing about the prover's secret

  soundness

  prover can convince verifier only if she knows the secret

  completeness

  if prover knows the secret she can always convince the verifier


© 2011 IBM Corporation

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

Prover wants to convince verifier that she *knows* $x = \log_g y$ such that verifier only learns $y$ and $g$.



Prover

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



Verifier

random $r \in Z_q$

$t := g^r$

t →

← c

random $c \in \{0,1\}$

$c=0$ $s := r$

$c=1$ $s := r - x \; (q)$

s →

$t = g^s y^c$ ?

completeness: $t = g^{r-cx} y^c = g^{r-cx} g^{xc} = g^r$



© 2011 IBM Corporation

**Zero-Knowledge Property:** If verifier does not learn anything

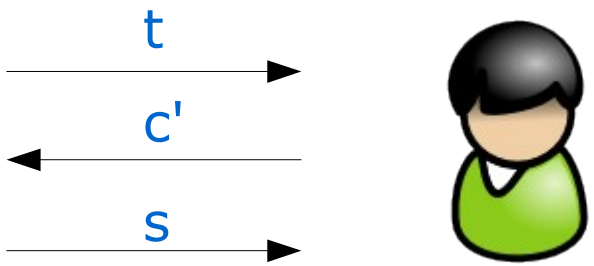
(except the fact that Alice knows $x = \log_g y$ )

Idea: One can simulate whatever Bob "sees".

choose random $c, s$

if $c = 0$ compute $t := g^s$

if $c = 1$ compute $t := g^s y$




if $c = c'$ send $s$ ,
otherwise restart

$t = g^s y^c$ ?

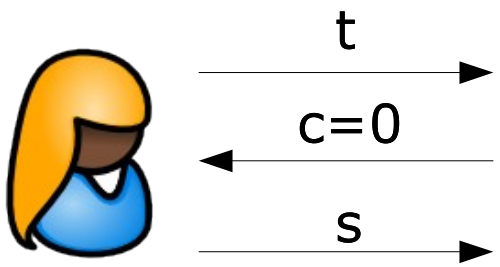
(works only if c' comes from small domain ...)

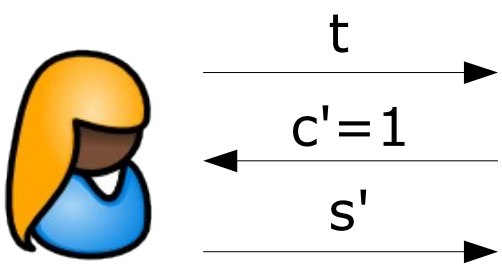

© 2011 IBM Corporation

**Soundness:** If prover is successful, then she "knows" $x = \log_g y$

i.e., one can extract $x$ from her

Idea: run two copies of Alice




$$g^s y^0 = t = g^{s'} y^1$$

$$g^s g^{0x} = t = g^{s'} g^{1x} = g^{s'+x}$$

$$\rightarrow \quad s = s' + x \mod q$$

$$\rightarrow \quad \mathbf{x} = s - s' / (c - c') \mod q$$


© 2011 IBM Corporation

# Zero-Knowledge Proofs

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:

$PK\{(\alpha): \; y = g^{\alpha} \wedge \alpha \in \pm \{0,1\}^{l}\}$

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

Non-interactive (Fiat-Shamir heuristic):

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


© 2011 IBM Corporation

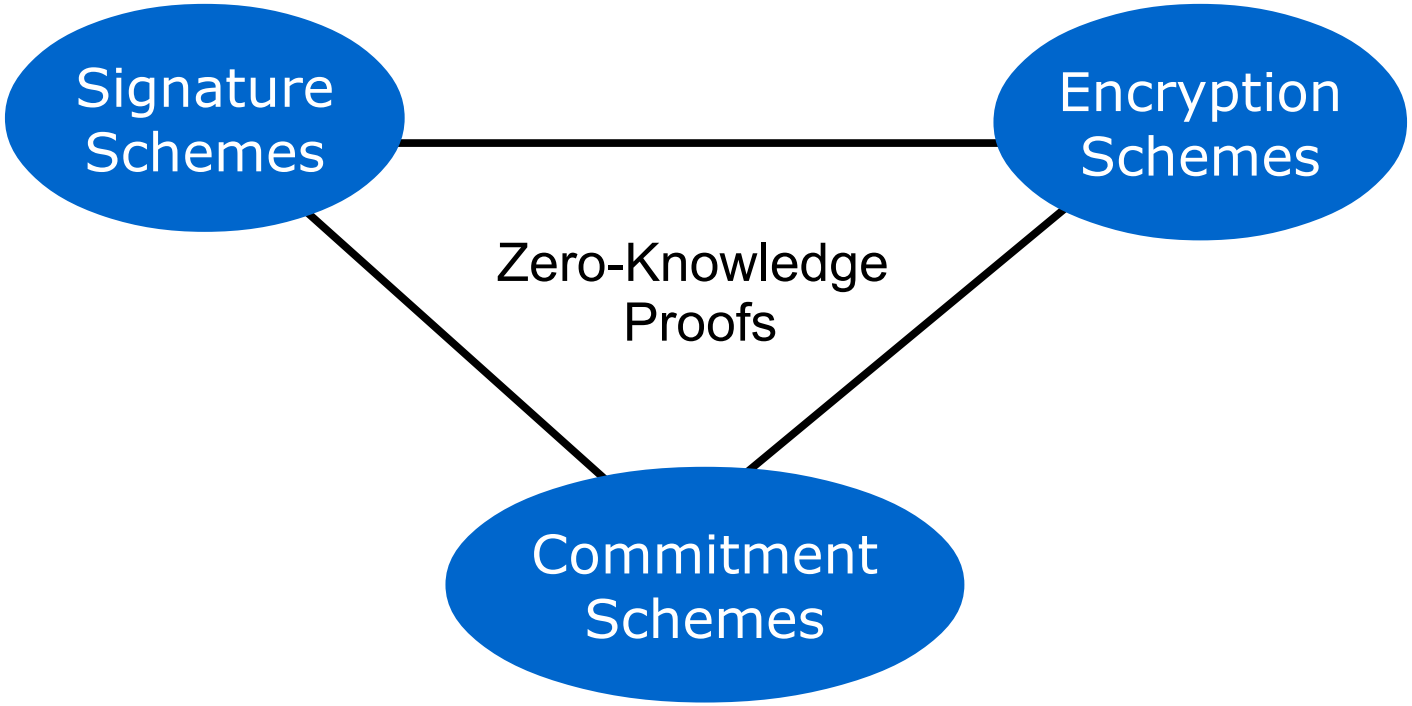
# Summary & Preview

Zero-Knowledge Proofs in Anonymous Credentials:

- Signature scheme to issue certificates
  - Prove statements about messages without revealing them
- Proof protocols for *proving* possession of certificates
  - Prove statements about messages without revealing them
- Verifiable encryption protocol
  - Prove that encryption contains certain attribute
- Dynamic accumulators
  - Prove that serial number is contained in accumulator


© 2011 IBM Corporation

# Summary & Preview





© 2011 IBM Corporation