Anonymous Credentials:

How to show credentials without compromising privacy

Melissa Chase

Microsoft Research

Credentials: Motivation

- ID cards
  - Sometimes used for other uses
    - E.g. prove you're over 21, or verify your address
  - Don't necessarily need to reveal all of your information
  - Don't necessarily want issuer of ID to track all of it's uses
  - How can we get the functionality/verifiability of an physical id in electronic form without extra privacy loss

Credentials: Motivation

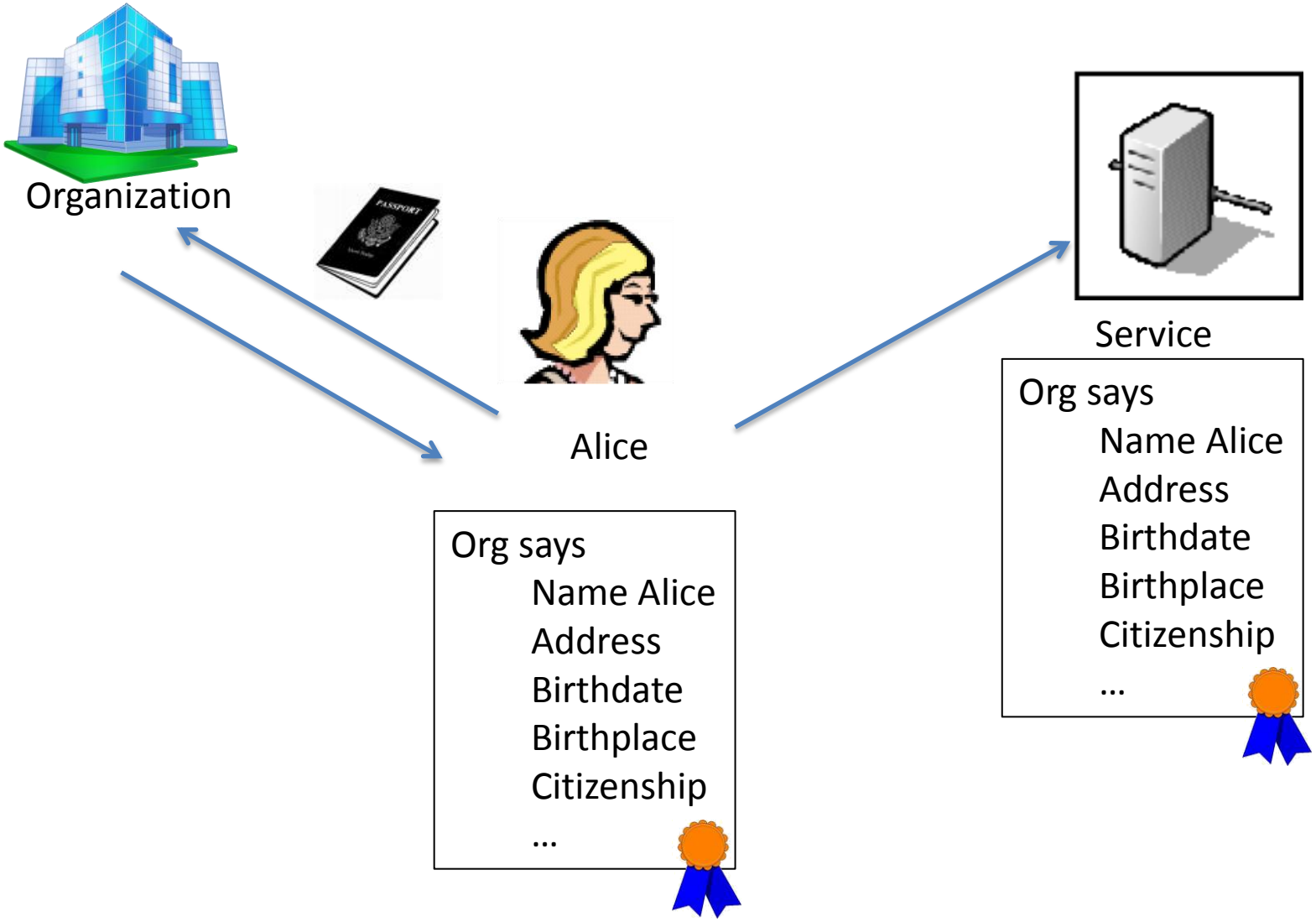
- The goal
  - Users should be able to
    - obtain credentials
    - Show some properties
  - Without
    - Revealing additional information
    - Allowing tracking

Credentials: Motivation

- Other applications
  - Transit tokens/passes
  - Electronic currency
  - Online polling

- Implementations
  - Idemix (IBM), UProve (Microsoft)

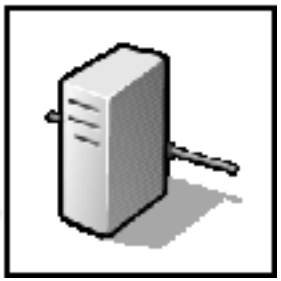
Credentials



Credentials

Organization

Alice



Service

Org says
- Name Alice
- Address
- Birthdate
- Birthplace
- Citizenship
- …

Org says
- Name Alice
- Address
- Birthdate
- Birthplace
- Citizenship
- …

Reveals a lot of info on Alice!

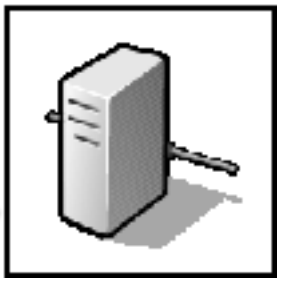
A new model

Anonymous Credentials/Minimal Disclosure Tokens

[Chaum83, …]

Organization

Alice



Service

"I have a cred from
Org saying
WA resident
Age >21"

Cred from Org
Name Alice
Address
Birthdate
Birthplace
Citizenship
…

Reveals only what Alice chooses to reveal

Need not reveal her name

(Need Accountability)

A new model

Anonymous Credentials/Minimal Disclosure Tokens

[Chaum83, …]

Organization

Alice

Service

"I have a cred from Org saying
WA resident

Cred from Org
Name Alice
Address
Birthdate
Birthplace
Citizenship
…

- Cannot
  - Identify Alice
    (if her name is not provided)
  - Learn anything beyond the info she gives
    (and what can be inferred)
  - Distinguish two users with the same attributes
  - Link multiple uses of the same credentials

How can we do this?

- Signatures/Certs?
  - No privacy!

- What about other crypto tools?
- We will use
  - Zero Knowledge Proof of knowledge
    - (interactive or Fiat-Shamir)
  - Commitments
  - Blind signatures

Roadmap

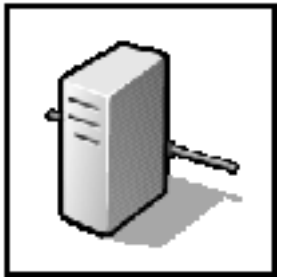
- Review crypto tools
- Construct basic credential systems
- Additional issues
  - Revocation
  - Deciding who to revoke
- Additional features
  - Non-interactive credentials/signatures
  - Delegation
- Conclusion

Zero Knowledge Proofs

Alice

Knows X is true

Statement X

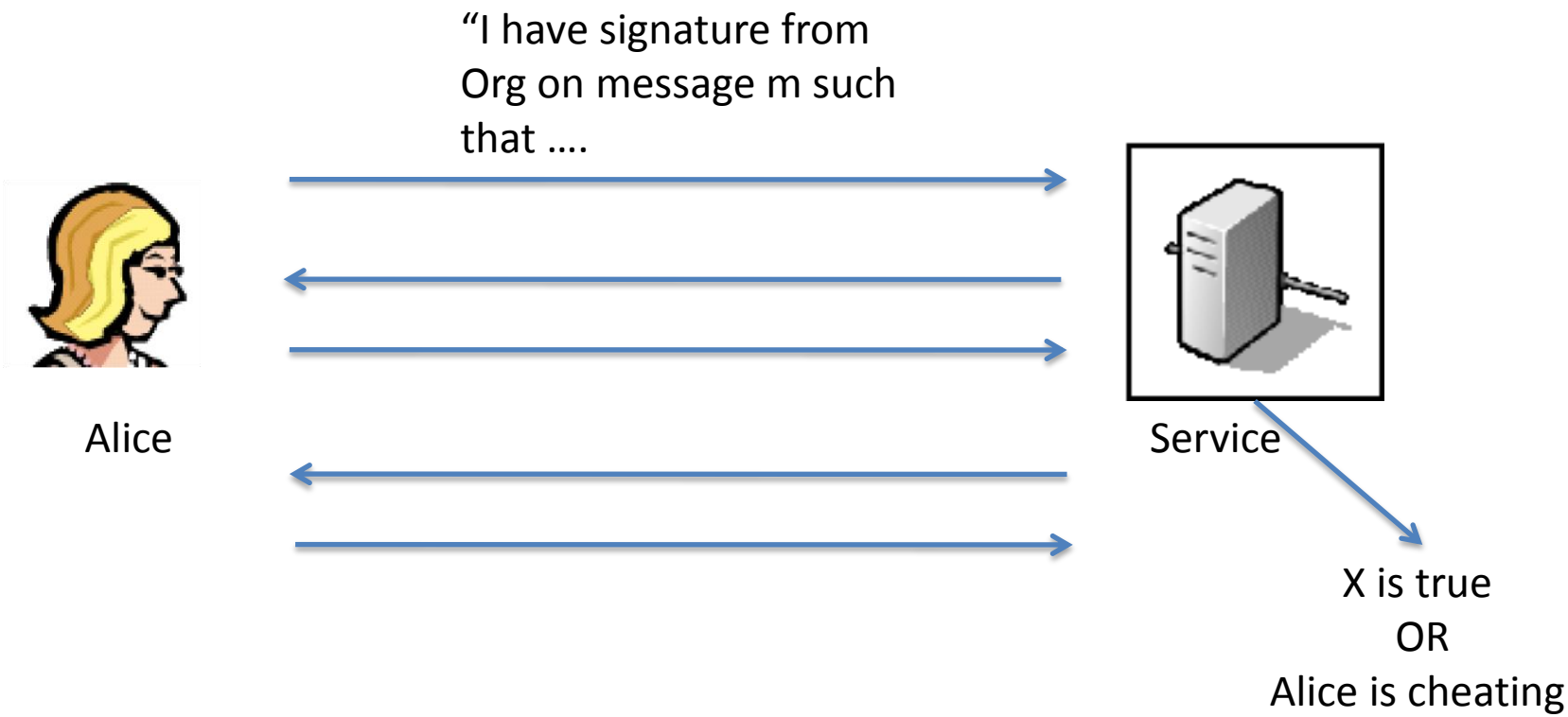


Service

X is true
OR
Alice is cheating

Alice wants to convince service that statement X is true,
Without revealing any other information

Zero Knowledge Proofs

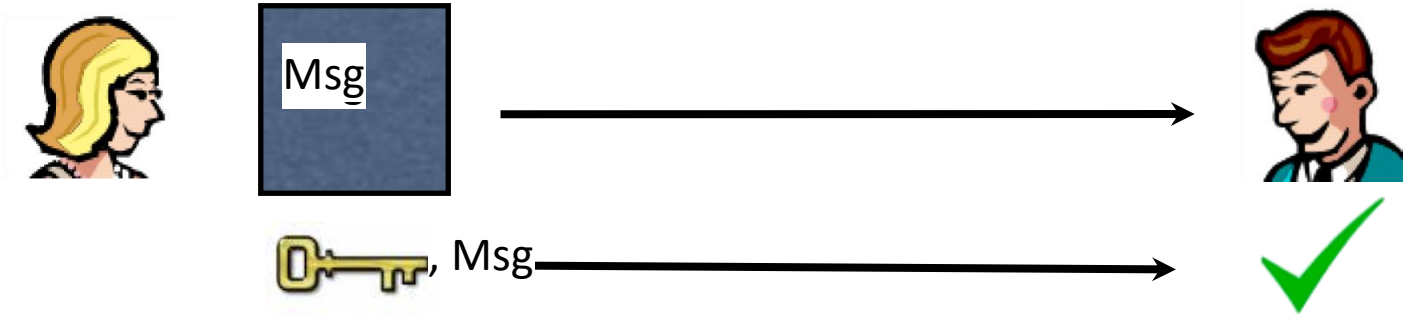


Alice wants to convince service that she has such a signature
Without revealing any other information

Fiat Shamir: get challenge from hash function

Commitments

- Like locked box or safe
- Hiding – hard to tell which message is committed to
- Binding – there is a unique message corresponding to each commitment



E.g. Pederson Commitment: $C = g^m h^r$

Blind signatures

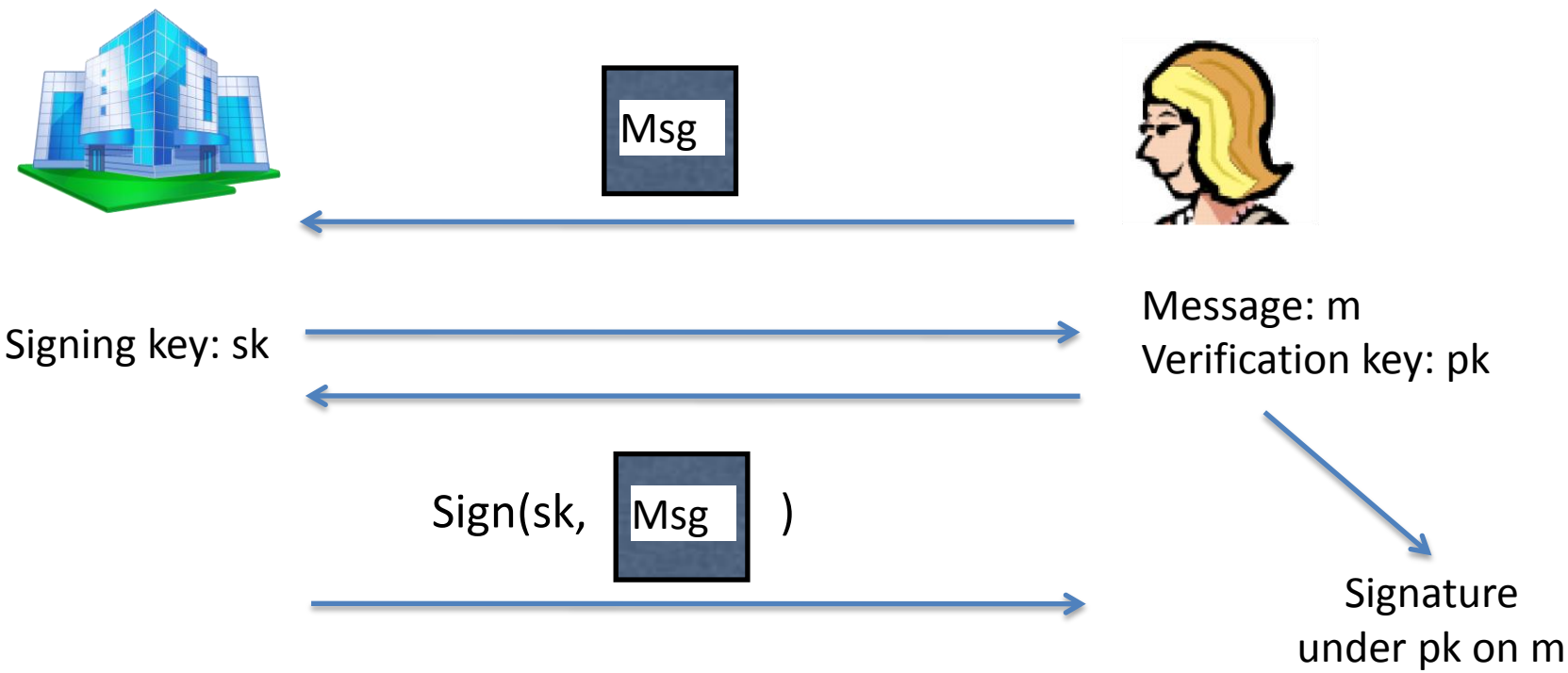
Signing key: sk

Message: m
Verification key: pk

Signature
under pk on m

Alice learns only signature on her message.
Signer learns nothing.

Blind signatures



Alice learns only signature on her message.
Signer learns nothing.

How it works (abstractly)

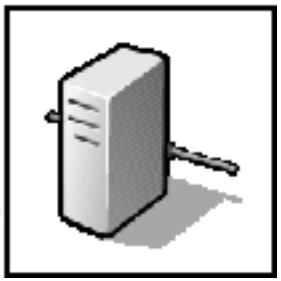
Anonymous Credentials/Minimal Disclosure Tokens

Organization

secret

- Prevents impersonation
- Tie multiple creds to one user

Alice



Service

"I have a cred from Org saying
WA resident
Age >21"

Cred from Org
Name Alice
Address
Birthdate
Birthplace
Citizenship
…

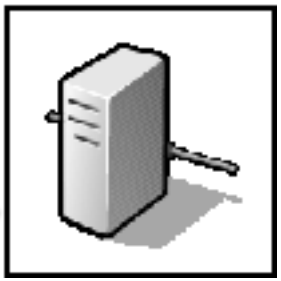
How it works

Anonymous Credentials/Minimal Disclosure Tokens

Organization

secret

Alice



Service

Prove
"I have a cred from
Org saying
WA resident
Age >21"

Signature fro
secret
Name Alice
Address
Birthdate
Birthplace
Citizenship
…

•Need to generate signature without Org learning secret

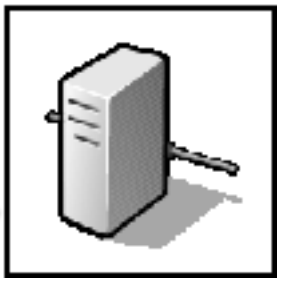
How it works

Anonymous Credentials/Minimal Disclosure Tokens

Organization

secret

Alice



Service

Prove
"I have sig from Org
*
@@@, WA
#>21

Signature from Org
secret
Name Alice
Address
Birthdate
Birthplace
Citizenship
…

How can we "prove" this
without revealing
- secret
- rest of message
- signature

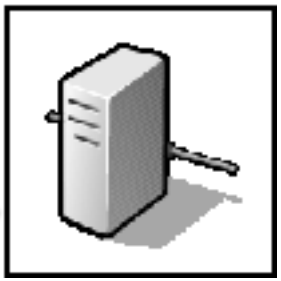
How it works

Anonymous Credentials/Minimal Disclosure Tokens

Organization

secret

Alice



Service

Zero Knowledge Proof

"I have sig from Org
*
@@@, WA
#>21

Signature from Org
secret
Name Alice
Address
Birthdate
Birthplace
Citizenship
…

Proof does not reveal

- secret
- rest of message
- signature

Is this practical?

- Depends on how we implement proofs and blind signatures
- Two main approaches:
  - RSA type signatures [CL02]
    - Based on strong version of RSA assumption
    - Idemix (IBM)
  - DSA type signatures [Brands 99]
    - Based on discrete logarithm problem (more or less)
    - UProve (Microsoft)
  - Also third type based on elliptic curves with pairings [BCKL08]
    - Less efficient
    - Allows for extra features

Is this practical?

- Key tool: Proof of knowledge of discrete log
  - Given Y, g, prove "I know x such that $Y = g^x$"
  - Generalized:
    - Given Y, g, h, prove "I know x, z such that $Y = g^x h^z$"
    - Given Y, W, g, h, prove "I know x such that $Y = g^x$ and $Z = h^x$"
    - Prove arithmetic relationships
    - Prove that values are not equal
    - …..
  - Prove statements about commitments, signatures, encryptions, etc.

Is this practical?

Alice

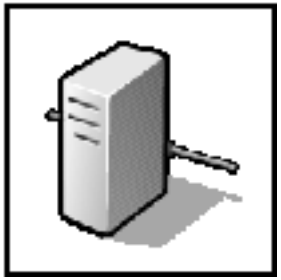
Knows X is true

I know x such that $Y = g^x$

$A = g^r$

c

$z = r + cx$



Service

Check if $AY^c = g^z$

Alice wants to convince service that she knows x,
Without revealing any other information

Is this practical?

- Key tool: Proof of knowledge of discrete log
  - Given Y, g, prove "I know x such that $Y = g^x$"
  - Generalized:
    - Given Y, g, h, prove "I know x, z such that $Y = g^x h^z$"
    - Given Y, W, g, h, prove "I know x such that $Y = g^x$ and $Z = h^x$"
    - Prove arithmetic relationships
    - Prove that values are not equal
    - …..
  - Prove statements about commitments, signatures, encryptions, etc.

Roadmap

- Review crypto tools
- Construct basic credential systems
- **Additional issues**
  - Revocation
  - Deciding who to revoke
- Additional features
  - Non-interactive credentials/signatures
  - Delegation
- Conclusion

Credentials

- Now we have an anonymous credential system. What other issues come up?

- What about misuse of credentials?
  - If everyone is completely anonymous, how do we deal with misuse of privileges?
  - Can we revoke credentials?
  - Can we even tell whose credential to revoke?

Credential Revocation

- Expiration dates
  - Can be embedded in anonymous credentials – prove that expiration date > current date
- CRL (Certificate Revocation List)
  - List of all revoked certificates
  - Verifier can check that presented cert is not on list
  - Anonymous CRLs? : How to check that the credential is not on the revoked list without compromising privacy?

Anonymous CRLs

- Option 1:
  - Verifier gives Alice CRL
  - Alice proves that her credential is not on the list (for each value on the list, prove that her value is different)
- Option 2:
  - We can do this more concisely using *accumulators*
  - Issuer publishes accumulator – single value that encapsulates all revoked credentials (or all good credentials)
  - Users, given updates to CRL (or list of all good credentials), can give short proof they are not on CRL (or they are on whitelist).

How do we deal with misuse of privileges?
(How do we tell who to revoke?)

- Depends how we define misuse:
  - Simple type: reused one-use token
    - Tried to vote twice in a poll
    - Tried to spend transit token twice
  - More complex scenarios
    - Trust a judge to determine misuse

How do we deal with misuse of privileges?
One-Time/Limited Use Credentials

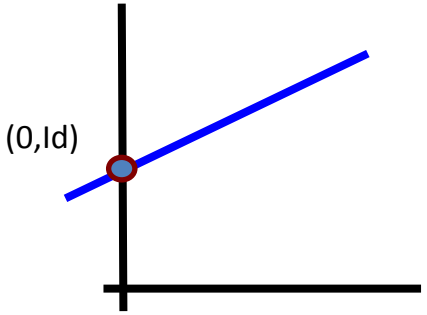
- Credentials meant to be used only once (or fixed number of times)
  - Subway tokens
  - Electronic currency (e-cash)
  - Movie tickets
  - Access passes for online service

- Service records "serial number" on every token used
- As long as each token is only used once
  - user is anonymous
  - multiple tokens used by the same user are unlinkable
- If token is used twice, identity of user is revealed.

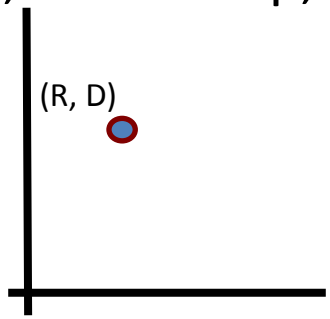
- Previous work [Chaum83, CFN90,… CHL05,… BCKL09]

How do we deal with misuse of privileges?
One-Time/Limited Use Credentials

- Anything digital can be copied!
- Why can't Alice just copy her credential, and give one copy to Bob and the other to Carol?
  - Efficient Solution: offline e-cash [CFN90]
    - Cred includes (T, Id) unknown to Org
      - Id: the identifying info for the user
      - T: the slope of a line with f(0)=Id

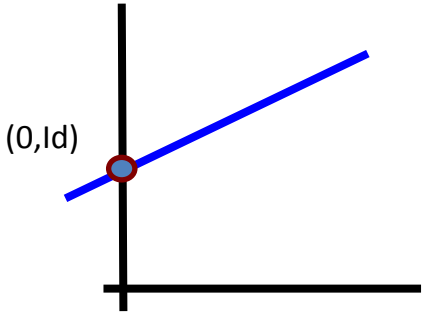


    - When cred is used it includes (R, D):
      - R: transaction information (station name, timestamp, etc)
      - D: Doublespending tag (f(R)).
        - » (R,D) and (R',D') gives Id

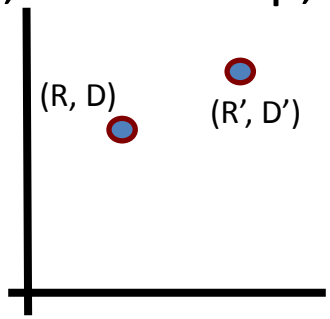


How do we deal with misuse of privileges?
One-Time/Limited Use Credentials

- Anything digital can be copied!
- Why can't Alice just copy her credential, and give one copy to Bob and the other to Carol?
  - Efficient Solution: offline e-cash [CFN90]
    - Cred includes (T, Id) unknown to Org
      - Id: the identifying info for the user
      - T: the slope of a line with f(0)=Id

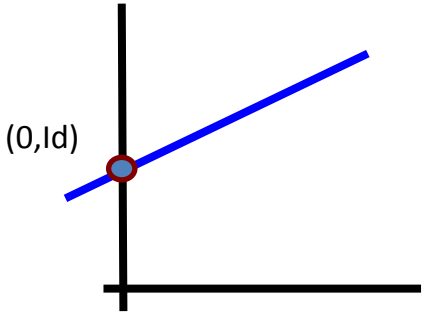


    - When cred is used it includes (R, D):
      - R: transaction information (station name, timestamp, etc)
      - D: Doublespending tag (f(R)).
        - » (R,D) and (R',D') gives Id

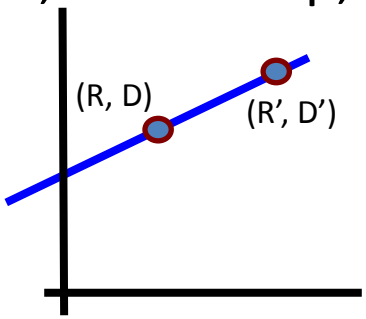


How do we deal with misuse of privileges?
One-Time/Limited Use Credentials

- Anything digital can be copied!
- Why can't Alice just copy her credential, and give one copy to Bob and the other to Carol?
  - Efficient Solution: offline e-cash [CFN90]
    - Cred includes (T, Id) unknown to Org
      - Id: the identifying info for the user
      - T: the slope of a line with f(0)=Id

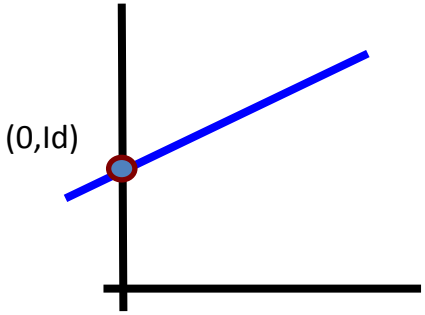


    - When cred is used it includes (R, D):
      - R: transaction information (station name, timestamp, etc)
      - D: Doublespending tag (f(R)).
        - » (R,D) and (R',D') gives Id

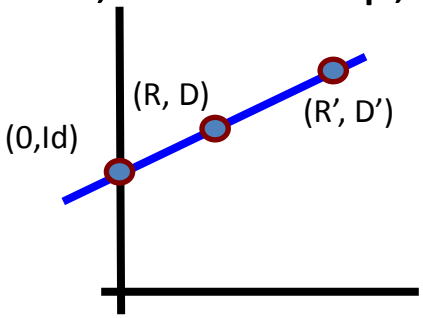


How do we deal with misuse of privileges?
One-Time/Limited Use Credentials

- Anything digital can be copied!
- Why can't Alice just copy her credential, and give one copy to Bob and the other to Carol?
  - Efficient Solution: offline e-cash [CFN90]
    - Cred includes (T, Id) unknown to Org
      - Id: the identifying info for the user
      - T: the slope of a line with f(0)=Id



    - When cred is used it includes (R, D):
      - R: transaction information (station name, timestamp, etc)
      - D: Doublespending tag (f(R)).
        - » (R,D) and (R',D') gives Id



How do we deal with misuse of privileges? More complex scenarios

- Trusted judge (anonymity revocation authority)
  - Alice also sends encryption of her identity under judge's public key (*Identity escrow*)
  - In case of misuse,
    - Service gives encryption to judge
    - If judge agrees credential was misused, it can decrypt and find Alice's identity
- Disadvantage: users have no anonymity w.r.t. revocation authority
    - Judge must be trusted
- Advantage: very flexible
- Techniques: Verifiable encryption

Roadmap

- Review crypto tools
- Construct basic credential systems
- Additional issues
  - Revocation
  - Deciding who to revoke
- **Additional features**
  - Non-interactive credentials/signatures
  - Delegation
- Conclusion

Other Features

- Log of all valid users and their credentials?
- Post an anonymous message with proof of a credential?
- Non-interactive credentials (Signatures)
  - Challenge: proof needs to be one message
  - Non interactive Zero Knowledge proof
    - Fiat-Shamir (using hash as challenge)
    - Or recent proof techniques based on special elliptic curves

Delegation

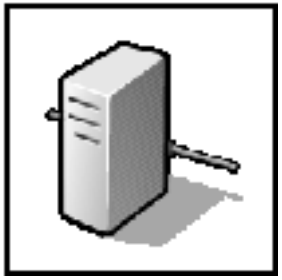
Webmaster

Forum Moderator

Cred from Webmaster
Moderator

Alice

Cred from Moderator
who has cred from Webmaster
Registered User



"I have a level 2 cred from Webmaster saying
Registered user"

Forum Moderator and Alice should remain anonymous

Delegation

Webmaster

Forum Moderator

Cred from Webmaster
Moderator

Alice

Cred from Moderator
who has cred from Webmaster
Registered User

"I have a level 2 cred from Webmaster saying
Registered user"

Forum Moderator and Alice should remain anonymous

Delegation

Webmaster

Forum Moderator

Cred from Webmaster
Moderator

Alice

Cred from Moderator
who has cred from Webmaster
Registered User

"I have a level 2 cred from Webmaster saying
Registered user"

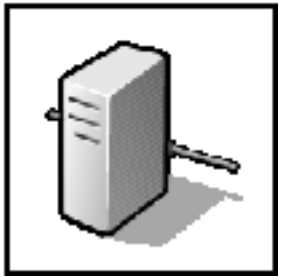
Forum Moderator and Alice should remain anonymous

Delegation

Webmaster

Forum Moderator

Alice



Sig from Webmaster
$secret_{Bob}$
Moderator

Sig from Bob
$secret_{Alice}$
Registered User

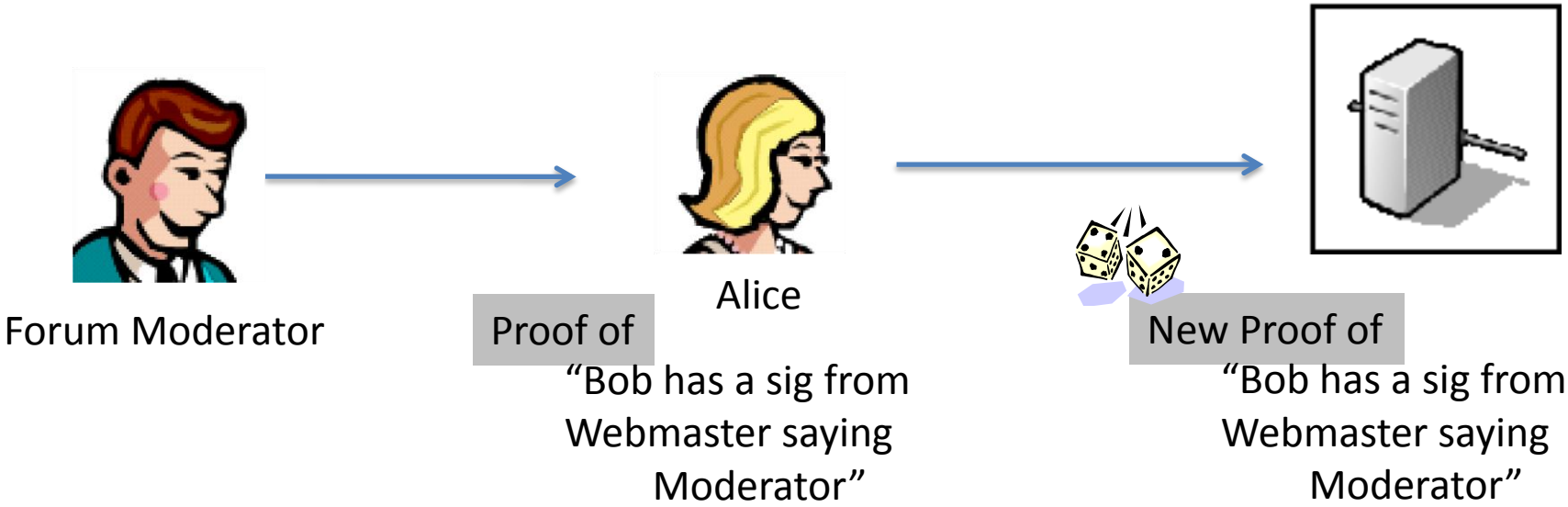
Proof of
"Bob has a sig from Webmaster saying Moderator"

Proof of
"I have a sig from Bob saying Registered User"

Proof of
"Bob has a sig from Webmaster saying Moderator"

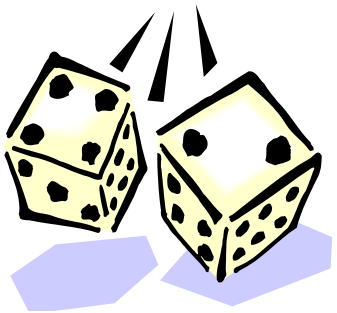
If Alice uses the same proof each time, service will know

Randomizable proofs



- Can we do this?
  - Not clear with traditional techniques
  - Need proofs with special properties

Delegating Credentials



- Randomizable proof system
  - Elliptic curve with pairings based proofs [GOS06,GS08] satisfy this property
- Delegatable Anonymous Credentials [BCCKLS09]
  - Requires some additional techniques
- In progress: delegatable one-time credentials (i.e. transferrable e-cash) [CCKR]

Roadmap

- Review crypto tools
- Construct basic credential systems
- Additional issues
  - Revocation
  - Deciding who to revoke
- Additional features
  - Non-interactive credentials/signatures
  - Delegation
- **Conclusion**

Other issues

- How do you tie a digital credential to a real world person/identity?
  - Harder when you add anonymity
  - Circular encryption, smart card, POK of credit card number
- Safety in numbers:
  - What if the issuer only ever issues one credential?
    - Even with anonymous credentials, if yours is the only credential issued, issuer will know when you show it
- Adoption – will anyone ever use this?
  - Do people care enough about privacy?

Questions